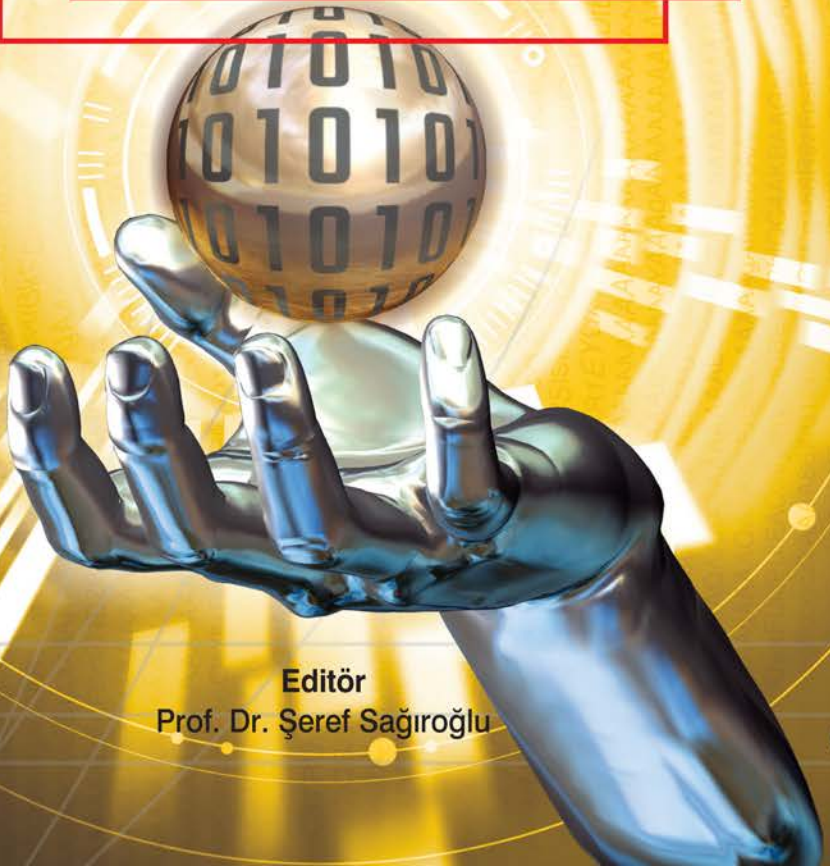
BGD Siber Güvenlik ve Savunma Kitap Serisi 3

BİLGİ GÜVENLİĞİ DERNEĞİ
Information Security Association

HAVELSAN

Siber Güvenlik ve Savunma

STANDARTLAR VE UYGULAMALAR



Editör
Prof. Dr. Şeref Sağıroğlu

Grafiker Yayınları

Siber Güvenlik ve Savunma

STANDARTLAR ve UYGULAMALAR

Editör
Prof. Dr. Şeref SAĞIROĞLU

Yazarlar
Prof. Dr. Şeref SAĞIROĞLU - Onur AKTAŞ
A. Oğuzhan ALKAN - Bilgehan ARSLAN
Dr. Öğr. Üyesi Atila BOSTAN - Dr. Öğr. Üyesi Eyüp Burak CEYHAN
Dr. Öğr. Üyesi İsmail Fatih CEYHAN
Dr. Öğr. Üyesi Onur ÇAKIRGÖZ
Dr. Öğr. Üyesi Mehmet DEMİRCİ - Sedef DEMİRCİ
Doç. Dr. Gülüstan DOĞAN
Dr. Öğr. Üyesi Muharrem Tuncay GENÇOĞLU
Doç. Dr. Ali Hakan IŞIK - Burak ÖZÇAKMAK
Dr. Öğr. Üyesi A. Nurdan SARAN - Doç. Dr. Gökhan ŞENGÜL
Seda YILMAZ - Özgür YÜREKTEN

Ankara 2019

Siber Güvenlik ve Savunma: Standartlar ve Uygulamalar

Editör
Prof. Dr. Şeref SAĞIROĞLU

Yazarlar
Prof. Dr. Şeref SAĞIROĞLU
Doç. Dr. Gökhan ŞENGÜL
Doç. Dr. Ali Hakan IŞIK
Doç. Dr. Gülüstan DOĞAN
Dr. Öğr. Üyesi Atila BOSTAN
Dr. Öğr. Üyesi Eyüp Burak CEYHAN
Dr. Öğr. Üyesi İsmail Fatih CEYHAN
Dr. Öğr. Üyesi Onur ÇAKIRGÖZ
Dr. Öğr. Üyesi Mehmet DEMİRCİ
Dr. Öğr. Üyesi Muharrem Tuncay GENÇOĞLU
Dr. Öğr. Üyesi A. Nurdan SARAN
Onur AKTAŞ
A. Oğuzhan ALKAN
Bilgehan ARSLAN
Sedef DEMİRCİ
Burak ÖZÇAKMAK
Seda YILMAZ
Özgür YÜREKTEN

ISBN: 978-605-2233-42-9

1. Baskı
Aralık, 2019 / Ankara
1500 Adet

Grafiker Yayınları
Yayın No: 334
Web: grafikeryayin.com

Kapak, Sayfa Tasarımı, Baskı ve Cilt
Grafiker
Grafik-Ofset Matbaacılık Reklamcılık San. ve Tic. Ltd. Şti.
1. Cadde 1396. Sokak No: 6
06520 (Oğuzlar Mahallesi) Balgat-ANKARA
Tel : 0 312. 284 16 39 Pbx - Faks : 0 312. 284 37 27
E-posta : grafiker@grafiker.com.tr
Web : grafiker.com.tr

HAVELSAN Bu kitap HAVELSAN'ın katkılarıyla basılmıştır.

İÇİNDEKİLER

3. BÖLÜM
BİLGİ, ÜRÜN VE SİSTEM AÇISINDAN SİBER GÜVENLİK STANDARTLARI

4. BÖLÜM
SİBER GÜVENLİKTE ASKERİ STANDARTLAR KAPSAMINDA AQAP İNCELEMESİ

6. BÖLÜM
WEB UYGULAMA ZAFİYETLERİ VE ÖNLEMLER

EDİTÖRDEN

Bilgi Güvenliği Derneği (BGD), kuruluşundan bugüne kadar ülkemizin **bilgi ve siber güvenliği ile savunmasının** gelişimine katkı sağlamakta, birikimini çevreye aktarmakta, bilgi güvenliği alanında açık kaynak yaklaşımını benimseyen ve bu kapsamda içerik üretilmesine ve geliştirilmesine destek vermekte, bunları yaymakta, paylaşmakta ve kamuoyunun kullanımına sunmaktadır. Düzenlediği ulusal ve uluslararası etkinliklere ait bildiri kitapları serisi, hazırladığı raporlar, taslak strateji dokümanları, eylem planları vb. bunların başında gelmektedir. **Siber Güvenlik ve Savunma Kitapları Serisi** ise BGD'nin ülkemizin siber güvenliğine önemli bir katkısıdır.

Tehditlerin, saldırıların ve açıklıkların artması, boyut ve yön değiştirmesi, farklılaşması, siber tehdit ekosisteminin gittikçe güçlenmeye başlaması, kritik altyapıların hedef haline gelmesi, bilgi ve kaynak hırsızlıklarının çoğalması, yeraltı yapıların etkinleşmesi, siber saldırıların artık savaşa dönüşmesi, siber suç ve suçlularının çoğalması, siber terörün yaygınlaşması vb. olumsuzlukların hızla artması, yapılacak mücadele, alınacak önlem ve karşı koymak için yaklaşımlara duyulan ihtiyacı artırmıştır. Kapsamlı bir mücadele için; ulusal strateji ve eylem planlarına, araştırma merkezlerine, gelişmiş altyapı ve araçlara, lisans ve lisansüstü programlara, nitelikli insan kaynağına, yerli ve milli ürünlerin geliştirilmesine, siber güvenlik ve savunma ekosisteminin oluşturulmasına, ulusal siber olaylara müdahale ekiplerinin sayısının ve niteliğinin arttırılmasına, Ulusal Siber Olaylara Müdahale Merkezinin (USOM) kapsamının büyütülmesine, siber güvenliğin ulusal güvenlikle bütünleşmesine ihtiyaç vardır. Duyulan bu ihtiyacı bir nebze de olsa karşılamak için bu kitap serisi hazırlanmıştır. Bu kitap serisinde, 100'e yakın konu başlığı irdelenmektedir. Her bölümde, farklı bir konu siber güvenlik ve sa-

vunma kapsamında ele alınmakta, değerlendirilmekte ve alınması gereken önlemlere yer verilmektedir.

Bu kitap serisinde sunulan konu başlıkları, ülkemizde bu alanda çalışan akademisyenler, uzmanlar ve çalışanlar ile paylaşılmış ve bu kitap serisine katkı sağlamaları istenilmiştir. Zamanı uygun olan, katkı vermek isteyen uzman veya akademisyenler belirlenen bir konuda bölüm yazarı olmaları için davet edilmişlerdir. Belirlenen süre içerisinde bölümlerini tamamlayan yazarlarımızın eserleri ise uygun olan ciltlerde basılmaktadır. Bundan sonraki süreçte, belirlenen diğer konular belirli sürelerde tamamlanıp takip eden ciltlerde yayımlanacaktır. Siber güvenlik ve savunmaya çok kapsamlı bir bakış sunmayı amaçlayan ve farklı başlıkları bir araya getiren bu kapsamlı eserin, ülke siber güvenliğimiz ve savunmasına katkı sağlaması beklenmektedir.

Kitap serimizin üçüncü cildinde, 13 farklı bölüm sunulmuştur. Siber güvenliğin farklı açılardan irdelendiği bu ciltte; siber güvenliğin kapsamı ve boyutu, "standartlar ve uygulamalar" açısından değerlendirilmiştir. Ayrıca, alınabilecek önlemler, karşılaşılan yeni riskler ve problemlere yer verilmiş, karşılaşılabilecek risklere dikkat çekilmiş ve sonuçta alınması gereken önlemler ve yapılması gerekenler özetlenmiştir. Her bir bölüm; ülkemizde bu alana katkı sağlayan, bu alanda eğitim almış, tez hazırlamış, çalışmalar yapmış değerli akademisyen, kamu çalışanı ve üst düzey yöneticiler tarafından hazırlanmıştır. Her bir bölüm, birbirinden bağımsız olarak hazırlansa da konu bütünlüğü ve devamlılığının sağlanmasına mümkün olduğunca dikkat edilmiştir. Her bölüm editörler olarak tarafımızdan değerlendirilmiş, yazarlara konu içeriği ve başlıklarla ilgili olarak önerilerde bulunulmuş, düzeltmeler yapılması istenilmiş ve sonuçta yapılan değişiklikler dikkate alınarak bu kitap hazırlanmıştır. Kitapta yazılan bölümler tekrar tekrar kontrol edilmiş, yapılan çalışmalar ise her bölümün sonunda bölüm yazarları tarafından değerlendirilmiştir.

Bu kitabın, siber güvenlik ve savunma konusunda yapılacak çalışmalara ışık tutması, yeni çalışmaların yapılmasına katkı sağlaması, bu konuda yapılacak olan işbirliklerini geliştirmesi, bu konunun boyutunun ve kapsamının daha iyi anlaşılmasına katkı sağlaması ve en önemlisi ise bilgi güvenliği ve siber güvenlik alanında duyulan ihtiyacı karşılamanın yanında açık kaynak olarak sunulması ile de kaynaklara erişimi kolaylaştırıcı **bir başvuru kitabı serisi** olması

beklenmektedir**. Bu eser serisi açık kaynak olarak**, Bilgi Güvenliği Derneği internet sayfasında (www.bilgiguvenligi.org.tr) yayımlanmaktadır.

Kitap bölüm yazarlarımız; alan uzmanlıklarına göre her bir bölümü hazırlamışlar, kişisel bilgi birikimlerini hazırladıkları bölümlerde sunmuşlar, eserlerinin açık kaynak olarak yayımlanmasını kabul etmişler ve bu kitabın basımı ve dağıtımı ile ilgili olarak herhangi bir telif hakkı talep etmemişlerdir. Yazarlarımıza, bu kitap serisinin editörü olarak çok özel teşekkürlerimizi ve şükranlarımızı sunarız.

Kitabın titizlikle hazırlanmasında, kontrolünde ve basılmasında başta yazarlarımız olmak üzere emeği geçen tüm paydaşlarımıza, kitap serisi fikrimizi hayata geçiren Bilgi Güvenliği Derneği Yönetim Kuruluna teşekkürlerimizi sunarız.

Prof. Dr. Şeref SAĞIROĞLU
BGD Kurucu Üyesi ve II. Başkanı
Gazi Üniversitesi MF Bilgisayar Mühendisliği Bölüm Başkanı
FutureTech Genel Müdürü

BİLGİ GÜVENLİĞİ DERNEĞİ'NDEN

Bilgi Güvenliği Derneği (BGD); 22 Temmuz 2007 tarihinde, Bilgi Güvenliği ve Siber Güvenlik alanında toplumun her kesiminde bilgi ve bilinç düzeyini arttırmak, bu konu ile ilgili teknolojik gelişmeleri izlemek, yerli ve milli teknolojilerin geliştirilmesine katkı sağlamak; bireysel, kurumsal ve ulusal düzeydeki riskler konusunda farkındalık oluşturmak ve kamu-sektör-üniversite işbirliklerini geliştirmek amacı ile kurulmuştur.

BGD'nin vizyonu; "bilgi güvenliği alanında ulusal ve uluslararası düzeyde tarafsız, güvenilir ve etkin bir ulusal sivil toplum kuruluşu olmaktır." BGD vizyonu doğrultusunda; tüm paydaşlarla işbirliği yaparak mevzuatın oluşturulmasında ve geliştirilmesinde aktif rol almakta, gerçekleştirdiği konferans, sempozyum, çalıştay ve eğitimler, yayımladığı rapor ve yazılar ile farkındalığın oluşmasına ve bunun davranışa dönüştürülmesine katkılar sağlamaktadır.

Derneğimiz bu kapsamda; "Ulusal Siber Güvenlik Strateji Belgesi" ve "Ulusal Siber Güvenlik Eylem Planı" hazırlanmasına öncülük etmiş, hazırladığı taslak metinler kabul görmüş ve sonuçta ülkemizin siber güvenlik stratejisi ve eylem planlarının gecikmeden yayımlanasına katkı sağlamıştır. Aynı zamanda; bu alanda nitelikli insan kaynağı yetiştirilmesi, mesleki yeterliliklerin belirlenmesi, kamu-endüstri-üniversite işbirliklerinin geliştirilmesi, kümelenme çalışmalarının başlaması gibi önemli politika ve stratejilerin oluşturulmasında etkin rol üstlenmektedir.

BGD, "Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı", "Ulusal Siber Güvenlik Stratejisi Çalıştayı", "Veri Merkezleri ve Siber Güvenlik Çalıştayı", "Siber Güvenlik Hukuku Çalıştayı", "Mobil Dünyada Çocuk ve Gençlerin Güvenliği Sempozyumu", "IPv6 Konferansı", "Kritik Enerji Altyapılarının Korunması Sempozyumu", "Ulusal Siber Terör Konferansı", "Siber Güvenlik Yaz Kampı" gibi

etkinlikleri düzenleyerek ve destekleyerek bilgi güvenliğine ihtiyaç duyulan her alanda çalışmalar yürütmüştür. Cumhurbaşkanlığı, Milli Eğitim Bakanlığı, Ulaştırma ve Altyapı Bakanlığı, Bilgi Teknolojileri ve İletişim Kurumu, Sosyal Güvenlik Kurumu ve Üniversiteler gibi farklı paydaşlar ile çalışmalar yürütmektedir.

BGD, **CyberMag Dergisi** ile toplumun tüm kesimlerine ulaşmaya çalışmaktadır. 2019 yılında 12'ncisini düzenleyeceğimiz "Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı" kısaca **ISCTurkey Konferansı** olarak bilinen uluslararası etkinlik ile kurulduğu günden bu yana kamu kurumları, özel sektör ve üniversiteleri bir araya getirmeyi başarmıştır.

Bununla birlikte, bilgi güvenliği ve siber güvenlik alanında **ulusal ve uluslararası düzeyde tarafsız, güvenilir ve etkin bir ulusal sivil toplum kuruluşu olan Bilgi Güvenliği Derneği**, bünyesinde oluşturulan BGD Genç ile; bireysel, kurumsal, ulusal ve evrensel boyutlarda bilgi ve iletişim güvenliği alanında teknik, bilimsel, sosyal ve kültürel faaliyetler yürütmek, orta ve yüksek öğrenim gören genç üyelerimizin mesleki gelişimini artırmak, siber güvenlik alanında farkındalık oluşturmak, ülkemizin siber güvenlik uzman kaynağını oluşturmak için gençlerimizin bu alana ilgisini artırmak için faaliyet göstermektedir.

ISCTurkey etkinlikleri, Gazi Üniversitesi, İstanbul Teknik Üniversitesi ve Ortadoğu Teknik Üniversitesi işbirliği ile düzenlenmekte, Ulaştırma ve Altyapı Bakanlığı ile Bilgi Teknolojileri ve İletişim Kurumu tarafından sürekli desteklenmektedir. Bu etkinlik, Avrupa Ağ ve Bilgi Güvenliği Ajansı (ENISA) tarafından "Avrupa Siber Güvenlik Ayı" platformu etkinliklerine dâhil edilen ilk ve tek etkinliktir. Ayrıca, düzenlendiği ilk yıldan beri ülkemizin siber güvenlik alanındaki bilimsel ve sektörel çalışmaların paylaşıldığı, üniversite-kamu-endüstri işbirliğinin geliştirildiği, kamunun bilgilendirildiği, paydaşların eğitildiği, tüm bilim insanları, araştırmacılar ve sektörel uygulayıcılar arasında bilgi alışverişinin sağlandığı ülkemizde bu alandaki en önemli etkinliktir.

Şubat 2019'da yeni bir yönetim kuruluyla göreve başlayan BGD Yönetimi, yapılan çalışmalara yenilerinin eklenmesi, açık kaynak olarak paylaşılacak olan çalışmaların artması ve ülkemizin bu alanda

ihtiyaç duyduğu Türkçe kaynak ihtiyacına katkılar sağlanmasını desteklemektedir.

Bu kitabın hazırlanmasında katkı sağlayan başta editörlerimize, hiç bir beklenti içerisinde olmadan bölüm yazan ve bunu kamuoyu ile ücretsiz paylaşılması konusunda destek veren saygıdeğer yazarlarımıza, destekleyicimize ve bugüne kadar ülke bilgi güvenliği ve siber güvenliğinin gelişimine katkı sağlayan BGD yöneticilerimize ve üyelerimize bu vesile ile şükranlarımı sunarım.

Bu kitap serisinin üçüncüsünün, ülkemiz siber güvenlik ve savunma çalışmalarına katkılar sağlaması dileğiyle.

Ahmet Hamdi ATALAY
Bilgi Güvenliği Derneği YK Başkanı

ÖN SÖZ

Günümüzde siber güvenlik, beşinci savaş ortamı olarak kabul edilmenin ötesinde tüm ülkeler için ulusal güvenliğin ayrılmaz ve en önemli bileşeni olarak değerlendirilmektedir.

Yerli, güvenilir, yenilikçi ve yüksek kaliteli Siber Güvenlik çözümleri geliştirerek ülkemizin siber güvenliğinin sağlanmasında ana unsur; uluslararası pazarlarda güçlü ve güvenilir Siber Güvenlik teknoloji ve hizmet sağlayıcısı olmak vizyonu ile çalışmalarını yürüten HAVELSAN, ülkemizin siber uzayda güvenliğini sağlayacak bir mükemmeliyet merkezi olmak, ülkemizin yetenek ve kaynaklarının etkin kullanılmasına öncülük etmek adına var gücüyle çalışmalarını sürdürmektedir.

Bir Türk Silahlı Kuvvetlerini Güçlendirme Vakfı şirketi olan HAVELSAN tarafından hayata geçirilen Siber Savunma Teknoloji Merkezi çatısı altında siber güvenlik operasyon merkezi hizmetleri, kurumsal siber güvenlik danışmanlık ve destek hizmetleri, güvenlik analiz ve test hizmetleri, siber güvenlik eğitimleri ve yerli siber güvenlik ürünleri geliştirme faaliyetleri yürütülmektedir.

Siber güvenlik alanında ülkemizin nitelikli insan kaynağını artırmak için Türkçe kaynak ihtiyacının en az bu alanda verilen eğitimler kadar değerli olduğunun bilincinde olan HAVELSAN, bu ihtiyacı karşılamada katkı sağlayacak değerli bir yayın olarak gördüğü bu kitabı desteklemektedir.

Ahmet Hamdi ATALAY
HAVELSAN Genel Müdürü

Siber Güvenlik Matematiği

BÖLÜM 1

M. Tuncay GENÇOĞLU

SİBER GÜVENLİK MATEMATİĞİ

Bu bölümde genel olarak Siber Güvenlik alanındaki uygulamalarda, problem ve çözümlerinde matematiksel model ortaya koymanın dolayısıyla matematiğin önemini vurgulamak ve farkındalık yaratmak hedeflenmektedir.

1.1. Giriş

Varlıkların sayısı, biçimi ve düzenlenmesi mantığı ile ilgilenen, niceliklerin, yapıların, uzayın ve değişikliğin irdelendiği bir bilim dalıdır matematik. Matematik; sayma, hesaplama, ölçüm ve fiziksel nesnelerin şekilleri ve hareketleri için mantıksal muhakeme ve soyutlaması ile gelişmiş, ölçü, özellik ve nesneler arasındaki ilişkiler bilgisi üzerine kurulmuş bir sistemdir. Sistem kuramsal veya uygulamalı olarak cebir, geometri, trigonometri, istatistik ve hesabı (Calculus) içerir.

Siber güvenlik ise; "siber ortamı oluşturan bilişim sistemlerinin saldırılardan korunmasını, bu ortamda işlenen veri ve bilginin gizlilik, bütünlük ve erişebilirliğinin güvence altına alınmasını, saldırıların ve siber güvenlik olaylarının tespit edilmesini, bu tespitlere karşı mekanizmalarının devreye alınmasını ve sonrasında ise sistemlerin yaşanan siber güvenlik olayı öncesi durumlarına geri döndürülmesidir [1].

Bilişim ise bilgi ve bilginin otomatik olarak işlenmesiyle ilgilenen bir yapısal bilim dalıdır.

Matematiğe benzer şekilde Bilişim Bilimi (Enformatik) bilginin, özellikle elektronik makineler aracılığıyla, düzenli ve ussal biçimde işlenmesi bilimidir. Bilişim bilimi, bilgi işlemlerinde uygulanabilen (soyut) matematiksel yapıları inceler. Bilişimin amacı ve görevi ise; bir yandan (matematiğin alt dalı olarak) temel aksiyomatik

matematiksel teoriler üretmek, ikinci olarak tüm diğer uzmanlık dallarının nesnelerini ve süreçlerini çözümleyip soyut matematiksel yapılara ve algoritmalara dönüştürmek ve üçüncü olarak soyut matematiksel yapıların aktarılabileceği, saklanabileceği ve algoritmalarla otomatik olarak işlenebileceği makineleri tasarlamaktır. Bu tanıma göre Matematik tüm bilimlerin babası ise bilişim uygulamaları da katkısından dolayı tüm bilimlerin anasıdır.

Bilişimin kuramsal temellerini bilmek bilgisayar bilimcisine, bilgisayar mühendisine, yazılım mühendisine ve bilişim sistemi tasarımcısına büyük katma değer kazandırır; üstelik bazı problemler vardır ki, bilişim matematiği konuları bilinmeden gerçekleştirildiğinde gerçek çözümden uzak olur; fazladan döngüler, fazladan bellek alanı kullanıldığı gibi elde edilen sonuçlara da pek güvenilmez; yani böcekleri bol olur.

Bilişim matematiği, ayrıca, donanım tasarımcıları için bile, özellikle gömülü sistemlerin tasarımcıları için gerekli bir konudur. İş yaşamında veya günlük yaşamda karşılaşılan problemleri modellemek ve onlara ait çözümleri evrensel düzeyde algoritmik olarak tasarlayabilmek için bilişim matematiği mutlaka bilinmelidir; önce çözüm için en uygun model belirlenmeli, daha sonra alt bileşenleri ortaya konularak problem, matematiksel olarak çözülmelidir.

Tarihsel olarak matematik bilişimi, bilişim de matematiği etkilemiş ve tetiklemiştir. İnsan doğası, ilk çağlarda hesaplama gereksinimini hissetmiş ve hesaplamayı önce parmakları kullanarak daha sonra da bir takım araç gereçlerle (ilk bilgisayarlar) yapma uğraşı içerisinde olmuştur.

Matematik hemen her disiplinde olduğu gibi bilgisayar biliminde ve dolayısıyla siber güvenlik alanında da en önemli unsur ve araçtır. Verimli, güçlü, sağlam ve dayanıklı siber güvenlik sistemlerinin geliştirilmesi, uygulamalarının yapılabilmesi için herşeyden önce, kurgulanacak sistemler en uygun matematiksel modele dayalı olmalıdır.

Problemler deneme yanılma yoluyla değil de matematiksel ifadesi kanıtlanmış kuramlar ile çözülmelidir. Bilgisayar biliminde;

- tamsayılar arasındaki ilişkiler;
- sayıların bellekte tutulma ve saklanma şekilleri,

- kümelere ait veriler üzerine çıkarımlar yapmak veya ilişkiler kurmak,
- çok karmaşık gibi görünen problemlerin graf teorisi ile modellenip çözülmesi,
- veritabanı sorgulamalarında optimum sorgulama ifadeleri yazılması,
- daha az büyüklüğü olması için verinin sıkıştırılıp geri elde edilmesi,
- problemlerin deneme yanılma yoluyla değil de matematiksel ifadesi kanıtlanmış kuramlar ile çözülmesi,
- verinin şifrelenip tekrar geri elde edilmesi,
- en temelde donanımsal ifadelerin elde edilmesi ve indirgenmesi,
- arama ve sıralama işlemlerinin optimum şekilde yapılması,
- geçmişte oluşma sıklığına bakılarak yeniden oluşma olasılığının öngörülmesi,
- sistemlerin davranışının modellenmesi,
- sayılar üzerinde matematiksel işlemlerin performanslı olarak yapılabilmesi,
- şekilsel yazılım modellemede sayılar ve özel simgelerle ilişkilerin gösterilmesi,

gibi birçok gereksinime ihtiyaç duyulur ve bilişim matematiği konuları bunların bilinçli bir şekilde yapılması için teorik ve pratik çözümler sağlar.

1.2. Siber Güvenlik için Matematiğin Önemi

Bilişim, toplum için var oluşunu farklı teknolojilerle gelişerek sürdürecek, matematiği tetikleyecek, matematik ise kuramsal gelişmesini sürdürerek bilişimi doğrudan veya dolaylı olarak etkileyecek ve yeni buluş ve gelişmelerin önünü açacaktır. Bu doğal etkileşim sürdükçe; toplumların gelişimi hızlanacak, daha rahat, üretken ve huzurlu bir yaşam sürdürülmesine, kişilerin kendilerini daha iyi tanımalarına, iş ve işlemleri daha hızlı ve kolaylıkla yapmalarına katkılar sağlayabileceklerdir.

Yarınlarda da bilişimin matematiği, matematiğin de bilişimi; güvenlik, nanoteknolojiler, e-ticaret, uzaktan hesaplama, yapay zekâ, blokzinciri, dijital ikiz, büyük veri, nesnelerin interneti, kriptografi, kuantum sonrası kriptografi, eğitim (e-öğrenme) veya daha yeni konularda etkileyeceğini öngörmek herhalde yanlış olmayacaktır.

Üniversitelerin bilişim alanındaki bölümleri (Bilgisayar Mühendisliği, Bilişim Sistemleri Mühendisliği, Yazılım Mühendisliği, Matematik, Kontrol Sistemleri Mühendisliği, Adli Bilişim Mühendisliği, Yönetim Bilişim Sistemleri ve Bilişim Teknolojileri, vb.) için hazırlanan program çıktılarına bakıldığında temelinde matematik olduğu görülecektir. Bunlar:

- Temel Matematik, Fen Bilimleri ve disipline yönelik matematik bilgilerine hâkim ve bu bilgileri mühendislik problemlerini modellemek için kullanma becerisine sahip olur.
- Alanla ilgili karmaşık problemleri tanımlama, modelleme ve çözme becerisine sahip olur ve bu amaçla uygun analiz yöntemlerini seçip uygulayabilir.
- Bilgisayar bilimleri uygulamalarını da içerecek şekilde ayrık matematik, olasılık ve istatistik, türev ve integral hesapları, çok değişkenli fonksiyonlar, lineer cebir, diferansiyel denklemler konularını içeren matematik bilgisine sahip olur.
- Bilgisayarların yapısını ve işleyişini çözümleyebilir, bilgisayar mimarisi, işletim sistemleri ve veritabanı sistemleri bilgilerine sahip olurlar.
- Karmaşık yazılım sistemlerinin, donanım ve yazılım içeren sistemlerin analizi ve tasarımı için gerekli bilgisayar bilimleri, algoritma ve veri yapıları, yazılım mühendisliği ve bilgisayar uygulamaları bilgilerine sahip olurlar.

Siber güvenlik alanındaki profesyoneller aynı zamanda bilişim profesyoneli de olacağından, siber güvenlik ile uğraşan profesyoneller öncelikle karşılaştığı yeni bir problemi uygun matematiksel ifade ve yazılım, donanım araçlarıyla modelleyebilmelidir. Dolayısıyla konuya özgü matematik ve modelleme oldukça önemlidir.

Bu açıdan bakıldığında bilgisayar bilimi matematiktir. Bu nedenle matematiğin konuları bilgisayar bilimlerinde birçok konuya alt yapı oluşturur. Sonuç olarak Siber Güvenlik Matematiği; bu alanda birçok problemin matematiksel çözümü ve modellenmesi için olmazsa olmazıdır [2].

Siber Güvenlik Matematiği genel olarak; Sayılar Teorisi, Sayı Dizileri, Küme Teorisi, Bağıntı, Fonksiyon, Lineer Cebir, Boole Cebiri, Kaos Teorisi, Algoritmalar, Algoritma Analizi, Matris Teorisi, Olasılık ve İstatistik, Polinom Zamanlı Problemler, Zaman Serileri, Graf Teorisi, Ağaçlar, Fark Denklemleri, Fourier Analizi, Morfolojik Analiz, İntegral ve Diferansiyel Hesap, Geometri, Koordinatlar (Kartezyen, Silindirik, Küresel ve Açısal), Vektörler, Dönüşümler ve Geometrik Dönüşümler gibi konuları kapsamaktadır [3]-[5].

1.3. Siber Savunmada Matematiksel Modelleme

Siber savunmada kullanılan matematiksel modelleme yaklaşımlarından bazıları aşağıda alt başlıklarda verilmiştir.

1.3.1. Matematiksel Modelleme

Bazen yüksek maliyet ve aşırı zaman ihtiyacı nedeniyle gerçek ortamda bir sistemin uygulanması mümkün olmayabilir. Bu durumda bir model oluşturup sistemin davranışını incelemek daha uygun olur. Modelleme gerçek bir sistemin yerine geçme ve bu sistemi basitleştirmedir. Buradan hareketle, Şekil 1.1'den de görülebileceği gibi birtakım farklı modeller vardır. Bu modellere göz atacak olursak;

I. Fiziksel Model: Mekanik, Elektrikli ya da Elektrik ve Hidrolik sistemlere dayalıdır.

II. Matematiksel Model: Matematiksel denklemlerle temsil edilen sistemlerdir.

III. Fiziksel-Statik Model: Zamana göre davranışları değişmeyen sistemlerdir.

IV. Fiziksel-Dinamik Model: Zamana göre davranışları değişen sistemlerdir.

V. Matematiksel-Statik Model: Sistem denge durumundayken bir matematiksel denklem veren modellerdir.

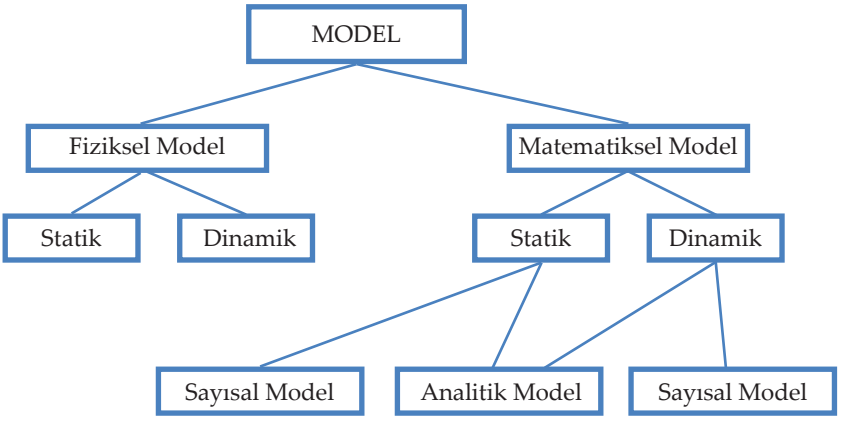
VI. Matematiksel-Dinamik Model: Bir zaman fonksiyonuna bağlı olarak sistem öz değerlerinin değişimine izin veren modellerdir.

VII. Matematiksel-Statik Sayısal Model: Simülasyon ile çözülebilen kompleks statik matematiksel modellerdir.

VII. Matematiksel-Statik Analitik Model: Temel matematik yöntemlerle çözülebilen küçük statik matematiksel modellerdir.

VIII. Matematiksel-Dinamik Analitik Model: Temel matematik yöntemlerle çözülebilen küçük dinamik matematiksel modellerdir.

IX. Matematiksel-Dinamik Sayısal Model: Simülasyon ile çözülebilen kompleks dinamik matematiksel modellerdir [6,7].

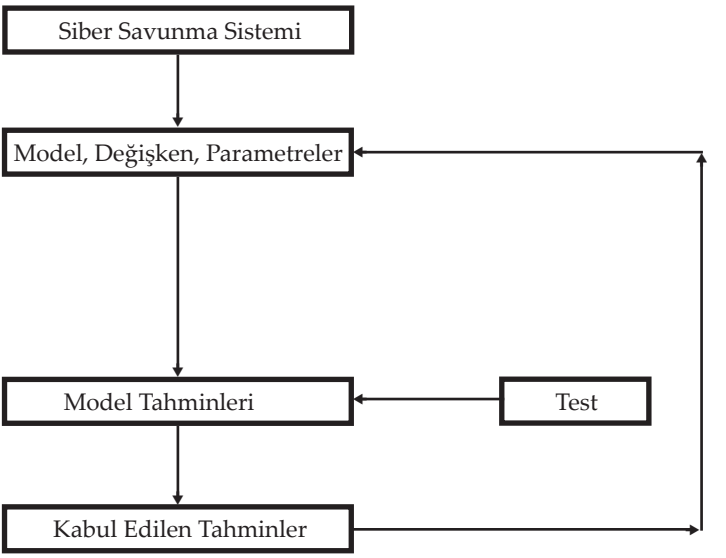


Şekil 1.1. Matematiksel Modeller

1.3.2. Siber Savunma Sistemi Modelleme Prensibi

Siber saldırılar, günümüz dünyasının en büyük problemidir. Bu sorunun üstesinden gelmek için kötü amaçlı nesnelerin, olayların ve girişimlerin davranışlarını anlamak şarttır. Matematiksel modellemede bu oldukça önemlidir. Virüs, Solucan, Truva Atı, Spam gibi kötü amaçlı nesneler ve anlık mesajlaşma, botlar, kimlik avı gibi belli teknolojilerin davranışları modelleme kullanılarak anlaşılır ve onlara karşı savunma sağlanabilir. Verilerin yaşam süresi, toplanma

zamanı, bağlantı sayısı gibi gerekli bazı varsayımların uygulanabileceği durumlar belirlenebilir. Kötü niyetli nesneler; yapılacak hesaplamalar ve bilginin durumunu temsil eden matematiksel denklemler yardımıyla tahmin edilmelidir. Güvenlik modelini uyarlanabilir hale getirmek için daha fazla alıştırma yapılabilmelidir [8]. Şekil 1.2'de bir örnek akış şeması verilmiştir.



Şekil 1.2. Matematiksel Modelleme Süreci

1.3.3. Kötü Niyetli Nesneler ve Savunma

Bilgisayar üzerindeki saldırılar tamamen stokastik olduğundan bir sonraki saldırının gerçek zamanı bilinemez. Ancak saldırının olasılığını modellemedeki olasılık kavramları sayesinde bulabiliriz.

x_i (i = 1,2,3, ...) stokastik değişkeni saldırı zamanını ifade etmek üzere, x_i 'nin ihtimali $P(x_i)$ ile ifade edilir.

n_i belli bir kaynaktan gelen saldırı sayısını ve N toplam saldırı sayısı olmak üzere

$$P(x_i) = \frac{n_i}{N} \text{ dir.} \tag{1.1}$$

Burada $P(x_i)$ sayı kümesi olarak düşünüldüğünde $\int_R P(x_i)dx_i = 1$ şartını sağlar, yani eğri altında kalan alan "1" dir. Bunu

$\sum^{\infty}_{i=1} P(x_i) = 1$ olarak ifade edebiliriz ki bu da olasılık yoğunluk fonksiyonudur. Verilen bir değere eşit veya küçük stokastik saldırıların ihtimalini veren bir olasılık dağılım fonksiyonu da bulunabilir.

$$F(x_i) = \sum_{xi \le i} P(x_i) \qquad (1.2)$$

Stokastik sistemin incelenmesi için, Ortalama, Mod, Medyan, Standart Sapma gibi olasılık fonksiyonlarının farklı ölçümleri kullanılabilir. Karakteristik denklem modelleri doğrusal ve doğrusal olmayan şeklinde olabilir. Doğrusal olmayan sistem kısmi diferansiyel denklemler ile ifade edilebilir.

Kötü amaçlı nesnenin; A, B, C, … gibi çeşitli diğer faktörlere bağlı *P* yayılma özelliğine sahip olduğunu kabul edelim. Bu durum $P = f(A, B, C, ...)$ ile gösterilebilir. Buradan ifadenin 1. ve 2. türevleri sırasıyla alınırsa ;

hız $\frac{\partial P}{\partial t} = \frac{\partial f(A,B,C, ...)}{\partial t}$, ivme $\frac{\partial^2 P}{\partial t^2} = \frac{\partial^2 f(A,B,C, ...)}{\partial^2}$ hesaplanır.

Aşağıda alt başlıklarda bahsedilmiş olan belirli yaklaşım tekniklerinin kullanılmasıyla elde edilen simüle edilmiş sonuçlar doğrulamanın yanısıra simülasyon ile üretilmiş verilerin tamamlanması içinde kullanılabilir.

1.3.3.1. Taylor Serisi Genişlemesi

Türevli herhangi bir fonksiyon, Taylor formülü ile genişletilebilir. $X = a$'nın yakınındaki bir bölgede, *x* bağımsız değişkenin değeri için $f(x)$ fonksiyonuna polinom yardımıyla yaklaşımda bulunulabilir.

$$f(x) = f(a) + f^1(a)(x - a) + \frac{f^{11}(a)}{2!}(x - a)^2 + ... + \frac{f^{(n)}(a)}{n!}(x - a)^n \qquad (1.3)$$

1.3.3.2. Sonlu Fark Yaklaşım Yöntemleri

Bu yöntem kısmi diferansiyel denklemleri küçük aralıklara böler. Bunu iki şekilde gerçekleştirir;

i. İleri Fark Yaklaşımı:

$f^1(x_i) = \frac{(f(n_{i+2}) - f(x_i))}{\Delta x}$ formülü ile çeşitli noktalarda fonksiyonun gradyanını hesaplar.

ii. Geriye Dönük Fark Yaklaşımı:

$f^1(x_i) = \frac{(f(x_i) - f(x_{i-1}))}{\Delta x}$ formülü ile çeşitli noktalarda fonksiyonun gradyanını hesaplar.

1.3.3.3. Yüksek Dereceden Türevler

Aşağıdaki formüle göre dağılımdaki çeşitli önemli noktaları ifade etmek için bu türevler kullanılabilir;

$$f^{(n)} = (f^{(n-1)})' \quad (1.4)$$

Polinom regresyon testleri gibi testler modelin doğrulanması için kullanılabilir. Böylece değerlerin bir polinom içerisine yerleştirilip yerleştirilemeyeceği tespit edilebilir. Karakteristik denklem elde edildikten sonra, sonuçlar mevcut standart matematik hipotezlere göre ampirik ya da analitik olarak doğrulanabilir. Matematiksel modelin doğrulanması için ilk olarak her terimin aynı ağ boyutuna sahip olmasını gerektiren boyutsal homojenliğinin irdelenmesidir. İkincisi ise modellerin nitelik ve limit davranışlarının kontrol edilerek doğrulanmasıdır. Bunların dışında, hataların ne kadar büyük olduğuna bağlı olarak doğruluk ve hassasiyet, verilerin Ortalama, Mod, Medyan ya da Standart Sapma ile hazırlanabilmesi gibi bazı hususlarda irdelenebilir. Bu veriler kolaylıkla karşılaştırılabilir ve kötücül nesnelerin davranışını anlamamız için bize yardımcı olabilir. Örneğin virüsün bazı tanımları aşağıdaki gibi modellenebilir;

i) Mevcut dosyaları etkileyen ve aynı şekilde davranmalarını sağlayan basit bir virüs v, programların bir kümesi P, $v \in P$ *ve* $p_i \in P$ olsun ve $f(v)$ *ve* $f(p_i)$ sırasıyla v virüsünün ve p_i programının davranışları olmak üzere;

$f(v) = f(p_i)$ dir.

ii) Virüsün sabit bir t anındaki tanımı

$T(v, p_i, e, t, S) = \log\left(\frac{f(v,e,t,S)}{f(p_i,e,t,S)}\right)$ dir.

Burada $f(v, e, t, S)$ ve $f(p_i, e, t, S)$ e olayının meydana geldiği S sistemindeki t zamanında sırasıyla v *ve* p_i programlarının davranışını verir.

Şimdi eğer $T(v, p_i, e, t, S) = 0$ ise o zaman v programı bir virüstür aksi takdirde değildir.

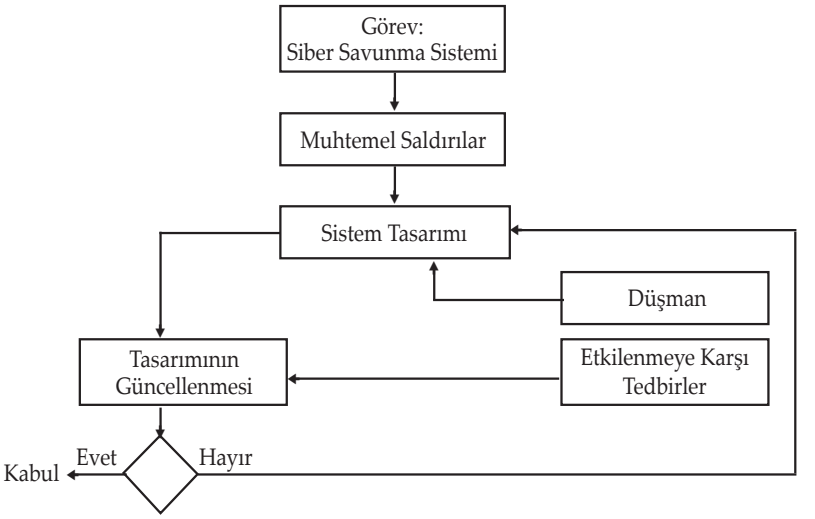
iii) Virüsün sürekli bir zaman aralığı olan Δt ye bağlı olarak tanımı

$$T(v, p_i, e, t, S) = \log\left(\frac{\int_{\tau_o}^{\tau_1} f(v,e,t,S)dt}{\int_{\tau_o}^{\tau_1} f(p_i,e,t,S)dt}\right) \text{ dır.}$$

Burada $\int_{\tau_o}^{\tau_1} f(v, e, t, S)dt$ ve $\int_{\tau_o}^{\tau_1} f(p_i, e, t, S)dt$ fonksiyonları sırasıyla v *ve* p_i programlarının e olayının meydana gelişindeki S sisteminde

$\Delta t = \tau_1 - \tau_o$ zaman aralığındaki davranışını verir. Eğer $T(v, p_i, e, t, S) = 0$ ise o zaman v programı bir virüstür aksi takdirde değildir.

Şimdi bir siber savunma sistemini modellemek için ihtiyaç duyulan sensörler ve kötüye kullanım, durum farkındalığı, savunma mekanizması, komuta ve kontrol, stratejiler ve taktikler ile bilim ve mühendislik gibi farklı bileşenleri birlikte kullanmak gerekir [9,10]. Bu bileşenlerin kullanıldığı bir siber savunma sistemi tasarım modeli Şekil 1.3'te verilmiştir.



Şekil 1.3. Siber Savunma Sistemi Tasarım Modeli

1.3.4. Değerlendirmeler

Her ne kadar çeşitli modeller ve çözümler ortaya konulsa da halen bazı problemler çözüm beklemektedir. Bu problemler başlıca şunlardır:

1. Kötücül nesnelerin tüm özellikleri, gelecekteki davranışlarını öngörmek için, matematiksel denklemler şeklinde temsil edilmelidir. Ayrıca, mevcut ortamda bu karakteristik denklemleri uygulamak için gerçekçi bir model oluşturulmalıdır.
2. Bir modelin doğruluğu simüle edilmiş sonuçlara dayalı olarak analiz edilip geliştirildikten sonra sağlanabilir. Sağlanan bu doğrulama, kötücül nesnelerin saldırısına karşı sistemi korumada

yardımcı olur. Kırmızı kod gibi solucanlar yüksek doğrulamayla modellenmiştir ve şuan kolayca kontrol edilebilirdir. Modellerin çoğu belirli doğrulama sınırlarına sahip olmalarına rağmen hala geliştirilmeleri mümkündür [11].

3. Belirlenmesi gereken oldukça fazla özelliğe sahip kötücül nesnelerin çoğunun davranışlarındaki karmaşıklıklarında artış vardır. Bu nedenle her bir özellik genelleştirilmeli ve özellik alanı daraltılmalıdır [12].
4. Siber savunma sistemlerinin çoğu, uygulandığında mevcut sistemi yavaşlatan paket uzunluğu, veri uzunluğunu artırma ya da karşılaştırma için daha fazla harcama gibi sabit giderler meydana gelir. Bu nedenle, daha fazla sabit gider oluşturmayan böyle bir siber savunma sistemi temin etmek veya kurgulamak gereklidir. Hem saldırı öncesi hem de saldırı sonrası için kurtarma sağlayan savunma sistemleri, matematiksel modellemeye dayalı yüksek doğrulamalı ve yeterince öngörülebilir olmalıdır.
5. Siber savunmada düşük farkındalık nedeniyle saldırganın izini sürmek zordur. Bu nedenle bu tür kötücül faaliyetleri sınırlamak için uygun bir politika ve farkındalık geliştirmelidir.

1.4. Sosyal Medya

Sosyal medya giderek daha yoğun bir dezenformasyon alanı haline geliyor. Hatta karma (hibrit) savaşın bir parçası olarak kullanıldığını da söyleyebiliriz. Askeri operasyonları desteklemek için bile sosyal medya kullanılabilir. Şöyleki Thomas Elkjer Nissen bu amaç için sosyal medyayı kullanmanın yollarını şu şekilde özetliyor:

1. İstihbarat toplama
2. Hedefleme
3. Bilgilendirme ve etki (psikolojik savaş)
4. Siber işlemler ve
5. Savunma ve komuta kontrol işlemidir.

Sosyal medya, bilginin tasnifi ve analizi noktasında önemli bir pozisyonda iken, eyleme dönüştürücü gücünün daha temkinli analiz edilmesi en önemli adımlardan biridir. Son yıllarda sosyal medya

kullanımının ve kullanıcısının artışı bu alanı da iyi analiz etmemizi gerektirmektedir. Sosyal medyayı analiz ederken karşımıza siber istihbarat faaliyetleri çıkmaktadır. Siber güvenlik alanı, çağımızın en önemli konularından birisidir. Siber tehdit istihbarat faaliyetleri ise siber güvenlik alanının önemli bir parçası haline gelmiştir. Siber tehdit istihbarat faaliyetleri içinde de sosyal medya istihbaratı, bilgi toplayıcı, analiz edici ve sonuçta önleyici en önemli siber güvenlik unsurlarından biri olma yolundadır. Günümüzde bu konuda da çalışmalar yapılmakta ise de ülkemizde çoğunlukla insan gücüyle yapılan işlemlerden yararlanılmaktadır. İşte bu tür istihbarat faaliyetlerini otomatikleştiren verimli algoritmaların tanımlanması, siber güvenlik alanında büyük imkânlar sunabilecektir. Bu algoritmalar, olayların tespitinde ve analizinde pek çok fayda sağlayacaktır. Bu amaçla kullanılan pek çok yazılım, program ve platform vardır ki bunların temelini de istatistik yöntemler ve olasılık teorisi ile birlikte polinom zamanlı problem çözebilen algoritmalar oluşturmaktadır.

1.5. Örnekler

Bu bölümde konunun önemini daha iyi anlatmak ve anlaşılmasını kolaylaştırmak için bazı örnekler verilmiştir.

1. Sosyal ağ analizinde en çok kullanılan kavramlardan birisi merkeziliktir. En sık kullanılan merkezilik çeşitleri ise yakınlık merkeziliği (closeness centrality) ve arasındalık merkeziliği (betweenness centrality)'dir. Yakınlık merkeziliği bir birimin diğer birimlere grafikteki uzaklığının toplamıdır.

$$c(i) = \sum_{i} d_{ij} \tag{1.5}$$

Arasındalık merkeziliği ise bir birimin ağda diğer birimler arasında bulunma derecesidir. Bir birimin yüksek derece arasındalığı varsa, köprü görevindedir.

Maksimum yakınlık merkeziliği ve maksimum arasındalık merkeziliği oranlarına bakılarak, elde edilen verilerin birbiriyle bağlantılı olup olmadıkları

$$b(i) = \sum_{j,\,k} \frac{g_{jik}}{g_{jk}} \tag{1.6}$$

formülünden anlaşılabilir [13].

2. Sosyal medya verileri üzerine yapılan bir araştırmada sosyal medyada harcanan zaman, sosyal medyada kullanılan araçlar ve farkındalık düzeyinin yatkınlık düzeyi üzerine etkisi belirlenmek istensin. Bu tür bir incelemede en sık kullanılan yöntem olan regresyon analizi;

Y : Yatkınlık düzeyi (bağımlı değişken)

X_1: Farkındalık düzeyi (bağımsız değişken)

X_2: Sosyal medyada harcanan zaman (bağımsız değişken)

X_3 : Kullanılan sosyal medya araçları (bağımsız değişken)

olmak üzere matematiksel olarak şu şekilde formüle edilebilir:

$$Y = a + b_1 X_1 + b_2 X_2 + b_3 X_3 + b_4 X_4 + \ldots + b_k X_k \qquad (1.7)$$

Bu matematiksel modelle aşağıdaki hipotezlerin doğru olup olmadıkları ve buna göre aralarındaki ilişkiler belirlenir:

H_1: Kullanılan sosyal medya verilerinin yatkınlık düzeyi üzerinde istatistiksel olarak anlamlı bir etkisi vardır.

H_2: Farkındalık düzeyinin yatkınlık düzeyi üzerinde istatistiksel olarak anlamlı bir etkisi vardır.

H_3: Sosyal medyada harcanan zamanın yatkınlık düzeyi üzerinde istatistiksel olarak anlamlı bir etkisi vardır [14].

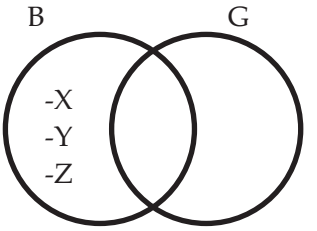
3. Bilgi Toplama

Sızma testlerinin en önemli aşaması olan bilgi toplama safhası için https://youtu.be/oYf0mT5umOo linkinden ulaşabilecek bir dakikalık videoda bahsedilen kişinin; boyunu, gölge uzunluğunu, resmin çekildiği saati bilmek şartıyla konumunu hesaplama olarak özetleyebileceğimiz Küresel Trigonometrinin bir uygulaması örnek olarak verilebilir [19].

4. Filtreleme

Bir güvenlik duvarında IP bloklaması işleminde karaliste mantığı kullanılır. Yani gelen istek kontrol mekanizmasına gönderilir ve pakete ait IP adresi listede bulunuyorsa geçişe izin verilmez. Bu işlemlerin matematiksel gösterimi aşağıdaki gibidir. f(x) fonksiyonuna göre sonuç 1 ise geçişe izin verilir, değilse verilmez [19].

B: Karaliste
G: Gelen istekler



$$f(x) = \begin{cases} s(B \cap G) = 0 \text{ , } 1 \\ s(B \cap G) > 0 \text{ , } 0 \end{cases} \quad (1.8)$$

5. Ölçekleme

Sistemin korunabilmesi için öncelikle ölçeklenebilmesi gerekir. Bir web sunucusuna ait iş yükünün teorik olarak hesaplanmasını örnek verecek olursak;

Bir web sunucusuna gelen istekler arasında geçen ortalama zaman 100 ms'dir. Sunucuya 1 saniye içerisinde ortalama kaç adet istek gelir?

X, sunucuya gelen istekler arasında geçen zamanı gösteren rastgele değişken olsun (Üstel bir rastgele değişken), $E[X] = 1 / \lambda = 100$ ms => $\lambda = 1/100$ (istek/ms).

Y, sunucuya 1ms. içinde gelen istek sayısını ifade eden rastgele değişken olsun. (Poisson rastgele değişken) $E[Y] = \lambda = 0{,}01$ istek/ms.

1 ms içerisinde ortalama 0,01 istek geliyorsa 1000 ms içerisinde ortalama 10 istek gelir [19].

6. Hata Olasılığı

10^9 bit/s hızla çalışan bir bilgisayar ağı üzerinden ikili sayıların iletilmesinde hata olasılığı 10^{-8} olarak verilmiştir. Buna göre 1 saniyede 5 veya daha fazla hata olma olasılığını bulalım;

$$\lambda = np = 10^9\ 10^{-8} = 10\ bit/s \quad (1.9)$$

N: 1 saniyede yapılan hata sayısı

$$P(N \geq 5) = 1 - P(n < 5) = 1 - \sum_{i=0}^{4} (e^{-10}) \frac{10^i}{i!} = 0{,}9707 \quad (1.10)$$

olarak hesaplanır [19].

7. Sosyal Mühendislik Saldırısı

Markov modeli kullanılarak başkasının adına bir yazı üretmek mümkündür. Markov modeli kısaca düğümlerin birbiri arasındaki geçişin istatistiksel olarak modellenmesidir. Eğer bir Twitter kullanıcısının tweetleri markov modeline verilirse o kullanıcının kullandığı kelimelerden yeni bir tweet üretmek mümkündür [19].

8. Oyun Teorisi

Oyun teorisi ile kurumun kriz durumunda en iyi kararı almasına katkı sağlanabilir. A ve B gibi iki banka düşünelim.

A bankası fidye yazılımı tehditlerine karşı bir önlem geliştirmiştir ve sistemleri bu zararlıdan etkilenmemektedir. Banka geliştirdiği yöntemi B bankasına belli bir ücretle satmak istemektedir. Bu durumda B bankasının geliştirilen yönteme ait bilgiyi alması gerekli midir?

Bilginin maliyeti : X

Bilginin yokluğunda oluşacak maliyet: Y

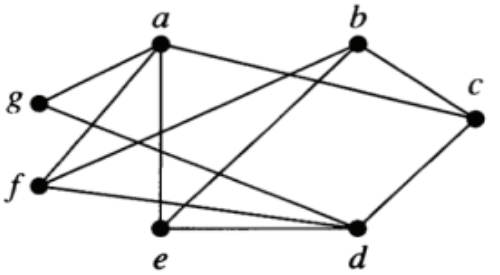
Bilginin değeri: Z olsun.

Eğer banka bilgiyi satın alırsa (Z – X) kadar kazanç elde etmiş olur,

Bilgiyi satın alıp herhangi bir önlem almazsa (X+Y) kadar zarar etmiş olur. Banka bu şekilde tüm ihtimalleri değerlendirdikten sonra en uygun kararı vermesi için elindeki sayısal verilerden faydalanabilir [20].

9. Ağ Trafik Analizi

Ağ trafiğinin analizinin kolaylaştırılması için ağ akışını modellemek istediğimizde graf teorisini kullanırız [19].



10. Kriptografi

Bu kitap serisinde kriptografi matematiği anlatıldığı için burada detaylara girilmemiştir.

Ancak kriptografide özellikle sayı teorisi, modüler aritmatik, fonksiyon, hash fonksiyonları, matris teorisi gibi konuların önemli bir yere sahip olduğunu hatırlatmakta fayda vardır.

Siber güvenlik alanında daha detaylı olarak matematiksel modelleme örnekleri için; bu bölüm hazırlanırken sıkça başvurulan "Siber Güvenlik Risk Analizi, Tehdit ve Hazırlık Seviyeleri", "Siber Terör Saldırılarından Korunmaya Yönelik Bulanık Mantık Tabanlı Karar Destek Modeli", "Milli Güç Unsurlarının Belirlenmesinde Siber Uzay Faktörü" ve "Çok Nitelikli Fayda Teorisiyle Saldırgan Profiline Yeni Parametrelerin Eklenmesi" gibi çalışmalar detaylı olarak incelenebilir [15]-[18].

1.6. Kuantum Kriptoloji

Siber güvenlik alanının en önemli ayaklarından biride kriptoloji bilimidir. Kriptolojinin şifreleme kısmı, günümüzde özellikle siber savaşların olduğu bir ortamda oldukça önem kazanmış durumdadır. Şifrelemenin daha güvenli yapılabilmesi için günümüzde kuantum şifreleme çalışmaları öne çıkmaktadır.

Kriptoloji bilimi, matematiğin alt dalı olup; matematiksel tekniklerden faydalanıp şifreleme sistemlerini kullanarak bilgiyi gizleme sanatı ve bilimi olarak bilinen kriptografi ile zeki, güçlü ve kötü niyetli gibi davranıp benzer matematiksel teknikleri, eldeki tüm hesapla-

ma gücünü ve tasarımlardaki zayıflıkları da kullanarak geliştirilmiş mevcut bilgi güvenliği sistemlerini alt etme olarak tanımlanan kriptonalizden oluşur.

Modern kripto sistemlerde en ciddi sorun anahtar dağıtım problemi olarak bilinen gizli anahtarın güvenliğidir. Bu nedenle anahtar dağıtım sorunlarının ve risklerinin olmadığı bir kripto sisteme ihtiyaç vardır. Bu da teknolojik gelişmelerden etkilenmeyen ve uzun vadeli, kalıcı gizlilik sağlayan yeni bir alan olan kuantum kriptografidir.

Kuantum kriptografi, siber alandaki güvenliğin kuantum mekaniğine ait belirsizlik ilkesi, foton polarizasyonu, dolaşıklık gibi yasalar ile garanti edildiği kriptografi tekniğidir. Asıl avantajı, kanıtlanmış evrensel kuantum mekaniği yasalarına dayanıyor olması, bunların klasik olarak eşdeğerinin bulunmaması ve güvenliğin ispatlanabilir olmasıdır.

Kriptonaliz; kriptografinin aksine şifreleri çözme ve şifreli bilgileri okuma sanatı ve bilimidir. Gizli anahtarı bir şekilde ele geçirerek ya da geçirmeden şifreli bilgiyi çözme işlemlerini kapsar. Kriptonaliz gizli anahtarı elde etmenin en zor yoludur. Çünkü aynı işi sistemdeki zayıflıklara odaklanarak daha kolay yapabiliriz.

Kuantum kriptonaliz ise; bazı kuantum mekaniksel sistemlerden, bir takım kuantum mekaniksel etkilerden yararlanarak yani kısacası kuantum bilgisayarlar kullanarak şifre kırmayla ilgilenen kriptografik bir uygulama alanıdır.

Kuantum kriptonalize en meşhur örnek; bir matematikçi olan Peter Shor tarafından 1994 yılında önerilen, çarpanlara ayırma problemini çözmenin verimli bir yolunu ortaya koyan, shor algoritmasıdır. Bu algoritma bir kuantum bilgisayar ile çok büyük tam sayıları kolaylıkla çarpanlarına ayırabilecektir. Böylece bazı simetrik şifreleme algoritmaları kırılmış olacaktır.

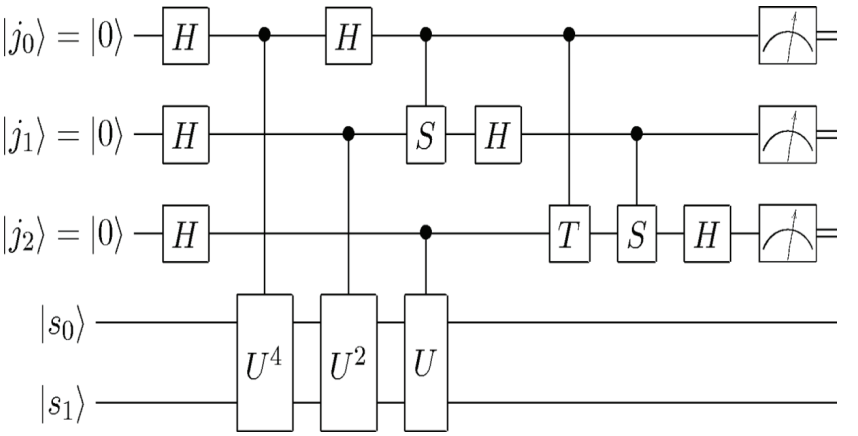
Bir başka örnek ise, bir bilgisayar bilimcisi Lov Grover tarafından önerilen, kuantum bilgisayar yardımıyla, kaba kuvvet saldırısı marifetiyle anahtar aramalarının karesel olarak daha hızlı yapılabileceğini belirten Grover algoritmasıdır.

Kuantum özel kanallar, kuantum simetrik şifreleme, kuantum hesaplama gibi kuantum kriptonalizde kapsamlı bir kuantum bilgisayarın yapılmasını beklemektedir [21, 22, 24].

1.7. Kuantum Bilgisayar ve Algoritmalar

Veri işleme bilgisine yeni bir yaklaşım getiren inanılmaz derecede güçlü makinelerdir. Bilgi üzerinde bir takım işlemleri gerçekleştirmek için süperpozisyon ve dolaşıklık gibi kuantum fiziğinin prensiplerini kullanan paralel bir hesaplama makinesidir. Kuantum bilgisayarlarda kuantum bilginin birimi olarak kubit kullanılır. Bir kuantum sistem klasik bitleri kuantum bitler ile değiştirir. Klasik bitler 0 ve 1 değerini alırken kubitler aynı anda hem 0 hem de 1 değerini alabilen yani aynı anda tüm olasılıklara sahip olan süperpozisyon ve iki kubitin birbiriyle ilişkili olması nedeniyle birindeki bir değişikliğin diğerini de etkilediği dolaşıklık olaylarını kullanır. Bu ise kuantum hesaplamanın gücünün temel unsurudur ki; kubitleri kullanan bilgisayarların daha az enerji kullanarak daha fazla bilgi depolayabileceği demektir. Kubitler bu şekilde elektron spinine veri kaydedebildiklerinden kuantum bilgisayarların temel veri birimi bit değil kubit ile ifade edilmiştir [20].

Bir kuantum bilgisayar hem giriş hem de çıkış kubitlerinin lineer kombinasyonundaki tüm temel durumları üzerinde aynı anda çalışabilir. Yani problemlere aynı anda odaklanır, tüm muhtemel çözümleri bir kerede ele alır ve çalışmayanları atar. Aslında, kuantum bilgisayar bir paralel makinedir. Şöyle ki n kubitlik bir kuantum bilgisayarın işlem gücü n bitlik 2^n tane klasik bilgisayara eşittir diyebiliriz. Bu durumda kuantum bilgisayar dendiğinde kuramsal alandaki bir insan olarak ilk aklıma gelen şey kuantum devreleridir. Çünkü kuantum bilgisayımının klasikten farkı kullanılan devre modelidir ve esas olan devredir. Zira bu teknoloji harikası ve milyon dolar maliyetli ürünler kuantum devre şemasının fiziksel olarak gerçekleştirilmesidir. Şekil 1.4'de bir kuantum devre modeli görülmektedir.



Şekil 1.4. Kuantum devre modeli [23].

Bir klasik bilgisayar x girişi alır ve f(x) çıkışını üretir. Ancak bir kuantum bilgisayar, giriş olarak tüm mümkün ve muhtemel x durumlarının bir toplamını alabilir;

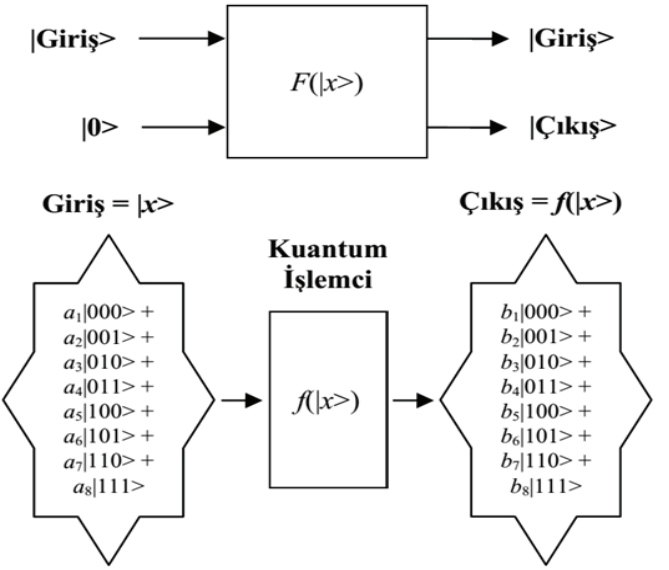
$$\frac{1}{c}\sum_{k=o}^{n}|x_k> = \frac{1}{c}(|x_o> + |x_1> + |x_2> + ... + |x_n>) \quad (1.11)$$

Burada c sabiti normalleştirme için kullanılır. Ürettiği çıkış ise;

$$\frac{1}{c}\sum_{k=o}^{n}|x_k, f(x_k)> = \frac{1}{c}(|x_o, f(x_o)> + |x_1, f(x_k)> + |x_2, f(x_2)> + ... + |x_n, f(x_n)>) \quad (1.12)$$

olabilir.

Burada eğer bir ölçüm yapacak olursak yani rastgele seçeceğimiz bir x_o değeri için $|x_2, f(x_2)>$ sonucunu elde edeceğimizden dolayı çıkıştaki tüm diğer durumlar yok edilecektir. Buda f(x) değerlerine bakmak için tek bir şansımızın olduğu anlamına gelir. Bu nedenle bir kuantum bilgisayarı programlarken temel hedef hesaplamayı tasarlama olacaktır. Yani bir kuantum bilgisayarla çarpanlara ayırma polinomsal zamanda yapılarak görmek istediğimiz çıkışlar diğerlerinden daha büyük bir ihtimalle görünür (Shor Algoritması). Şekil 1.5'te bir kuantum bilgisayarın çalışma prensibi görülmektedir.



Şekil 1.5. Bir kuantum bilgisayarın çalışma prensibi [24].

Donanım uzmanları kullanılabilir ilk kuantum bilgisayarı geliştirirken bilgisayar bilimciler ve matematikçiler de doğal olarak boş durmuyor ve 1990'lı yılların başından itibaren kuantum bilgisayarlarda uygulanabilecek ilk algoritmaları geliştirmeye çalışıyorlar. Bilgilerin bitler yerine kubitlerde saklandığı ve kuantum mekaniğinin geçerli olduğu bu ortamda kuantum algoritmaları, kuantum bitlerinin süperpozisyon özelliğini kullanarak işlem yapmaktadırlar [24]. 1980'li yılların ortalarından günümüze kadar geliştirilmiş sadece bir kaç kuantum algoritması mevcuttur. Bunlardan en çok bilinenleri ise Deutsch, Shor ve Grover algoritmalarıdır. Bu algoritmalar aşağıda kısaca açıklanmıştır.

1.7.1. Deutsch Algoritması

1985'te David Deutsch tarafından geliştirilen Deutsch algoritması bilim tarihindeki ilk kuantum algoritmasıdır. Sadece tek bir kubit üzerinde işlem yapabilen Deutsch algoritması, günümüzde de klasik algoritmaların sınırlarına dayandığı yerde kuantum algoritmalarının olağanüstü bir işlem hızıyla sonuca ulaşabildiğini kanıtlaması açısından oldukça önemlidir. 1992'de yine David Deutsch ve Richard Josza tarafından genelleştirilerek sınırsız sayıda (n tane)

kubit üzerinde işlem yapabilecek şekilde tekrar formüle edilen ve Deutsch-Jozsa algoritması adını alan Deutsch algoritması, daha sonraki yıllarda geliştirilen Shor ve Grover algoritmaları için gerçek bir ilham kaynağı olmuştur.

1.7.2. Shor Algoritması

Günümüzde laboratuvarlarda sadece bilimsel amaçlı deneyler için geliştirilen kuantum bilgisayarların test edilmesi için özellikle iki kuantum algoritması ön plana çıkmaktadır ki bunlar; Shor algoritması ve Grover algoritmasıdır. 1994'te Amerikalı matematikçi Peter W. Shor tarafından geliştirilen bu algoritma kuantum bilgisayarlarda çok büyük sayıları kolaylıkla çarpanlarına ayırabilmektedir. Belirli bir olasılık dâhilinde periyod bulma özelliği ile Shor algoritması kriptoloji açısından çok büyük önem ifade etmektedir, çünkü günümüzdeki şifreleme mekanizmaları çok büyük sayıların klasik bilgisayarlar tarafından kabul edilir bir zaman dilimi içerisinde çarpanlarına ayrılmasının mümkün olmadığı varsayımına dayanmaktadır. Oysa laboratuvar ortamları için geliştirilmiş ve çok az sayıda kubite sahip kuantum bilgisayarlarının bile en büyük sayıları, çok çok kısa sürede çarpanlarına ayırabilmesi bugüne kadar bildiğimiz klasik kriptoloji biliminin temellerini şimdiden sarsarak kuantum kriptoloji adlı yeni bir bilim dalının yolunu açmıştır. Shor algoritması klasik ve kuantum olmak üzere iki kısımdan oluşur;

-Klasik Kısım

Çarpanlara ayırma problemi bir mertebe / periyot bulma problemine indirgenir. N'in asal çarpanları için algoritma şu şekildedir;

1. Rastgele bir $\propto < N$ sayısı üretilir.
2. *OBEB* $(\propto, N)$'i hesaplar. Eğer *OBEB* $(\propto, N) \neq 1$ ise $\propto$, N 'in bir asal çarpanıdır, işlem tamam.
3. $N^2 \leq Q = 2_m \leq 2N^2$ olan bir Q belirler ve $f(x) = \propto^x mod\ N$ fonksiyonunun r periyodunun bulunması için kuantum kısma geçer.
4. Eğer r tek ise 1. adıma döner.
5. Eğer $\propto^{r/2} \equiv -1\ (Mod\ N)$ ise 1. adıma döner.
6. *OBEB* $\left(\propto^{r/2} \pm 1, N\right) = N$ 'in asal çarpanı ise işlem tamam.

-Kuantum Kısım

Mertebe bulma problemini çözmek üzere bir kuantum algoritma içerir. Başka bir ifadeyle; kuantum mekaniği kullanılarak mertebe/ periyot bulma işlemi yerine getirilir.

1. Saklayıcılar ilklendirilir;
$Q^{-\frac{1}{2}} \sum_{x=0}^{Q-1} |x, o>$, m kubitlik giriş, $\frac{m}{2}$ kubitlik çıkış.

2. f(x), kuantum bir fonksiyon olarak gerçeklenip yukarıdaki kuantum duruma uygulanır.

$Q^{-\frac{1}{2}} \sum_x |x, f(x)>$. Tüm olası $Q = 2^m$ durumun bir süperpozisyonudur. Dolayısıyla tüm olası girişler ve çıkışlar saklayıcılardadır.

3. İkinci yarıda ölçüm yapılır;
$\frac{1}{c} \sum_{o \le x \le 2^m} |x, f(x)>$. Burada c, toplamdaki terimlerin sayısının karekökü dür. Yani vektör uzunluğunu 1 yapmak için gereken faktördür.

Bu ölçüm, bir u (mod N) sayısı verir ve tüm sistemi $|x, u>$ formundaki durumların bir lineer kombinasyonuna zorlar ki; tüm $a^x \equiv u \ (mod\ N)$ durumları elde edilir.

4. Giriş saklayıcısına kuantum fourier dönüşümü uygulanır;
$U_{QFT} |x> = Q^{-\frac{1}{2}} \sum_y W^{xy} |y>$, burada $W = e^{\frac{2\pi}{Q}}, O \le y < Q.$
Kuantum fourier dönüşümü periyodu bulmak için gerekli olan frekansları ölçer. Eğer r 2^m in bir böleni ise elde edilen frekanslar f_o temel frekansının katlarıdır ve $rf_o = 2^m$ olur. Ancak genelde r, 2^m in böleni değildir. Bu durumda ise; bazı baskın frekanslar olacaktır ve bunlar bir f_o temel frekansının yaklaşık katları olur. Yani $rf_o \approx 2^m$ dir. Kuantum fourier dönüşümü sonucu olan kuantum durum üzerinde ölçüm yapılır ve bir $f = j.f_o$ frekansı belirlenir.

5. r 'yi elde etmek için *frekans* = $\frac{Uzunluk}{Periyot}$ tanımı kullanılarak dizinin kaç defa tekrar ettiğini hesaplayan $\frac{f}{r.f_o} \approx \frac{j.f_o}{2^m} \Rightarrow \frac{j}{r} \approx \frac{f}{2^m}$ ilişkisi üzerinde sürekli bölme açılımı uygulanır. Çünkü uzunluğu belli olan bir dizinin frekansı bulunursa periyodu da bulunur.

Euler'in Ø fonksiyonu, p,q asal ve N = p.q olmak üzere; Ø(N) = (p-1)(q-1) alınarak $r \le Ø(N) < N$ eşitsizliğinden r periyodu

bulunur. Genel olarak, yukarıdaki bölme açılımından N'den küçük en son payda aranılan r periyodudur.

6. $a^r \equiv 1 \pmod{N}$ ise işlem tamamlanır.

7. $a^r \not\equiv 1 \pmod{N}$ ise 1.adıma geri dönülür.

Bu algoritmanın kuantum kısmı için her bir N ve a ya bağlı olan özel olarak kuantum devreler tasarlanır. Yöntem bazen düzgün çalışmayabilir, bu durumda algoritma yeniden tasarlanır ve baştan çalıştırılır.

1.7.3. Grover Algoritması

1996'da Hint asıllı Amerikalı bilgisayar bilimci Lov Grover tarafından geliştirilen Grover algoritması (GSA) çok büyük veri tabanlarında aranan bir bilginin, gerekli sorgulamanın çok detaylı bir şekilde formüle edilmesine gerek kalmadan fakat yine de hızlı bir şekilde bulunmasını sağlar. GSA da diğer birçok kuantum algoritması gibi olasılık kuramı tabanlı çalışan bir algoritma olduğundan doğru cevabı bulabilmesi için veriler üzerinde çoğu zaman sadece bir kez değil, birçok defa çalıştırılması gerekmektedir. Bu şekilde aynı verileri birçok defa işleyen algoritma, en sonunda doğru olma olasılığı en yüksek cevabı bulur.

1. İlklendirme: Walsh-Hadamard dönüşümü uygulanarak aşağıdaki süperpozisyon elde edilir;

$$|\delta> = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x> \tag{1.13}$$

2. Yineleme: Aşağıdaki tüm işlemler M defa tekrar edilir;

a) Mevcut süperpozisyondaki her bir $|x>$ durumu için $F(x) = 1$ ise faz π radyanlık döndürülür, aksi takdirde sistem değişmemiştir durdurulur.

b) Walsh-Hadamard dönüşümü ve Faz rotasyon matrisinden oluşan

$$D_{ij} = \begin{cases} \frac{2}{N}, & i \neq j \\ -1 + \frac{2}{N}, & i = j \end{cases} \tag{1.14}$$

dönüşümü uygulanır.

3. Ölçüm: Ortaya çıkan süperpozisyon ölçülür ve genliklerin belirlediği olasılıklara göre bir durum elde edilir [20-22].

1.8. Değerlendirmeler

Siber güvenlik matematiğinin konularını bilmek bu alanda faaliyet gösteren profesyonellere ciddi katkılar sağlar. Bazı konulardaki problemler matematiğin bu konularını bilmeden çözüldüğünde reel çözümden uzak olmakla beraber fazla döngülerle zaman kaybı oluşturacak, sonuçların güvenilirliğini sorgulatacak, zaman ve maddi kayıplara sebebiyet verebilecektir. Siber Güvenlik Matematiği özellikle milli siber güvenlik çözümlemelerinde gerekli bir konudur. Siber güvenlik alanında karşılaşılan problemleri modellemenin ve onlara ait çözümleri milli düzeyde algoritmik olarak tasarlayabilmenin yolu kesinlikle siber güvenlik matematiğine hâkimiyetten geçmektedir. Öncelikle çözüm için en uygun model belirlenmeli daha sonra alt bileşenler ortaya konularak problem önce matematiksel olarak çözülmelidir.

Siber güvenlik matematiğine yeterince hâkim olmak hem verimliliğe hem de bilişim projelerinin kalitesine olumlu yansıyacaktır. Ayrıca Milli Siber Güvenlik çözümleri konusunda da pozitif yansımaları olacaktır.

Kaynaklar

[1] 2016-2019 Ulusal Siber Güvenlik Strateji ve Eylem Planı Belgesi.

[2] T.R. Çölkesen, Bilişim Matematiği, Uygulamalı Ayrık Matematik, Papatya Yayınları, 2015.

[3] J.S. Milne, Field and Galois theory, Lecturer Notes, 2015.

[4] L. Gilbert and J. Gilbert, Elements of Modern Algebra, McGraw-Hill Education, 2011.

[5] H. Kenneth, Discrete Mathematics and Its Application, McGraw-Hill Education, 1999.

[6] D.K. Saini, "A Mathematical Model for the Effect of Malicious Object on Computer Network Immune System," Applied Mathematical Modeling, vol. 35, pp. 3777-3787 USA, doi:10.1016/.2011.02.025, 2011.

[7] D.K. Saini and B. K. Mishra, "Design Patterns and their effect on Software Quality," ACCST Research Journal, vol. 5, no. 1, pp. 356-365 India, 2007.

[8] D.K. Saini and N. Gupta, "Fault Detection Effectiveness in GUI Components of Java Environment through Smoke Test," Journal of Information Technology, ISSN 0973-2896 vol. 3, no. 3, pp. 7-17 2007.

[9] D.K. Saini and H. Saini, "VAIN: A Stochastic Model for Dynamics of Malicious Objects," the ICFAI Journal of Systems Management, vol. 6, no. 1, pp. 14- 28, 2008.

[10] D.K. Saini, Cyber Defense: Mathematical Modelling and Simulation, International Journal of Applied Physics and Mathematics, Vol. 2, No. 5, September 2012.

[11] A.O. Kalashinkov, Example of using game-theoretic approach in problems, Cybersecurity Issues, No.1(2),49-54,2014.

[12] O.I. Stasuk and L.L. Goncharova, Differantial mathematical models to investigate the computer network architecture of an all-mode Systems of control over a distance of railways, Cybernetics and systems Analysis, vol.53, No.1, 157-164,2017.

[13] S. Savaş ve N. Topaloğlu, Sosyal Medya Verileri Üzerinden Siber İstihbarat Faaliyetleri, 8. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı (iscturkey), 2015.

[14] H.D. Keskin ve H.S. Kurtuldu, Üniversite Öğrencilerinin Dijital Pazarlamaya Yatkınlık Düzeylerinin Belirlenmesi Üzerine Bir Araştırma, Küresel İktisat ve İşletme Çalışmaları Dergisi, Cilt: 7 Sayı: 14, 117-128, 2018.

[15] S. Yılmaz ve Ş. Sağıroğlu, Siber Güvenlik Risk Analizi, Tehdit ve Hazırlık Seviyeleri, 6. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı, (iscturkey),2013.

[16] K. Göztepe ve A. Ejder, Siber Terör Saldırılarından Korunmaya Yönelik Bulanık Mantık Tabanlı Karar Destek Modeli, Siber Güvenlik Çalıştayı, Ankara, 2011.

[17] A.N. Ünal ve B.S.B. Yarman, Milli Güç Unsurlarının Belirlenmesinde Siber Uzay Faktörü, 7. Bilgi Güvenliği ve Kriptoloji Konferansı, (iscturkey), 2014.

[18] E. Irmak ve İ. Erkek, Çok Nitelikli Fayda Teorisiyle Saldırgan Profiline Yeni Parametrelerin Eklenmesi, Uluslararası Bilgi Güvenliği Mühendisliği Dergisi, Cilt:2, No:2, S:1-9, 2016.

[19] Ö. Günal, Matematik ve Siber Güvenlik, https://ogunal.com/matematik-ve-siber-guvenlik/

[20] Ege, B., Kuantum Mekaniğinden Kuantum Bilgisayarlarına, Bilim Teknik, Ekim 2012.

[21] Yamamura, A., Ishizuka, H., Quantum cryptanalysis of block ciphers, Research Institute for Mathematical Sciences, Kyoto University, pp. 235-243, 2000.

[22] Beth, T., Müller-Quade,J., Steinwandt, R., Cryptanalysis of a Practical Quantum Key Distribution With Polarization-Entangled Photons, Quantum Physics, pp. 3865-3871, 2004.

[23] Z. Seskir, Kuantum Bilgisayarların Matematiği Üzerine, https://duzensiz.org/kuantum-bilgisayarlar

[24] M. Toyran, T. B. Pedersen ve arkadaşları, Bilgi Güvenliğinde Kuantum Teknikler, IV.Ağ ve Bilgi Güvenliği Ulusal Sempozyumu, 2011.

Siber Güvenlik Standartları

BÖLÜM 2

Prof. Dr. Şeref SAĞIROĞLU

SİBER GÜVENLİK STANDARTLARI

Siber güvenliğinin yüksek seviyede sağlanması için kurumların ve ulusların sahip oldukları bilgi varlıklarını bilinmesi, kıymetlendirmesi, sahip çıkması, politika ve standartlar çerçevesinde bu varlıklarını korunması gereklidir. Bunun için ise; mevcut standartların bilinmesi, yeni geliştirilen standartların takip edilmesi, bunların uygulanması ve güncellenmeleri gereklidir. Bu bölümde, siber güvenlik standartları gözden geçirilmiş, bazı standartlar ise detaylı olarak açıklanmış, genel olarak standartlar değerlendirilmiş, siber güvenliğinin sağlanmasında sağladığı katkılar açıklanmıştır.

2.1. Giriş

Veri hacminin, boyutunun ve çeşitliliğinin hızla arttığı günümüzde, verinin bilgiye ve özbilgiye yani değere dönüştürülmesi en önemli hususdur. Bu değer, veriye verilen önemi her geçen gün daha da arttırmakta dolayısıyla da verinin korunması ve mahremiyetinin sağlanmasının gereğini de ortaya çıkarmaktadır. Tehditlerin sürekli olarak artması, boyut değiştirmesi, yenilenmesi, kullanılan ve yeni geliştirilen yazılım veya donanımlarda meydana gelen güvenlik açıkları, insan faktörünün her zamankinden daha fazla etkili olmasından dolayı denetlenmesi veya kontrolü, politikaların, kuralların, yapıların ve süreçlerin takip edilebilmesi ve en üst seviyede bilgi güvenliğinin sağlanması için bilgi güvenliği süreçlerinin çok iyi bilinmesi ve yönetilmesi için çalışmalar yapılmaktadır.

Kişilerin sahip olduğu verilerin (kişisel verilerin) güvenliği önem arz ederken, bundan daha önemlisi, kişilerin güvenliğini doğrudan veya dolaylı olarak etkileyebilecek kurumsal ve ulusal bilgi güvenliğidir. Her birey kişisel bilgi varlıkları üzerinden kurumsal bilgi varlıklarına eriştiği veya kurumsal bilgi varlıkları üzerinden

hizmet aldığı için kurumsal bilgi varlıklarının yapılandırılması ve yüksek seviyede korunması için, erişimden doğrulamaya, depolamadan paylaşıma, analizden erişimi engellemeye verilerin ve siber güvenliğin sağlanması için standartlardan faydalanılmalıdır. Diğer bir ifade ile kişisel ve kurumsal bilgi varlıklarının korunabilmesi ve güvenliğin sağlanması için; bilginin üretildiği, erişildiği, işlendiği, taşındığı ve saklandığı her ortamda güvenliğinin sağlanması gereklidir. Bunun sağlanmasında; kurumun sahip olduğu mevcut yazılımlar, donanımlar, ortamlar, süreçler, politikalar, dokümanlar, projeler, lisanslar, insan kaynakları gibi hususlar ve bu hususların ortaya çıkardığı riskleri önleme çok önemli iken "standartlar", "politikalar", "sertifikalandırma", "denetim" gibi unsurlar ise bunu tamamlayan önemli unsurlar olarak karşımıza çıkmaktadır.

Literatür çalışmaları genel olarak incelendiğinde, bilgi güvenliği ve siber güvenlik konusunda;

- en zayıf halkanın insan olduğu, insani zafiyetleri saldırganların çok iyi kullandığı,
- bilinç ve farkındalık seviyesinin beklenilen ve istenilen seviyede olmadığı,
- açıklıklar, zayıflıklar ve kayıpların sürekli artış göstermesi sebebiyle bu konunun henüz doğru olarak anlaşılamadığı veya konuya gereken önemin verilemediği,
- bu kadar önlem alınmasına, yatırım yapılmasına, ve yeni çözümler geliştirilmesine karşın riskin artarak devam ettiği,
- birçok teknik veya teknik olmayan güvenlik kontrollerinin güvenliği sağlamada kullanıldığı,
- geliştirilen ve uygulanan pek çok standardın bulunduğu,
- farklı kurumların, ülkelerin, organizasyonların veya yapıların standart geliştirmeye veya güncellemeye devam ettikleri,
- standartları uygulamanın çok yüksek seviyede güvenlik sağlanmasına katkı sağladığı,
- standartları harfiyen uygulamanın bile bazen yüksek seviyede bilgi güvenliği sağlanmasına yeteri kadar hattakatkı sağlayamadığı,

- ülkelerin ulusal siber güvenliği sağlamaya yönelik olarak "ulusal siber güvenlik stratejileri ve eylem planları" geliştirdikleri ve uyguladıkları,
- artık her cihaz, konu, yapı, iş, işlem veya çalışma alanına yönelik olarak özel siber güvenlik çözümleri geliştirildiği,
- yeni iş alanları oluştuğu,
- yüksek niteliklere ve yeteneklere sahip uzmanlara çok ihtiyaç olduğu, ve
- bu alana yönelik olarak yeni teknik ve teknolojilerin geliştirilmesine paralel olarak, siber eklentili (siber savaş, oyun, alan, dünya, vb.) kelimelerin artık sıkça kullanıldığı, yeni terminolojilerin artık hayatımızın bir parçası olduğu

görülmektedir.

Bilgi varlıklarının yüksek seviyede korunması ve güvenliğinin sağlanması için;

- kurumsal bilgi varlıklarının bilinmesi ve değerinin farkında olunması,
- varlıkların karşılaşılabileceği risklerin önceden bilinmesi veya öngörülmesi,
- öngörülen ihlalleri ve riskleri en aza indirgeyecek veya ortadan kaldıracak çözümlerin geliştirilmesi,
- iş sürekliliğini sağlayacak çözümlere ağırlık verilmesi,
- standartlardan mutlaka faydalanılması,
- denetim yapılması ve denetim sonucuna uygun olarak sistemlerin iyileştirilmesi veya sıkılaştırılması,
- BGYS'nin kurumlarda hayata geçirilmesi ve kurumların belgelendirilmesi,
- karşılaşılan veya karşılaşılacak risklerin önceden ciddiye alınarak çözümlenmesi ve
- yapılan işlemlerin bir politika çerçevesinde yapılması

gereklidir.

Güvenliğin yüksek seviyede sağlanmasında temel unsurlarından olan uluslararası standartlar; konunun daha iyi anlaşılması, gerekli tedbirlerin doğru bir şekilde alınabilmesi, risklerin belirlenmesi ve giderilmesi, uygulamalarda karşılaşılabilecek olumsuzlukları gidermeye yönelik önceden önlem alınması, sistemlerin yapılarının ve işleyişlerin denetlenmesi ve yapılacak iyileştirmeler, politikalar ve risklerin belirlenmesi, risklerin akıllıca yönetilmesi gibi pek çok unsuru içermektedir.

2.2. Güvenlik Politikaları

Güvenlik politikaları;

- kurum veya kuruluşlarda kabul edilebilir güvenlik seviyesinin tanımlanması, uygulanması, denetlenmesi ve iyileştirilmesi gibi hususlara yardımcı olmaktadır. En önemlisi ise; standartlar ise kapsamlı politikalar oluşturulmasına katkılar sağlarlar.
- tüm çalışanların ve ortak çalışma içerisinde bulunan diğer paydaşların uyması gereken kurallar bütünüdür.
- bir kurumun bilgi güvenliğini sağlamak için tüm güvenlik faaliyetlerini kapsayan ve yönlendiren, yapılmasına yardımcı olan, kolayca yürütülmesi için prosedürleri içeren talimatlar olup kurumsal bilgi kaynaklarına erişim yetkisi olan tüm çalışanların uyması gereken kuralları içeren belgeler ve kararlardır.
- her kuruluş için farklılık gösterse de genellikle çalışanın sorumluluklarını, güvenlik denetim araçlarını, amaç ve hedeflerini, kurumsal bilgi varlıklarının yönetimini, korunmasını ve paylaşılmasını, önemli işlevlerin daha sıkı korunmasını düzenleyen kurallar, kararlar, uygulamalar, ve iyileştirmeler gibi hususları açıklayan ifadelerdir.

2.3. Güvenlik Standartlarını Destekleyen Organizasyonlar

Bilgi güvenliği unsurlarını destekleyen pek çok standart farklı yapılar ve organizasyon vardır [1-7]. Bunlar aşağıda kısaca açıklanmıştır. ISO, IEC, ANSI, IEEE, NIST, ITU, ISACA, NATO, ACM ve IETF

gibi organizasyonlar ve yapılar bunlardan bazıları olup açılımları verilmiş ve aşağıda kısaca tanıtılmıştır.

ISO (International Standards Organization) Uluslararası Standartlar Organizasyonu;

ANSI (American National Standards Institute) Amerikan Ulusal Standartlar Enstitüsü;

IEEE (Institute of Electrical and Electronics Engineers) Elektrik ve Elektronik Mühendisleri Odası;

NIST (National Institute of Standards and Technology) Ulusal Standartlar ve Teknoloji Enstitüsü;

IETF (Internet Engineering Task Force) İnternet Mühendisliği Çalışma Grubu;

AB (European Union) Avrupa Birliği;

WTO (World Trade Organisation) Dünya Ticaret Örgütü;

ICC (International Commerce Chamber) Uluslararası Ticaret Odası;

ITU (International Telecommunications Union) Uluslararası Telekomünikasyon Birliği;

CEN (European Committe for Standardization) Avrupa Standartlaşma Örgütü;

ETSI (European Telecommunication Standards Institute) Avrupa Telekomünikasyon Standartları Enstitüsü;

NATO (North Atlantic Treaty Organisation) Kuzey Atlantik Paktı;

AQAP (Allied Quality Assurance Publication) Müttefik Kalite Güvence Yayınları Standardı

TSE (Türk Standardları Enstitüsü)

ACM (Assoclation for Computing Macinery) Bilgisayar Derneği veya Hesaplaşma Makinesi Derneği;

BSI (British Standard Institution) İngiliz Standartlar Enstitüsü;

IEC (The International Electrotechnical Organization-IEC) Uluslararası Elektroteknik Komisyonu;

2.4. Bilgi Güvenliği Standartları

Bir önceki bölümde verilen kurumlar ve organizasyonlar, siber güvenlikte kullanılan standartları temel olarak geliştiren, değerlendiren ve güncelleyen kurumlardır.

İlk bilgisayar geliştirildiğinde, aslında o bilgisayarda oluşacak riskler belirlenmiş ve uyulması gereken kurallar ise "Turuncu Kitap" altında toplanmıştır. İlgili kitapta, güvenilir bilgisayar sistemleri değerlendirmek kriterleri verilmiş olup, belki de bu bilgisayar alanındaki ilk standart olarak kabul edilebilir.

Bilgi ve bilgisayarların güvenliğini ciddiye alan, literatürde kabul gören yaklaşımları geliştiren veya konuya profesyonel olarak yaklaşan İngiliz Standartlar Enstitüsü, bu alandaki ilk çalışmaları yapmış, hazırladığı dokümanları BS7799 standartı olarak 1995'de yayımlanmıştır. BS7799:V1 ise bunun ilk versiyonudur. 1999 ise aynı standardın ikinci kısmı olan BS7799:V2 standardını yayımlamıştır. Dünyanın konuya önem vermesi, diğer ülkelerin yaptığı çalışmalardan da faydalanılarak, BS7799:V1 standardı 2000 yılında bazı düzeltmeler ve küçük değişikliklerle ISO tarafından ISO/IEC 17799 adıyla uluslararası ISO standardı haline getirilmiştir. ISO tarafından daha sonra ise ISO 27001:2005 adıyla dünya genelinde "bilgi güvenliği standardı" olarak kabul edilmiştir.

Ülkemizde de Avrupa Birliği Uyum Kriterlerinde de adı geçen bu standartların uygulanması konusunda yapılan çalışmalar kapsamında, ISO 27001:2005 standardı Türkçeye çevrilerek Türk Standardları Enstitüsü (TSE) tarafından TS ISO/IEC 27001 "Bilgi Güvenliği Yönetim Sistemi (BGYS)" standardı adı altında yayınlanmış ve belgeleme çalışmaları başlatılmıştır. BGYS; insanları, süreçleri ve bilgi sistemlerini içine alan ve üst yönetim tarafından desteklenen bir yönetim sistemidir.

Daha sonraki yıllarda ise bilgi güvenliği standartları ailesi olarak 27xxx serisi olarak kabul edilmiş, mevcut standartlar ise aşama aşama bu ailenin birer üyesi haline getirilmeye başlanmıştır. Bunu yapan organizasyon, çalışma prensipleri ve geliştirilen standartlar ise aşağıda alt başlıklarda tanıtılmıştır.

2.4.1. ISO/IEC Standartları

Uluslararası Elektroteknik Komisyonu 1906, Uluslararası Standartlar Organizasyonu ise 1947 yılında uluslararası alanda ticari ve elektroteknik standardizasyonun sağlanması için, İsviçre'nin Cenova şehrinde kurulmuştur. ISO ve IEC birlikte teknik çalışma grupları oluşturarak (Joint Technical Committee-JTC) ve Bilimsel Komiteler (SC) koordinasyonunda tüm dünyada geçerli olacak standartları geliştirmektedirler. Bu standartlarla ilgili olarak detay bilgiye https://www.iso.org/ics/35/ adresinden erişebilirsiniz.

ISO tarafından BT (Bilişim Teknolojileri) Güvenlik Standartları ile ilgili çalışmalar JTC–1 BT Komitesine bağlı SC-27'ye bağlı olarak çalışan BT Güvenlik Teknikleri Alt Komisyonunda ele alınmaktadır. Bu komisyonun sorumluluk alanları ise aşağıda verilmiştir olup bunlar:

- BT sistemleri güvenlik hizmetlerinin ve ihtiyaçların tanımlanması,
- Güvenlik teknikleri ve yapılarının geliştirilmesi,
- Güvenlik rehberlerinin geliştirilmesi ve
- Yönetim destek dokümanları ile standartların geliştirilmesidir.

Yukarıda belirtilen görevleri yerine getirmek üzere bu komisyon içinde 5 ayrı çalışma grubu (working group-WG) bulunmaktadır. Bu gruplar ve bunların sorumlulukları ise aşağıda maddeler halinde verilmiştir.

- Çalışma Grubu–1 (JTC-1/SC-27/WG-1), bilgi güvenliği yönetim sistemleri üzerine çalışmaktadır.
- Çalışma Grubu–2 (JTC-1/SC-27/WG-2), şifreleme sistemleri ve güvenlik yapıları üzerine çalışmaktadır.
- Çalışma Grubu–3 (JTC-1/SC-27/WG-3), güvenlik değerlendirme kriterleri üzerine çalışmaktadır.
- Çalışma Grubu–4 (JTC-1/SC-27/WG-4), güvenlik denetimleri ve hizmetleri üzerine çalışmaktadır. Son olarak ise
- Çalışma Grubu–5 (JTC-1/SC-27/WG-5), kimlik yönetimi ve mahremiyet konuları üzerine çalışmakta ve çözümler geliştirmektedir.

Bu yapının daha iyi anlaşılması için bir örnek verilecek olursa; SC-27'ye bağlı olarak çalışmalar yapan Çalışma Grubu–1 (WG-1), bilgi güvenliği yönetim sistemleri standartları olan ISO/IEC 27000 ve ISO/IEC 27001 çalışmalarını yürütmektedir.

Diğer bir ifadeyle; bilgi güvenliği konularında; karşılaşılan veya karşılaşılabilecek tehditler, tehlikeler, açıklar veya riskler belirli sürelerde, ihtiyaç duyulduğunda veya karşılaşılan özel durumlar veya bildirimler dikkate alınarak, belirlenen süreçlerde iyileştirmeler ve güncellemeler yapılmakta, gerektiğinde ise yeni çalışmalarda başlatılabilmektedir.

Bu standart ailesinin tüm standartları, Bölüm 2.5'de Bilgi Güvenliği Standartları Ailesi başlığı altında kısaca tanıtılmıştır.

2.4.2. Türk Standartları (TSE Standartları)

Ülkemizde bilgi güvenliği standartları çalışmaları, uluslararası standartlara uygunluk, belgelendirmeler, güvenlik denetimleri, Türk Standardları Enstitüsü (TSE) tarafından yapılmaktadır. TSE bu çalışmaları, teknik kurullar, komiteler ve çalışma grupları ile yürütmektedir. Bu konu ile ilgili detay bilgiler bir sonraki bölümde verildiği için burada detaylı olarak açıklanmamıştır.

2.5. ISO/IEC Bilgi Güvenliği Standartları Ailesi

Kişisel ve kurumsal bilgi güvenliğinin üst düzeyde sağlanması için gerekli olan bilgi güvenliği yönetiminde kullanılan uluslararası standartlara http://www.iso27001security.com/index.html kısaca özetlenmiştir.

ISO/IEC 27000: teknik terimler ve açıklamalarının yer aldığı genel bir sözlüktür.

ISO/IEC 27001: BGYS için gereklilikleri ortaya koyan bir standarttır.

ISO/IEC 27002: bilgi güvenliği kontrol hedeflerini ve kontrollerini açıklayan bilgi güvenliği kontrolleri için iyi uygulamaları kapsar.

ISO/IEC 27003: 27001 standardının nasıl kullanılacağına dair açıklamalar ve örnekler içeren uygulama rehberi olarak geliştirilmektedir.

ISO/IEC 27004: Bilgi güvenliği yönetimi ölçümünü kapsar.

ISO/IEC 27005: Bilgi ve güvenliğinin risk yönetimini kapsamaktadır.

ISO/IEC 27006: BGYS belgelendirme kurumları için akreditasyon ve sertifikasyon süreci için bir kılavuz olup "Bilgi Teknolojileri Felaket Önleme Hizmetleri Kılavuzu" ismiyle yayımlanmıştır.

ISO/IEC 27007: BGYS'nin yönetim sistemi unsurlarını denetlemek için hazırlanmış bir kılavuzdur.

ISO/IEC 27008: güvenlik kontrolleri ile ilgili olarak yapılacak denetimlerin yapılmasında yönlendirici kılavuz niteliğindedir.

ISO/IEC 27009: sektörel veya sektöre özgü ISO 27000 serisi standartların geliştirilmesinde etkili olan SC-27'nin hazırladığı bir rehber niteliğindedir.

ISO/IEC 27010: Sektörler ve kurumlar arası iletişim için bilgi güvenliği yönetimine rehberlik eden bir standarttır.

ISO/IEC 27011: Telekomünikasyon kuruluşları için bir bilgi güvenliği yönetimi kılavuzudur. Uluslararası Haberleşme Birliği'nin yayımladığı ITU-T X.1051 dokümanını temel alır.

ISO/IEC 27013: Hem ISO/IEC 27001 hem de ISO/IEC 20000-1 (BT hizmeti yönetimi veya ITIL) ortak uygulamasına ilişkin rehberlik sağlar.

ISO/IEC 27014: Bilgi güvenliğinin yönetilmesine rehberlik sunmaktadır. Uluslararası Haberleşme Birliği'nin yayımladığı ITU-T X.1054 dokümanını temel alır.

ISO/IEC 27016: Bilgi güvenliği yönetiminin ekonomisi ile ilgili olan standarttır.

ISO/IEC 27017: Bulut bilişim için bilgi güvenliği kontrolleri ile ilgilidir. Uluslararası Haberleşme Birliği'nin yayımladığı ITU-T X.1631 dokümanını temel alır.

ISO/IEC 27018: Halka açık bulutlarda Kişisel Bilgilere (Kişisel Tanımlanabilir Bilgiler) ilişkindir.

ISO/IEC 27019: Nükleer olmayan enerji endüstrisinde süreç kontrolü için bilgi güvenliği ile ilgilenir.

ISO/IEC 27021: Bilgi güvenliği yönetimi uzmanlarının gerektirdiği yetkinlikleri, becerileri ve bilgiyi açıklar.

ISO/IEC 27023: ISO/IEC 27001 ve 27002'nin 2005 ve 2013 sürümleri arasındaki farklılıklara odaklanılmıştır.

ISO/IEC 27030: Nesnelerin İnterneti için güvenlik ve gizliliği kapsayacaktır.

ISO/IEC 27031: BT dayanıklılığı ve iş sürekliliğinde felaket kurtarma yaklaşımlarıyla ilgilidir.

ISO/IEC 27032: doğrudan siber güvenlik ile ilgili olarak yapılacak işlemleri kapsayan dokümanları içerir.

ISO/IEC 27033: BT ağ güvenliği ile ilgilidir.

ISO/IEC 27034: uygulama güvenliğine rehberlik etmek için geliştirilmektedir.

ISO/IEC 27035: güvenlik olay yönetimi ile ilgilidir.

ISO/IEC 27036: bulut bilişim ilişki yönetimi yönleri dahil olmak üzere tedarikçi ilişkileri için bir güvenlik kılavuzudur.

ISO/IEC 27037: dijital kanıtların tanımlanması, toplanması ve korunması ile ilgilidir.

ISO/IEC 27038: dijital belgelerin redaksiyonu için bir şartnamedir.

ISO/IEC 27039: Saldırı Tespit ve Önleme Sistemleri (IDS / IPS) ile ilgilidir.

ISO/IEC 27040: depolama güvenliği ile ilgilidir.

ISO/IEC 27041: adli bilişimde güvence (eForensics) ile ilgilidir.

ISO/IEC 27042: dijital kanıtların analizi ve yorumlanması ile ilgilidir.

ISO/IEC 27043: olay araştırması (eForensics) ile ilgilidir.

ISO/IEC 27045: Büyük veri sistemlerinin güvenlik ve gizlilik süreçlerini kapsayacaktır.

ISO/IEC 27050: eDiscovery / dijital adli bilimlerle ilgilidir.

ISO/IEC 27070: Bulutta sanallaştırılmış güven kökleri oluşturmak için güvenlik gereksinimlerini açıklar.

ISO/IEC 27099: AAA ile Güven Hizmet Sağlayıcıları için bilgi güvenliği yönetimi gereksinimlerini belirler.

ISO/IEC 27100: siber güvenlik kavramlarına genel bir bakış niteliğindedir.

ISO/IEC 27101: siber güvenlik çerçevelerinin geliştirilmesi konusunda bir kılavuz olacaktır.

ISO/IEC 27102: siber sigortaları kapsayacaktır.

ISO/IEC 27103: ISO27k ve diğer ISO ve IEC standartlarının siber güvenliği nasıl uygulanabileceğini açıklar.

ISO/IEC 27550: BT sistemlerinde mahremiyet mühendisliğini konularını kapsayacaktır

ISO/IEC 27551: Öznitelik tabanlı bağlanılamaz varlık kimlik doğrulaması için gereksinimleri belirleyecektir.

ISO/IEC 27552: gereksinimleri belirleyecek ve gizlilik yönetimi için ISO/IEC 27001 ve 27002'yi genişletme konusunda rehberlik edecektir.

ISO/IEC 27553: mobil cihazlarda biyometrik kimlik doğrulama için gereksinimleri belirleyecektir.

ISO/IEC 27554: kimlik yönetimi ile ilgili riski değerlendirmek için ISO 31000'i kullanmasını tavsiye edecektir.

ISO/IEC 27555: kişisel verilerin (PII) silinmesi hakkında yol gösterecektir.

ISO 27799: sağlık sektörüne özgü BGYS'yi uygulama rehberidir.

ISO/IEC 15408: 2016 Ortak Kriterler; Bilgi Güvenliği Standartlarının önemli olanlarından birisi olup, alınan bilgi teknolojileri güvenliği önlemlerini değerlendirmek amacıyla geliştirilmiş kriterler bütünüdür.

Bu bölümde standartlar kısaca açıklanmış olup, bu kitabın bir sonraki bölümde kısıtlı da olsa bazı standartlar, daha detaylı olarak hem açıklanmış hem de değerlendirilmiştir.

2.6. Açık Anahtar Şifreleme Standartları (PCKS-Public Key Crypto Standard)

RSA Laboratuvarları tarafından altyapısı oluşturulan ve Apple, Microsoft, DEC, Oracle, Lotus, Sun gibi uluslararası kuruluşlar ile MIT desteğiyle geliştirilen açık anahtar şifreleme standartları bir dizi standarttan oluşmaktadır. Bu standartlarda, algoritmalar ile uygulama ve programlama arayüzleri bulunmaktadır. PKCS bir Açık Sistem Arayüzü (OSI-Open System Interface) standardı olup ITU-T X.509 standardı gibi standartlarla da uyumluluk içerisindedir. Bu standartlar seri şekilde olup bunların bazıları yayımlanmamış, bazıları ise isim değiştirilerek günümüzde kullanılmaktadır. Yayımlanan standartlar sırasıyla PKCS #1, #3, #5, #6, #7, #8, #9, #10, #11 ve #15 dir. Bunlar aşağıda kısaca tanıtılmıştır. Bunlar;

- **PKCS #1:** PKCS #1, RSA açık anahtar şifreleme yaklaşımı kullanılarak, şifreleme ve imzalama verisi ilişkisinin nasıl kurulması gerektiğiyle ilgili şifreleme standardıdır.
- **PKCS #3**: Diffie-Hellman Anahtar Anlaşması standardını tanımlar.
- **PKCS #5:** Şifreyle desteklenen gizli (özel) anahtar şifreleme standardını tanımlar.
- **PKCS #6:** X.509 V.3. standardına sahip genişletilmiş sertifika standardını tanımlar.
- **PKCS #7:** Sayısal imza ve şifreleme gibi kriptografik gelişmeleri içeren, genel mesaj sözdizimi standardını tanımlar.
- **PKCS #8:** Özel anahtar bilgi sözdizimi standardını tanımlar.
- **PKCS #9:** Diğer PKCS standartlarında kullanılan özelliklerinden seçilmiş bir standardı tanımlar.
- **PKCS #10:** Sertifika talebinde sözdizimi standardını tanımlar.
- **PKCS #11:** Token ve akıllı kartlar (PCMCIA) gibi donanımların, teknoloji bağımsız kriptografik arayüz standardını tanımlar.

- **PKCS #12:** Özel anahtarları ve sertifikaları, güvenli olarak saklamak için en iyi standartlardan biridir. Kişisel bilgi değişimi, sözdizimi standardı olarak ta bilinir. Netscape ve Microsoft Internet Explorer gibi tarayıcılarda kullanılabilmektedir.
- **PKCS #15:** Akıllı anahtar ve tokenlarda kriptografik bilgi değişimi standardıdır.

2.7. ISO/IEC 15408: 2016 Ortak Kriterler

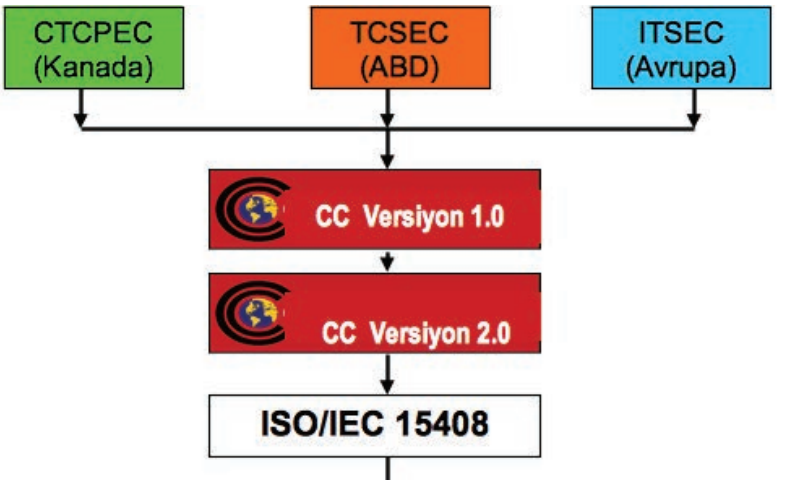
ISO/IEC 15408, Bilgi Güvenliği Standartlarının önemli olanlarından birisidir. Uzun süren çalışmalar sonucunda, Şekil 2.1'de verilen akışta açıklanan uluslararası kurum, kuruluş ve komitelerin desteğiyle hazırlanmış, bilgi teknolojileri güvenliği değerlendirme amacıyla geliştirilmiş kriterler bütünüdür. Kullanılan teknolojilerin güvenlik seviyelerinin belirlenmesi, geliştirilmesi ve değerlendirilebilmesinin uluslararası düzeyde kabul görmesi amaçlanmıştır. Üretilen bir ürünün veya sistemin güvenlik özelliklerini tespit ederken ve değerlendirirken, bir ürüne veya sisteme güvenlik özellikleri eklerken veya bu ürünlerin satın alınırken kullanılır ve uygulanır.

Ortak Kriterler, kullanıcılar, üreticiler veya geliştiriciler ile değerlendiriciler olmak üzere temelde 3 başlıkta gruplandırılmakta olup faydaları aşağıda kısaca özetlenmiştir. Bunlar;

- değerlendirme sonuçları karşılaştırılabilen güvenli sistemler tasarlanması, kullanılması ve yaygınlaştırılmasını kolaylaştırır.
- ihtiyaç duyulan güvenlik gereksinimlerinin üründe olduğunu garanti eder.
- istenilen güvenlik özelliklerini sağlayan ürünlerin talep edebilmesi ve bunların bir rehber olarak kullanılabilmesini sağlar.
- sertifikalı ürün kütüphanelerini temel alarak, ürün özelliklerinin isteklerini karşılayıp karşılamadığını kontrol edilebilir.
- bir ürünün tasarımından satışa sunulduğu tüm aşamalarda gerekli güvenlik özelliklerini sağlandığını garnti eden bir rehber niteliğindedir.
- Testi yapılan BT ürünlerinin standarda uygunluğunu değerlendirmede bir kaynak olarak kullanırlar.

- ürün değerlendirme sürecinde geliştirici ve değerlendirici arasındaki iletişimi sağlar ve değerlendirme süreçlerine kaynak bulunmasına destek olabilir.

Bu standardın kapsamı; giriş ve genel model, güvenlik fonksiyonel gereksinimleri ve güvenlik garanti gereksinimleri olmak üzere, üç kısımdan oluşmaktadır. Değerlendirme işlemi; bir ürünün standartlara göre değerlendirilmesi ve değerlendirilen ürünün sertifikalandırması aşamalarını kapsamaktadır.



Şekil 2.1. Ortak Kriter Oluşturma Çalışmaları Akışı

Ortak Kriterler Tanıma Antlaşması (Common Criteria Recognition Arrangement - CCRA) altına imza atan ve aralarında Türkiye'nin de bulunduğu birçok ülke tarafından kabul edilmiştir.

ISO tarafından yayınlanan Ortak Kriterler Serisi Türkçeye tercüme edilerek TS ISO/IEC 15408 başlığı altında 3 bölüm halinde Türk Standardı olarak yayımlanmıştır. Bu standart dokümanın;

- Birinci bölümünde; Giriş ve Genel Model, Ortak Kriterler'in genel kavramlarını güvenlik hedef ve gereksinimlerinin neler olduğunu tanımlamaktadır. Ayrıca, Güvenlik Hedefi (Security Target-ST) ve Koruma Profili (Protection Profile-PP)'ın içeriği de bu bölümde yer alır.
- İkinci bölümünde; güvenlik fonksiyonel gereksinimleri (Security Functional Requirements-SFR) listeleyen bir rehberdir.

- Üçüncü bölümünde ise; güvenlik garanti fonksiyonlarını listeleyen bölüm olup, bu bölümde garanti seviyeleri ve bu seviyelerin içermesi gereken seviyeleri garanti eden yapıları içermektedir [1].
- Koruma profilleri ve güvenlik hedefleri için değerlendirme kriterleri ve değerlendirme hedefleri için güvenlik seviyeleri belirlemede kullanılmak üzere **Değerlendirme Garanti Düzeyleri (EAL-Evaluation Assurance Level)** tanımlanmaktadır. EAL güvenlik garanti gereksinimleri;

• konfigürasyon yönetimi,
• dağıtım ve işletim,
• geliştirme,
• kılavuz dokümanları,
• yaşam döngüsü desteği,
• testler,
• açıklık değerlendirmesi, ve
• garantinin sürdürülmesi

gibi sekiz alt başlıkta incelenmektedir. Bu standart içerisinde farklı seviyelerde testler bulunmaktadır. Bu seviyelere göre ürünler sertifikalandırılmaktadır. Güvenlik değerlendirme garanti düzeyleri ve bunların açıklamaları aşağıda verilmiştir. Bunlar;

- **EAL-1 seviye:** Bu seyiyede, fonksiyonel olarak testler yapılmaktadır.
- **EAL-2 seviyesi:** Bu seviyede ise yazılım ve donanımların yapısal olarak testleri yapılmaktadır.
- **EAL-3 seviyesi:** Bu seviyede, testler metodolojik olarak yapılmaktadır.
- **EAL-4 seviyesi:** Bu seviyede, yapılan testler metodolojik tasarım, test ve kontrol şeklindedir.
- **EAL-5 seviyesi:** Bu seviyede testler, yarı-biçimsel tasarım ve testler şeklinde yapılmaktadır.
- **EAL-6 seviyesi:** Bu seviyede testler, yarı-biçimsel ve doğrulanmış tasarım ve testler şeklinde yapılmaktadır.

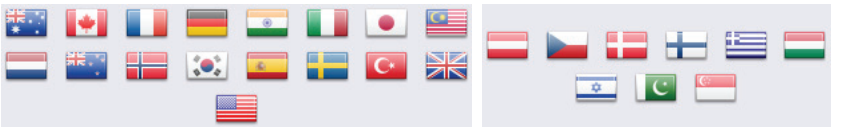
- **EAL-7 seviyesi:** Bu seviyede testler, biçimsel ve doğrulanmış tasarım ve testler şeklinde yapılmaktadır.

Yapılan testlerin önemini ve kapsamını belirtmek için daha kapsamlı bilgiler Şekil 2.2'de verilmiştir. Şekilden de görülebileceği gibi seviyelere göre daha fazla detay içermekte ve ürünler farklı seviyelerde ve detaylarda incelenmekte ve buna uygun olarak değerlendirmeler yapılmaktadır.

EAL-7 Biçimsel ve Doğrulanmış Tasarım ve Test
EAL-6 Yarı-Biçimsel ve Doğrulanmış Tasarım ve Test
EAL-5 Yarı-Biçimsel Tasarım ve Test
EAL-4 Metodolojik Tasarım, Test ve Kontrol
EAL-3 Metodolojik Olarak Test Edilmiş
EAL-2 Yapısal Olarak Test Edilmiş
EAL-1 Fonksiyonel Olarak Test Edilmiş

Şekil 2.2. Ortak Kriterler Değerlendirme Adımları

Sertifikalandırma Yapabilen Ülkeler	Sertifika Kullanan Ülkeler



Şekil 2.3. Ortak Kriterler Sertifikalandırma Yapan Ülkeler

Şekil 2.3'de ise yukarıdaki belirtilen seviyelerde üretilen ve testleri geçen ürünler sertifikalandırılmaktadır. Ortak Kriterler Sertifikalandırması yapan ülkeler içerisinde olan Türkiye'mizde vardır. Ülkemizde ise "değerlendirme" görevi TSE'dedir. TSE, bir sertifikasyon kuruluşu olup, aynı zamanda ise onaylayıcı konumda bir görev üstlenmiştir.

Yukarıda belirtilen testleri ülkemizde, TÜRKAK'tan ISO 17025 kapsamında akredite olmuş birimler bu testleri yapmaktadır. Bunlar; TÜBİTAK Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü Ortak Kriterler Test Merkezi (OKTEM) ve BEAM Teknoloji A.Ş. olup bu sertifikasyonu almış kurumlarımızdır. Tüm testler, bu birimlerimizde bağımsız olarak yapılabilmektedir.

Ürünün sertifikalandırılması ise, ülkemizde sertifikasyon kuruluşu olarak TSE'nin sorumluluğundadır. Bu sorumluluk çerçevesinde; Şekil 2.4'de özetlendiği gibi tüm aşama farklı açılardan değerlendirilir. Değerlendirme raporlarını inceleme, sertifika raporu hazırlama, sertifika hazırlama, yapıyı denetleme, değerlendirme laboratuvarını yetkilendirme ve performansını değerlendirme, değerlendirmenin ortak kriterlere ve ortak değerlendirme metodolojisine uygunluğuna dair garanti verme, değerlendirmeleri destekleme ve yönlendirme, teknik öngörüde bulunma gibi hususlar yerine getirilmektedir.

Şekil 2.4. Ortak Kriterler Ürün Sertifikalandırma Aşamaları ve Dikkat Edilecek Hususlar

Ortak Kriterler standartları belirli bir metodolojiye göre değerlendirilmektedir. Bu metodolojiler, Şekil 2.3'de verilen ülkelerden bazılarının hazırladıkları ve tamamının kabul ettiği "değerlendirme metodolojisi" dikkate alınarak yapılır. Buna bir örnek Şekil 2.5'de verilmiştir. Ortak Değerlendirme Metodolojisi (Common Evaluation Methodology-CEM) olarak isimlendirilen bu yaklaşım temel alınarak, daha öbce açıklanan PP, ST ve TOE değerlendirmeleri adımları temel alınarak yapılır [6]. Değerlendirmeyi yapan test laboratuvarı, değerlendirmelerin uluslararası geçerliliği olması için belirlenen metodoloji uygulamak ve buna göre rapor hazırlamak zorundadır.

Şekil 2.5. Ortak Kriterler Değerlendirme Metodolojisi

Bu birimlerde yapılan testlerde değerlendirme süreçleri; gerekli verilerin toplanması, başvuruda bulunan üreticinin güvenlik hedefleri, koruma profili ve değerlendirme hedefi, güvenlik hedefleri ile karşılaştırılma gibi hususlar temel alınarak ortak değerlendirme metodolojisine göre güvenlik ve kalite garantisi kapsamında yapılan inceleme işlemlerini kapsamaktadır.

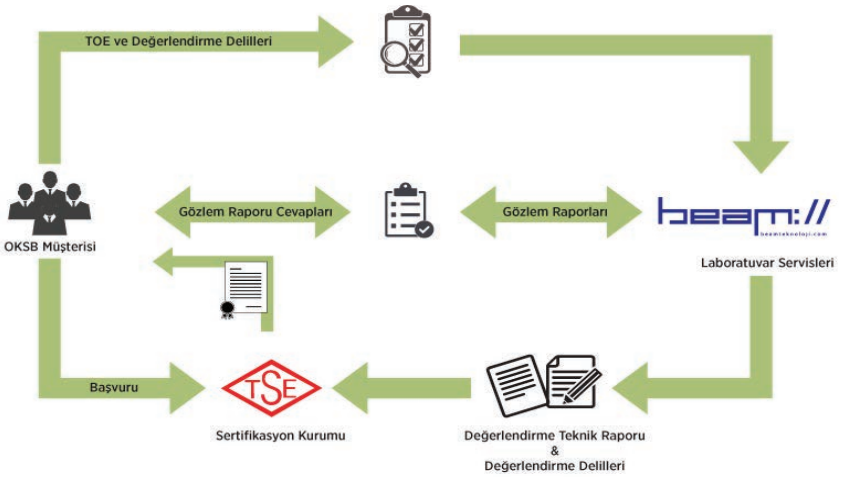
[6] nolu kaynakta verilen bu aşamalar aşağıda özetlenmiştir. Bunlar;

1. Ürünün ST'si değerlendirilip onaylanır.
2. ST onaylandıktan sonra TOE değerlendirilir.
3. Değerlendirme seviyesi belirlenir.

   Standarda göre yedi farklı değerlendirme seviyesi vardır. EAL1 ve EAL2 düşük garanti seviyeleridir. EAL3 ve EAL4 orta düzeyde garanti sağlayan ürünlere verilen seviyelerdir. EAL5 ve EAL6 yüksek derecede garanti veren seviyelerdir. EAL7 ise tam anlamıyla dört dörtlük garanti düzeyi sağlar.

4. ST yazılırken üretici veya geliştirici, iddia edilen garanti düzeyini ve ürünün sağladığı garanti gereksinimlerini belirtir. Bu gereksininmler, değerlendiricinin kontrol etmesi gereken hususlardır. Belirlenen ürünün sağladığı güvenlik gereksinimlerinin iddia edilen garanti düzeyinde olup olmadığı, gereksinimlerin doğruluğu gibi hususlardır.
5. Değerlendirici, değerlendirmeyi somuylaştırmak için TOE'nin değerlendirilmesi sırasında birtakım dokümanları üreticiden talep eder. Üretici, değerlendiricinin istediği bilgileri ve dokümanları değerlendiriciye sağlamak zorundadır.
6. Metodolojiye uygun olarak değerlendirilen ürün, değerlendirme teknik raporu ile birlikte ürüne uluslararası Ortak Kriterler sertifikasını verecek olan sertifikasyon kurumuna gönderilir.

Ülkemizde değerlendirme yapabilen kurum sayısı sınırlıdır. Bu testleri TÜRKAK'tan sertifikalı kurumlarımızdan TÜBİTAK BİLGEM ve BGD Kurumsal Üyesi olan BEAM Teknoloji yapabilmektedir. BEAM Teknoloji firmasının yaptığı değerlendirme süreçlerine ait akış [6], Şekil 2.6'da verilmiştir.



Şekil 2.6. Ortak Kriterler Müracaatlarını Değerlendiren Bir Merkeze ait Değerlendirme Süreci [6]

2.8. Müttefik Kalite Güvence Yayınları Standardı (Allied Quality Assurance Publications-AQAP)

Müttefik Kalite Güvence Yayınları, NATO'nun kalite gerekleri için yayınlamış olduğu ve NATO ülkelerinin uyması gereken, askeri alanda kalite standartlarının sağlanması için 1968'de geliştirilmiş ve kullanımda olan bir standarttır [8]. Aşağıda bu standartlar ve detayları verilmiştir.

- AQAP 2000: Ömür Devri Boyunca Kaliteye Bütünleşik Sistemler Yaklaşımına İlişkin NATO Politikası
- AQAP 2009: AQAP-2000 Serisinin Kullanımı için NATO Rehberi
- AQAP 2110: Tasarım, Geliştirme ve Üretim için NATO Kalite Güvence Gerekleri
- AQAP 2120: Üretim için NATO Kalite Güvence Gerekleri
- AQAP 2130: Muayene ve Test için NATO Kalite Güvence Gerekleri
- AQAP 2131: Son Muayene için NATO Kalite Güvence Gerekleri

TSE ise bu standartları Türkçeye çevirmiş ve TS 10000, TS10001, TS10002, TS10004, TS10005, TS10009 olarak yayımlanmaktadır.

AQAP belgesi, askeri alanda faaliyet gösteren firmaların Milli Savunma Bakanlığınca düzenlenen ihalelere katılabilmesi için ön şart niteliği taşımaktadır. AQAP belgelendirme ve ara denetim faaliyetleri Milli Savunma Bakanlığınca gerçekleştirilmektedir. Bu konu, kitabımızın 4. Bölümde detaylı açıklandığı için, bu bölümde açıklanmamıştır.

2.9. IEEE Standartları

Temelleri 1884'de Alexander Graham Bell ve Thomas Edison gibi önemli bilim insanları tarafından atılmış olan "Institute of Electrical and Electronics Engineers", mühendislik dallarından ve hatta bilim alanlarının artık içiçe olduğu günümüzde IEEE'nin açılımı "Institute of Engineers and Everyone Else" olarak ta ifade edilmektedir.

IEEE tüm dünyada toplam 10 bölgede, 150'den fazla ülkede, 420.000'in üzerinde üyesi bulunan, 350'ye yakın yerel bölge ve 2.000'den fazla öğrenci kolundan oluşan bir dünya organizasyondur.

Ülkemizde 8. bölgede faaliyet gösteren bu organizasyon, her yıl ulusal ve uluslararası konferanslar, teknik seminerler, gönüllü etkinlikler, hafif siklet (soft skill) eğitimler, sosyal sorumluluk projeleri ve çeşitli çalıştaylar gerçekleştirmekte veya yapılanları desteklemekte, üyelerine iş ve staj imkanı sunmakta veya üyelerine IEEE portal üzerinden pek çok hizmet vermektedir.

Bu hizmetler, yukarıda verilenlerle sınırlı olmayıp, bugün günlük hayatımızda kullandığımız pek çok teknolojide kullanan standartlar da geliştirilmektedir [9-14]. Güvenlik alanında 400'ün üzerinde standart çalışması vardır. Siber güvenlik alanında da yapılan standart çalışmalarından bazıları aşağıda kısaca tanıtılmıştır. Bunlar:

- **IEEE C37.240-2014**
  IEEE Standardı: Trafo Merkezi Otomasyonu, Koruma ve Kontrol Sistemleri için Siber Güvenlik Gereklilikleri
- **IEEE 1686-2013**
  IEEE Standardı: Akıllı Elektronik Cihazlar İçin Siber Güvenlik Özellikleri

- **IEEE 1711-2010**
  IEEE Standardı: Trafo Merkezi Seri Bağlantılarının Siber Güvenliği İçin Şifreleme Protokolü İçin Deneme Kullanım Standardı
- **IEEE 692-2013**
  IEEE Standardı: Nükleer Enerji Üretme İstasyonları için Güvenlik Sistemleri Kriterleri
- **IEEE 2030-2011**
  Enerji Şebekesi ile Akıllı Şebekenin Birlikte Çalışabilirliği için IEEE Kılavuzu ve Elektrik Enerjisi Sistemi (EPS), Son Kullanım Uygulamaları ve Yüklerle Çalışma Bilgi Teknolojisi
- **IEEE C37.240-2014**
  IEEE Trafo Merkezi, Otomasyon, Koruma ve Kontrol Sistemlerinde Standart Siber Güvenlik Gereklilikleri
- **IEEE 1686-2013**
  IEEE Akıllı Elektronik Cihazlar Siber Güvenlik Yetenekleri Standardı

- **IEEE 1711-2010**
  IEEE Trafo Merkezi Seri Bağlantılarının Siber Güvenliği İçin Şifreleme Protokolü İçin Deneme Kullanım Standardı
- **IEEE 1815.1-2016**
  IEC 61850 ve IEEE Std 1815 Uygulayan Ağlar Arasında Bilgi Alışverişi İçin Onaylı Taslak Standart
- **IEEE 1815-2012**
  IEEE Elektrik Enerjisi Sistemlerinde Dağıtık Ağ Protokolü Tabanlı Haberleşme Standardı
- **IEEE 692-2013**
  IEEE Nükleer Enerji Üretme İstasyonları için Güvenlik Sistemleri Kriterleri Standardı
- **IEEE 2030-2011**
  IEEE Elektrik Enerjisi (EPS), Son Kullanım Uygulamaları ve Yüklerin Çalışma Enerji Teknolojisi ve Bilgi Teknolojisinin Akıllı Birlikte Çalışabilirliği Kılavuzu

- **IEEE 1363-2000**
  IEEE Açık Anahtar Şifreleme için Standart Özellikler
- **IEEE 1619-2007**
  IEEE Blok Odaklı Depolama Aygıtlarında Verileri Şifreleme Koruma Standardı
- **IEEE 2410-2015**
  IEEE Biyometrik Açık Protokol Standardı,
- **IEEE P1912**
  Kablosuz Tüketici Cihazları için Gizlilik ve Güvenlik Mimarisi Standardı
- **IEEE 2600-2008**
  IEEE Bilgi Teknolojisi Standardı: Basım Cihazı ve Sistem Güvenliği
- **IEEE 802.1AR-2009**
  Yerel ve büyükşehir alan ağları için standart - Güvenli Cihaz Kimliği
- **IEEE 802.21a-2012**
  IEEE Yerel ve Metropolitan Alan Ağları Standardı
- **IEEE 1888-2014**
  IEEE Her Türlü Çevre Dosyu Kontrol Ağ Protokolü Standardı

2.10. ETSI Standartları

Kısa adı ETSI olan **Avrupa Telekomünikasyon Standartları Enstitüsü**, **Avrupa Posta ve Telekomünikasyon İdareleri Birliği** tarafından 1988 yılında Fransa'da kurulmuştur. Avrupa düzeyinde standardizasyon alanında çalışmalarda bulunan bir kurum olan ETSI, telekomünikasyon, televizyon ve radyo yayıncılığı ile BT alanlarında standardizasyon çalışmalarını yürütmektedir. Bilgi Teknolojileri ve İletişim Kurumumuzun da gözlemci statüde üye olduğu ETSI, 55 ülkeden 700'e yakın üyesi olan bir yapıdır. AB'nin girişimi ile CEPT, CEN ve CENELEC tarafından kurulan ETSI'nin amacı, üye ülkeler arasında telekomünikasyon altyapılarını birleştirmek, terminal donanımlarının uyumluluğunu sağlamak ve Avrupa telekomünikasyon ağını oluşturmaktır. ETSI, telekomünikasyon sektörünün gide-

rek küreselleşmesine etkili olan standartlar geliştirmektedir. Standartlarla ilgili daha detay bilgilere https://www.etsi.org adresinden erişilebilir. ETSI'nin güncel olarak yayımladığı siber güvenlik ile ilgili standartlardan güncel olanları aşağıda verilmiştir. Bunlar;

- **ETSI TR 103 306 V1.3.1 (2018-08)**
  Küresel Siber Güvenlik Ekosistemi
- **ETSI TS 103 645 V1.1.1 (2019-02)**
  Nesnelerin İnterneti İçin Siber Güvenlik
- **ETSI TR 103 308 V1.1.1 (2016-01)**
  NFV ve ilgili platformlar için LI ve RD ile ilgili güvenlik temelleri
- **ETSI TS 103 307 V1.3.1 (2018-04)**
  LI ve RD Arabirimleri için Güvenlik Yönleri
- **ETSI TR 103 642 V1.1.1 (2018-10)**
  Beyaz kutu modelinde yazılımı korumak için güvenlik teknikleri
- **ETSI TR 103 456 V1.1.1 (2017-10)**
  Ağ ve Bilgi Güvenliği (NIS) Direktifinin Uygulanması
- **ETSI TR 103 421 V1.1.1 (2017-04)**
  Ağ Geçidi Siber Savunma
- **ETSI TR 103 533 V1.1.1 (2019-08)**
  SmartM2M; Güvenlik; Standartlar Peyzaj ve en iyi uygulamalar
- **ETSI TR 103 305-5 V1.1.1 (2018-09)**
  Etkili Siber Savunma İçin Kritik Güvenlik Kontrolleri; Bölüm 5: Gizlilik geliştirme
- **ETSI TR 103 305-4 V2.1.1 (2018-09)**
  Etkili Siber Savunma İçin Kritik Güvenlik Kontrolleri;
- **ETSI TR 103 305-3 V2.1.1 (2018-09)**
  Etkili Siber Savunma İçin Kritik Güvenlik Kontrolleri
- **ETSI TR 103 305-2 V2.1.1 (2018-09)**
  Etkili Siber Savunma İçin Kritik Güvenlik Kontrolleri
- **ETSI TR 103 305-1 V3.1.1 (2018-09)**
  Etkili Siber Savunma İçin Kritik Güvenlik Kontrolleri

- **ETSI TS 103 523-3 V1.3.1 (2019-08)**
  Middlebox Güvenlik Protokolü
- **ETSI TR 103 534-1 V1.1.1 (2019-08)**
  SmartM2M; Öğretim materyali;
- **ETSI TR 103 331 V1.1.1 (2016-08)**
  Yapısal tehdit bilgi paylaşımı
- **ETSI GS ISI 003 V1.2.1 (2018-01)**
  Bilgi Güvenliği Göstergeleri (ISI); Güvenlik olayı tespitinin olgunluğunu değerlendirmek için Anahtar Performans Güvenlik Göstergeleri (KPSI)
- **ETSI TR 103 303 V1.1.1 (2016-04)**
  Kritik Altyapı bağlamında BİT için koruma önlemleri
- **ETSI TR 103 118 V1.1.1 (2015-08)**
  Makineden Makineye iletişim (M2M); Akıllı Enerji Altyapıları güvenliği; Mevcut güvenlik önlemlerinin gözden geçirilmesi ve yakınsama araştırmaları

- **ETSI EG 203 251 V1.1.1 (2016-01)**
  Test ve Şartname Metodları; Riske Dayalı Güvenlik Değerlendirme ve Test Metodolojileri
- **ETSI GS ISI 007 V1.1.1 (2018-12)**
  Bilgi Güvenliği Göstergeleri (ISI); Güvenli bir Güvenlik Operasyon Merkezi (SOC) oluşturmak ve işletmek için rehber
- **ETSI TS 103 487 V1.1.1 (2016-04)**
  NFV ve ilgili platformlar için hassas fonksiyonlarla ilgili temel güvenlik gereksinimleri
- **ETSI TR 103 309 V1.1.1 (2015-08)**
  Varsayılan olarak güvenli - platform güvenliği teknolojisi
- **ETSI TS 103 457 V1.1.1 (2018-10)**
  Güvenilir Etki Alanları Arası Arabirim: Hassas işlevleri güvenilir bir etki alanına boşaltan arabirim
- **ETSI GR QSC 006 V1.1.1 (2017-02)**
  Kuantum Güvenli Şifreleme (QSC); Simetrik anahtar boyutlarına uygulanan Quantum Computing ile sınırlar

- **ETSI EG 203 310 V1.1.1 (2016-06)**
  Bilişim Sistemlerinin Güvenliği Üzerine Kuantum Hesaplama Etkisi; İş Sürekliliği ve Algoritma Seçimi Önerileri
- **ETSI GS ISI 006 V1.1.1 (2019-02)**
  Bilgi Güvenliği Göstergeleri (ISI); ISI odaklı bir Ölçüm ve Etkinlik Yönetimi Mimarisi (IMA) ve CSlang - Ortak bir ISI Semantics Spesifikasyon Dili
- **ETSI GS ISI 002 V1.2.1 (2015-11)**
  Bilgi Güvenliği Göstergeleri (ISI); Olay Modeli Bir güvenlik olayı sınıflandırma modeli ve taksonomisi
- **ETSI GS ISI 001-2 V1.1.2 (2015-06)**
  Bilgi Güvenliği Göstergeleri (ISI)
- **ETSI TR 187 010 V2.1.1 (2008-07)**
  Telekomünikasyon ve İnternet bağlantılı Gelişmiş Ağ İletişimi için Servis ve Protokoller (TISPAN); NGN Güvenliği; Kimlik bağlantısında güvenlik ve NGN'de çözülmeleri ile ilgili konularda rapor
- **ETSI GS ISI 008 V1.1.1 (2018-06)**
  Bilgi Güvenliği Göstergeleri (ISI); Genel Kurum Genelinde Güvenlik Bilgi ve Etkinlik Yönetimi (SIEM) Yaklaşımının Tanımı
- **ETSI GS ISI 004 V1.1.1 (2013-12)**
  Bilgi Güvenliği Göstergeleri (ISI); Olay algılama uygulaması için yönergeler
- **ETSI TR 103 370 V1.1.1 (2019-01)**
  Gizlilik için Teknik Standartlar için pratik tanıtım rehberi
- **ETSI TR 103 304 V1.1.1 (2016-07)**
  Kişisel Olarak Tanımlanabilir Bilgi (PII) Mobil ve bulut hizmetlerinde koruma
- **ETSI TS 102 165-1 V5.2.3 (2017-10)**
  Tehdit, Güvenlik Açığı, Risk Analizi (TVRA) için Yöntem ve Protokoller
- **ETSI TR 103 617 V1.1.1 (2018-09)**
  Kuantum Güvenli Sanal Özel Ağlar

- **ETSI TS 103 458 V1.1.1 (2018-06)**
  IoT cihazları, WLAN, bulut ve mobil servislerde PII ve kişisel verilerin korunması için Öznitelik Tabanlı Şifreleme (ABE) Uygulaması - Yüksek seviye gereksinimler
- **ETSI TR 103 570 V1.1.1 (2017-10)**
  Kuantum Güvenli Anahtar Değişimleri
- **ETSI TS 103 532 V1.1.1 (2018-03)**
  Özellik Tabanlı Erişim Kontrolü için Özellik Tabanlı Şifreleme
- **ETSI GS NFV-SEC 013 V3.1.1 (2017-02)**
  Ağ İşlevleri Sanallaştırma (NFV) Sürüm 3; Güvenlik; Güvenlik Yönetimi ve İzleme şartname
- **ETSI GS NFV-REL 003 V1.1.2 (2016-07)**
  Ağ İşlevleri Sanallaştırma (NFV); Güvenilirlik; Uçtan Uca Güvenilirlik için Modeller ve Özellikler Raporu
- **ETSI GR QSC 004 V1.1.1 (2017-03)**
  Kuantum Güvenli Şifreleme; Kuantum Güvenli tehdit değerlendirmesi

2.11. ITU (Uluslararası Telekomünikasyon Birliği) Standatları ve Siber Güvenlik Faaliyetleri

ITU [20], 1865 yılında iletişim ağlarında uluslararası bağlantıyı kolaylaştırmak için kurulan küresel radyo spektrum ve uydu yörüngelerini tahsis eden, ağlar ve teknolojilerin sorunsuz bir şekilde birbirine bağlanmasını sağlayan teknik standartlar geliştiren ve dünya genelinde hizmet vermeyen topluluklara erişim sağlamak için çalışan uluslararası bir birliktir. Cep telefonuyla bir telefon görüşmesi yapıldığında, İnternete girildiğinde veya bir e-posta gönderdiğinde, ITU'nun çalışmalarından faydalanılmaktadır. ITU, tüm dünya insanlarını bir araya getiren, çalışmalarında herkesin iletişim kurma hakkını koruçalışan ve destekleyen bir yapıda hizmet vermektedir.

ITU'nun temel bir rollerinden birisi de, Bilgi Toplumu Zirvesi (WSIS) ve ITU Ortak Konferansı'nın rehberliğine dayanan Bilgi ve İletişim Teknolojilerinin kullanımında güven oluşturmak ve güvenliği sağlamaktır. WSIS'de, Devlet Başkanları ve dünya liderleri, ITU'nun 2007'de Küresel Siber Güvenlik Gündemini (GCA) başla-

tarak, bu alanda uluslararası işbirliği için "Bilişim Teknolojilerinin Kullanımında Güven oluşturmak ve Güvenliği Sağlamak" amacına yönelik çerçeve oluşturmak amacıyla C5 Eylemi kapsamında kolaylaştırıcısı olarak ITU'yu görevlendirmiş olup, bu kapsamda çalışmalarını sürdürmektedir. Bu kapsamda aşağıdaki programlar kapsamında faaliyetler sürdürmektedir [20]. Bunlar;

- **USOM (NATIONAL CIRT) PROGRAMI**

  Siber olaylarla başa çıkacak kurumsal yapıların ve dolandırıcılığa veya bilgilerin tahrip olmasına yol açan saldırıların olmaması, siber tehditlerle mücadeleye katkı sağlamaktır.

- **KÜRESEL SORUMLULUK ENDEKSİ**

  Küresel Siber Güvenlik Endeksi (GCI), ulus devletlerin siber güvenlik yeteneklerini ölçen ve dolayısıyla küresel bir siber güvenlik kültürünü teşvik etmek için bilinçli kararların alınmasına katkı sağlamak için geliştirilmiş bir projedir.

- **ÇOCUK ONLINE KORUMA (COP)**

  COP, dünya çapında çocukların çevrimiçi korunmasını teşvik ve ortak mücadele etmek amacıyla kurulmuş uluslararası bir işbirliği ağıdır.

- **ULUSAL STRATEJİLER**

  Ulusal siber güvenlik kapasitesini etkin bir şekilde arttırmak için tüm paydaşlara kabul edilebilir bir yol haritası hazırlamalarına katkı sağlamak amacıyla oluşturulmuştur.

- **GÜVENLİK STANDARTLARI**

  Bu çalışmalar, ITU-T Çalışma Grubu 17 tarafından yürütülmektedir. Bilgi ve İletişim Teknolojileri (BİT) kullanımında güven ve güvenlik oluşturmadan sorumludur. Siber güvenlik ile ilgili çeşitli teknolojilerin çalışmalarına odaklanmıştır.

- **GÜVENLİ RADYO HABERLEŞMESİ**

  ITU-R, IMT (3G ve 4G) ağları için açık güvenlik ilkeleri kapsamında dijital uydu sistemleri için ağ yönetimi mimarisindeki güvenlik sorunları ve uydu ağları üzerinden iletim kontrol protokolünün performans iyileştirmeleri için tavsiyeleri içerir.

Bunlara ilave olarak; **ITU-T** güvenlikle ilgili standardizasyon boşluğunun kaldırılması için çalışan ITU-T Çalışma Grubu 17, telekomünikasyon güvenliği faaliyetleri için lider çalışma grubudur. ITU-T Çalışma Grubu 17, pratik güvenlik çözümlerini belirlerken gelişmekte olan ülkelere ilgi duyabilecek ve kullanabilecek materyalleri üretmektedir. Bunun bir örneği yeni revize edilmiş BİT güvenlik standartları yol haritasıdır. Bu yol haritası, yalnızca ITU-T'nin değil, aynı zamanda ISO/IEC, IETF ve konsorsiyum gruplarının da erişemeyeceği faaliyetlerin bir parçası olarak ağla ilgili güvenlik çalışmalarını ele almaktadır. Günümüzde ITU-T güvenlikle ilgili standartların gelişmekte olan ülkelerinde dağıtım ve farkındalığı arttırmak için ortak ITU-T/ITU-D faaliyetleri yürütülmektedir. Mevcut ITU-T güvenlik standartları hakkındaki bilgiler, ITU'nun güvenlik standartlarının geliştirilmesinde, gelişmekte olan ülkelerden daha fazla sayıda katılımcının yer almasını sağlamak için dünya çapındaki ITU etkinliklerinde üye devletlerine yaygın olarak dağıtılmaktadır. ITU Genel Kurul Kararı 123 (Rev. Antalya, 2006) özellikle "gelişmekte olan ülkeler ile gelişmiş ülkeler arasındaki standardizasyon açığının kapatılması" ile ilgilidir.

Bu konularda yapılan çalışmalar, faaliyetler, raporlar, öneriler ve kaynaklara ITU http://www.itu.int/ITU-D/cyb/cybersecurity/standards.html bağlantısından erişilebilir. Bu sayfada yer alan bazı önemli başlıklar aşağıda verilmiştir. Bunlar;

- ITU WTSA Kararı 50: Siber Güvenlik (Rev. Johannesburg, 2008)
- ITU WTSA Karar 52: İstenmeyen postalarla mücadele ve mücadele (Rev. Johannesburg, 2008)
- ITU WTSA Kararı 58: Özellikle gelişmekte olan ülkeler için ulusal bilgisayar olayı müdahale ekiplerinin oluşturulmasını teşvik etmek (Johannesburg, 2008)

ITU-T Çalışma Grubu 17'nin ürettiği çıktılara yine aynı web sayfasından erişilebilinir. Bunlar;

- ITU-T telekomünikasyon güvenlik web sitesi
- ITU-T kimlik yönetimi web sitesi

- ITU-T Güvenlik Özeti, "Telekomünikasyon güvenliği ile ilgili onaylanmış ITU-T Önerileri Kataloğu" ve "ITU-T onaylı güvenlik tanımlarının çıkarılması" bölümünü içerir.
- Tüm Çalışma Grubu özetleri 17 Geliştirme veya revize edilen öneriler. (En son taslak özetler.)
- ITU-T'in güvenlikle ilgili faaliyetlerini özetleyen belge
- ITU-T Tavsiye E.408: Telekomünikasyon ağları güvenlik gereksinimleri
- ITU-T Tavsiye E.409: Olay organizasyonu ve güvenlik olayı ele alma: Telekomünikasyon kuruluşları için rehber
- X-Serisindeki ITU-T Tavsiyeleri: Veri ağları, açık sistem iletişimi ve güvenlik
- ITU-T Tavsiyesi X.1205: Siber Güvenliğe Genel Bakış
- Son İnternet Yönetişim Forumu (IGF) toplantılarında yapılan ITU-T Çalışma Grubu 17'nin çalışmalarına ilişkin sunumlar:
  - 2008 (Haydarabad, Hindistan): Siber Güvenlik Açık Forumu: Küresel Siber Güvenlik için Eylem
  - 2007 (Rio de Janeiro, Brezilya): ITU-T Güvenlik Girişimleri - Güncelleme
  - 2006 (Atina, Yunanistan): ITU-T Güvenlik Girişimlerine Genel Bakış
- ITU-D Siber Güvenlik Girişimleri: ITU-T Çalışma Grubu için ITU-D Sunumu 17

2.12. PCI Güvenlik Standartları Konseyi

PCI (Payment Card Industry) Güvenlik Standartları Konseyi [21], ödeme sistemlerinin güvenliği için standartların anlaşılması, geliştirilmesi, yaygınlaştırılması ve sektörün bir araya gelmesi için oluşturulmuş küresel bir forum olup, Ödeme Kartı Endüstrisi Güvenlik Standartlarını sağlama, koruma, geliştirme ve teşvik etme yönünde çalışmalar yapmaktadır. Ayrıca, değerlendirme ve tarama nitelikleri, öz değerlendirme anketleri, eğitim ve öğretim ve ürün sertifikasyon programları gibi standartların uygulanması için gerekli kritik

araçları sağlar. Konseyin kurucu üyeleri; American Express, Discover Financial Services, JCB International, MasterCard ve Visa Inc., veri güvenliği uyumluluk programlarının her biri için teknik gereksinimlerin bir parçası olarak PCI Veri Güvenliği Standardı (PCI DSS) geliştirilmiştir. PCI konseyi tarafından sağlanan Qualified Security Assessor (QSA) sertifikasına sahip olan denetçiler aracılığıyla yapılan işlemlerin denetimleri yapılmaktadır.

2.13. NIST Siber Güvenlik Platformu (NIST Cybersecurity Framework)

Amerika Standart Enstitüsü (NIST), oluşturduğu bu gönüllü çerçeve platform ile, siber güvenlikle ilgili riski yönetmek için standartlardan, yönergelerden ve en iyi uygulamalardan kolaylıkla faydalanılmasını ve paylaşılmasını sağlayan bir platform geliştirmiştir. Siber Güvenlik Çerçeve Platformunun amacı [17] ise; öncelikli olarak ulusal güvenlik için kritik öneme sahip altyapılar ile diğer sektörlerin korunmasını ve saldırılara dayanıklılığını arttırmaya yönelik esnek ve uygun maliyetli yaklaşım sunmaya yardımcı olmaktadır. Bu platformda; karşılaşılan problemlere çözümler, başarı hikayeleri, çevrimiçi eğitimler, değerlendirmeler, öneriler, yönlendirmeler, uygulamalar, raporlar, uyarılar, sunumlar, etkinlikler, önemli bilgi kaynakları ve bu kitap bölüm ile ilgili önemli olan hususu destekleyen, karşılaşılan problemlerin çözümüne yönelik standartlar önerilmektedir. Bu web sayfası mutlaka incelenmelidir. Detay bilgi için https://www.nist.gov/cyberframework web portalı ziyaret edilebilir.

2.14. Bilişim Teknolojileri Yönetim ve Denetim Enstitüsü (ISACA) Standartları

ISACA; Bilgisayar Sistemlerinin Denetimi ve Kontrolü (Information Systems Audit and Control) ile ilgili bir meslek grubunun belirlenen alanda rehberlik ihtiyacını hem karşılamak hem de tartışmak ve geliştirmek üzere 1969 yılında ABD'de kurulmuş uluslararası bir sivil toplum örgütüdür. 1976 yılında faaliyetleri alanına BT Yönetişimi (IT Governance) eklemiş, BT Yönetişim Enstitüsü (ITGI - IT Governance Institute) ile birleşmiştir. Bu uluslararası organizasyon, Bilgi Sistemleri Denetimi (CISA), Bilgi Güvenliği Yönetimi (CISM), Ku-

rumsal Bilgi Teknolojileri Yönetişimi (CGEIT), Bilgi Sistemleri Risk Yönetimi (CRISC) gibi alanlarda temel norm ve ilkeleri tanımlama ve sertifikasyon faaliyetleri, eğitim programları ile mesleki yeterlilik belgelendirme faaliyetlerini yürütmekte olup, bugün için, dünyada 200'den fazla temsilcilikleri olan 100.000'in üzerinde üyesi bulunan bir yapıda faaliyet göstermektedir. Ülkemizde de İstanbul ve Ankara'da temsilcilikleri olan bu yapı içerisinde ülkemizde de ilk ve tek üniversite öğrenci topluluğu Gazi Üniversitesinde 2017 yılında kurulmuş, benim de koordinatörlüğünü yürüttüğüm bir yapı içerisinde çalışmalarını yürütmektedir.

Bilişim Teknolojileri Yönetim ve Denetim Enstitüsü Derneği 2011 yılında Ankara'da kurulmuş olan ve benimde belirli bir zaman dernek üyesi olarak Akademik Koordinatör olarak katkı verdiğim bu derneğin amacı; "Bilişim Sistemleri ve Bilgi Teknolojileri alanında Yönetim, Yönetişim, Denetim, İç Kontrol, Uyumluluk, Güvenlik, Risk Yönetimi, Süreç Yönetimi, Danışmanlık, Proje Yönetimi ve Bilimsel Araştırma faaliyetlerinde bulunan kişilerin bir araya gelmesini sağlayarak, bu konulardaki bilgi ve birikimlerin paylaşılarak mesleki alanda gelişmeye, standardizasyona, farkındalık oluşturmaya, yapılan uygulamalarda verimliliği ve bilimselliği arttırmayı destekleyecek etkinlikler ile bireylere, organizasyonlara ve topluma katkıda bulunmak" olarak tanımlamakta ve ISACA-ITGI olmak üzere COBIT, ISO, ITIL, CMMI, PRINCE, PMI gibi uluslararası referanslar, yöntem ve standartlar ile uyumlu çalışmalar yürütmektir.

Bu kitap serisinin, 2. Ciltinin 9. Bölümünde detaylı açıklamalar olduğu için burada bu konu detaylı olarak açıklanmamıştır. Detay için, ilgili bölüme okuyunuz.

2.15. ENISA (European Union Agency For Cybersecurity)

Avrupa Birliği Siber Güvenlik Ajansı (ENISA) [19], 2004 yılından beri Avrupa siber güvenliğini sağlamak için çalışan bir ajans olup, merkezi Yunanistan'ın Atina şehrindedir. Ayrıca, Yunanistan'ın Kandiye kentinde de ikinci bir ofisi bulunmaktadır. ENISA, iki veya daha fazla AB Üye Devletinin etkilendiği durumlarda sınırlar arasında gerçekleşen büyük ölçekli siber olaylara karşı koymak için üye ülkeler ile Avrupa Birliği paydaşlarını destekleyen politikaları

oluşturan ve aktif olarak katkıda bulunan bir yapıdır. Ajans, kabiliyetlerini arttırmanın yanı sıra tavsiye ve çözümler sunmak için üye devletler ve özel sektörle birlikte çalışmaktadır. Verilen destek bununla sınırlı olmayıp, aşağıdaki hususları da içerir:

- pan-Avrupa Siber Güvenlik Egzersizleri, Ulusal Siber Güvenlik Stratejilerinin geliştirilmesi ve değerlendirilmesi,
- CSIRT'ler işbirliği ve kapasite geliştirme,
- IoT ve akıllı altyapılar üzerine çalışmalar, veri koruma konularını ele alma, gizlilik arttırıcı teknolojiler ve yeni ortaya çıkan teknolojilerdeki gizlilik, eID'ler ve güven hizmetleri, siber tehdit ortamını ve diğerlerini belirlemedir.

ENISA ayrıca, AB'nin ağ ve bilgi güvenliği (NIS) ile ilgili konularda politika ve kanunlarının geliştirilmesini ve uygulanmasını desteklemekte ve üye devletlere ve AB kurumlarına, organlarına ve ajanslarına, güvenlik açığı ifşa politikalarının gönüllü olarak oluşturulmasında ve uygulanmasında yardımcı olmaktadır. 2019'dan bu yana, Siber Güvenlik Yasası'nın yürürlüğe girmesini takiben (Yönetmelik 2019/881), ENISA'nın teslim edilmesini destekleyen ürün, süreç ve hizmetlerin belgelendirilmesine temel teşkil eden "Avrupa siber güvenlik sertifika şemalarını" hazırlamakla görevlendirilmiştir. Avrupa Siber Güvenlik Yasası, BİT ürünlerinin, işlemlerinin ve hizmetlerinin siber güvenlik sertifikasyonunu destekleyen işlemleri sunmaktadır. Özellikle, bu tür BT ürünlerinin, süreçlerinin ve hizmetlerinin siber güvenlik sertifikası için AB çapındaki kuralları ve Avrupa planlarını oluşturmaktadır.

ENISA'nın temel faaliyetleri alanları aşağıda maddeler halinde verilmiştir. Bunlar;

- Siber güvenlik ve bağımsız danışmanlık hizmetleri verme ve tavsiyelerde bulunma
- Politika oluşturma faaliyetleri ile uygulamayı destekleme
- ENISA'nın AB'deki operasyonel ekiplerle doğrudan işbirliği yaptığı "Hands On" çalışmalara destek verme
- AB Topluluklarını bir araya getirmek ve büyük, büyük ölçekli sınır ötesi siber güvenlik olaylarına verilen mücadeleyi koordine etmek

- Siber güvenlik faaliyetlerinin sertifikalandırılması yapısının oluşturulması gibi hususlardır.

Avrupa Siber Güvenlik Ajansı (ENISA), Avrupa Komisyonu tarafından koordine edilen ve Üye Devletler tarafından desteklenen Avrupa Siber Güvenlik Ayının (ECSM) başlamasına işaret ediyor. Bu kampanya, Avrupa genelinde vatandaşlara siber güvenlik konusundaki farkındalığı arttırmaya odaklanmaktadır. Bu etkinliğin logosu Şekil 2.7'de verilmiştir. Bilgi Güvenliği Derneğimizin düzenlediği, ISCTurkey etkinliği de bu ay kapsamında kabül edilmiş olan ve ENISA tarafından desteklenen bir etkinliktir.

Şekil 2.7. Siber Güvenlik Ayı Logosu

2.16. Değerlendirmeler

Bu bölümde, kişisel ve kurumsal bilgi güvenliğinin sağlanmasında önemli olan standartlar gözden geçirilmiş, kişisel ve kurumsal bilgi güvenliğinin sağlanmasında takip edilecek ulusal ve uluslararası standartlar kısaca özetlenmiştir. Yüksek seviyede bir bilgi güvenliğinin sağlanabilmesi için;

- bilgi güvenliği standartlarının bilinmesi, uygulanması, oluşturulan politikalar kapsamında denetlenmesi ve karşılaşılan olumsuzlukların giderilmesi gerekmektedir.
- standartlar çerçevesinde oluşturulacak politikaların üst yönetim tarafından desteklenmesi, tüm çalışanlar ve paydaşlar tarafından tavizsiz uygulanmalıdır.

- siber güvenliği sağlamanın dinamik bir süreç olduğunun farkında olunması ve oluşan risklerin yönetilmesi gereklidir.
- kurumların standartlara uyduğunu belgelendirmeleri, uluslararası alanda geçerli sertifikasyona sahip olmaları, yüksek seviyede bir farkındalığın oluşturulması için gereklidir.
- En zayıf halka kadar güvende olunacağı varsayımıyla hareket edilerek gerekli önlemlerin alınması gerektiği bilinmeli ve uygulanmalıdır.
- Özellikle bu bölümde açıklanan TSE 15408 Ortak Kriterler kapsamında hem ürünlerin sertifikalandırılması hem de sertifikalı ürün kullanılmasının özendirilmesinin de yerinde olacağı değerlendirilmektedir.

Sonuç olarak; standartlar yüksek seviyede bir güvenliği garanti etse de bazen standartlarında yetersiz kalabileceği, siber güvenliğe daha geniş bir perspektiften bakılması ve önlemlerinde ona göre alınması gerektiği de unutulmamalıdır.

Kaynaklar

[1] Ortak Kriterler Portalı, http://www.commoncriteriaportal.org

[2] CEN (European Committee for Standardization) kurumsal web sitesi: www.cen.eu

[3] CENELEC (European Committee for Electrotechnical Standardization) kurumsal web sitesi: www.cenelec.eu

[4] Türk Standardları Enstitüsü, kurumsal web sitesi: www.tse.org.tr

[5] S. Sagiroglu, Kişisel ve Kurumsal Bilgi Güvenliği Dersi, Ders Notları, 2018.

[6] https://www.beamteknoloji.com/wp-content/uploads/2014/10/ISO-IEC-15408-Ortak-Kriterler-Standardı-TanıtımV3.pdf

[7] ISO (International Standardization Organization) kurumsal web sitesi: www.iso.org

[8] IEEE Standartları, http://www.oaib.org.tr/tr/bilgi-merkezi-ihracat-belgeleri-urune-ozel-belgeler-aqap-belgesi.html

[9] IEEE Standartları, http://standards.ieee.org/develop/project/status.html

[10] IEEE Standartları, http://grouper.ieee.org/groups/2413/Intro-to-IEEE-P2413.pdf

[11] IEEE Standartları, http://standards.ieee.org/findstds/standard/21450-2010.html

[12] IEEE Standartları, http://standards.ieee.org/findstds/standard/2410-2015.html

[13] IEEE Standartları, http://standards.ieee.org/findstds/standard/802.1AE-2006.html

[14] IEEE Akıllı Şebekeler Standartları, http://smartgrid.ieee.org/resources/standards

[15] IEEE Standartları, https://standards.ieee.org

[16] S. Sagiroglu, M. Alkan, Her Yönüyle Elektronik İmza, Grafiker Yayınevi, 2005.

[17] NIST Siber Güvenlik Platformu, https://www.nist.gov/cyberframework

[18] Bilişim Teknolojileri Yönetim ve Denetim Enstitüsü Derneği http://isaca-ankara.org/

[19] Avrupa Siber Güvenlik Ajansı, https://www.enisa.europa.eu/about-enisa

[20] ITU Siber Güvenlik Faaliyetleri, https://www.itu.int/en/action/cybersecurity/Pages/default.aspx

[21] PCI Güvenlik Standartları Konseyi, https://tr.pcisecuritystandards.org/index.php

Bilgi, Ürün ve Sistem Açısından Siber Güvenlik Standartları

BÖLÜM 3

Atila BOSTAN
Gökhan ŞENGÜL

BİLGİ, ÜRÜN VE SİSTEM AÇISINDAN SİBER GÜVENLİK STANDARTLARI

Bu bölümde, siber güvenlikte alınan tedbirlerin ya da gerçekleştirilen uygulamaların seviyesini ve/veya kalitesini ölçmek için kullanılabilen ulusal ya da uluslararası standardizasyon kurumları tarafından yayınlanmış standartlar özetlenmiştir.

3.1. Giriş

İnsanoğlunun gelişimi ile birlikte birçok alanda mamuller, mahsuller, hizmetler ve metotlar geliştirilmeye başlamıştır. Zaman içerisinde farklı kişi, kuruluş ya da gruplarca geliştirilen bu olguların belirli bir düzene koyulabilmesi, ortak bir anlayış haline getirilebilmesi ve olgunun gerek işleyişinin gerekse de diğer kalite özelliklerinin ölçülebilmesi için bazı kriterlere ihtiyaç duyulmuştur. İşte bu bağlamda standart terimi ortaya çıkmış ve standardizasyon çalışmalarına ihtiyaç duyulmuştur.

Uluslararası Standardizasyon Teşkilatı (ISO) tarafından standartın tanımı "imalatta, anlayışta, ölçme ve deneyde bir örnekliliktir" olarak yapılmıştır [1]. Bir başka ifade ile standart, belirli bir ürün, süreç, yöntem ya da sistemin taşıması gereken asgari kurallar bütünüdür. Burada bahsedilen kurallar ürün, süreç, yöntem ya da sistemin fiziki özelliklerini içerebileceği gibi sistemin fonksiyonel özellikleri, kalitesi, işleyişi ya da emniyet ya da güvenliği ile ilgili de olabilir.

Standartlarda yer alan kuralları oluşturma süreci ise standardizasyon olarak adlandırılmaktadır. ISO tarafından yapılan tanımlamaya göre standardizasyon; belirli bir faaliyetle ilgili olarak tüm paydaşların katılımı ile kural koyma süreci olarak tanımlanmıştır [1]. Burada standartların hazırlanması sürecine tüm paydaşların katılımı hususu özellikle önemlidir. Standardizasyon süreci bu bağlamda tüm paydaşların katılımını gerektirdiği gibi aynı zamanda tüm paydaş-

ların standart kuralları üzerinde hemfikir olmasını da gerektirmektedir. Bu nedenden ötürü standardizasyon çalışmalarını koordine etmek ve standardizasyon çalışmalarına tüm paydaşların katılımını sağlayarak tarafsız bir anlayışla standartların hazırlanması için çeşitli standardizasyon kuruluşları kurulmuştur.

Dünya da standardizasyon çalışmalarını yürüten en önemli kuruluş Uluslararası Standardizasyon Teşkilatıdır (ISO). ISO 1946 yılında 25 ülkenin standardizasyon kuruluşlarının katılımıyla kurulmuş olup günümüzde 146 ülkenin üyesi olduğu uluslararası bağımsız bir standardizasyon teşkilatı olarak görevine devam etmektedir [1]. Ayrıca elektroteknik alanında standartları hazırlamak üzere Uluslararası Elektroteknik Komisyonu (IEC-International Electrotechnical Commission) da ISO ile birlikte çalışmaktadır. Avrupa Birliği'nde farklı konulardaki standart çalışmalarını koordine etmek üzere Avrupa Standardizasyon Komitesi (CEN: European Committe for Standardization) [2] ve Avrupa Elektroteknik Standardizasyon Komitesi (CENELEC–European Committee for Electrotechnical Standardization) [3] kuruluşları kurulmuştur. Her iki kuruluşa da 33 üye ülke bulunmaktadır.

Türkiye'de ise; 132 sayılı Kuruluş Kanunu ile her türlü madde ve mamuller ile usul ve hizmet standartlarının hazırlanması görevi Türk Standardları Enstitüsü'ne (TSE) verilmiştir [4]. TSE, uluslararası standardizasyon kuruluşları olan ISO ve IEC ile Avrupa standardizasyon kuruluşları CEN ve CENELEC'in tam üyesidir.

3.2. Siber Güvenlik ve Standartlar

Gelişen teknolojik ilerlemeler ve gelişmeler, siber güvenlik alanında hem yeni ürün ve süreçlerin hem de büyük miktarda değerli verinin üretilmesine sebep olmuştur. Bu bilgiler aynı zamanda kötü niyetli kullanıcıların hedefi haline gelmiş ve bu bilgilerin güvenli bir şekilde saklanması ve bilgilerin korunması için gerekli tedbirlerin alınması gerekliliği ortaya çıkmıştır. Ancak alınan tedbirlerin ne derecede yeterli olduğu/olacağı konusu ise her zaman tartışma konusudur. İşte bu aşamada ürün ve sistemlerin güvenliklerine yönelik alınan tedbirlerin hangi şartları sağlaması gerektiği ve bu şartların sağlanıp sağlanmadığını belirlemek üzere standardizasyon ve belgelendirme çalışmaları başlatılmıştır.

Diğer alanlarda olduğu gibi siber güvenlik alanındaki standartlar da ulusal ve uluslararası standardizasyon kuruluşlarının koordinesinde ve tüm paydaşların katılımları ile hazırlanmaktadır. Bu bölümde siber güvenlik alanında uluslararası standardizasyon kuruluşları ve ulusal standardizasyon kurumu olan TSE tarafından hazırlanan standartlar özetlenmiştir. Bu bölümde bahsedilecek standartların bir bölümü, doğrudan siber güvenlik ve bilgi güvenliği alanındaki ürün ve süreçlerin sahip olması gereken özellikleri açıklayan ve ürün ve süreçlerin belgelendirilmesinde (standarta uygunluğunun tescil edilmesinde) kullanılan standartlar iken bazıları ise daha çok ürün geliştirici ve son kullanıcılara kılavuzluk etmek üzere tasarlanmış kılavuz standartlardır.

Siber güvenlik alanı çok hızlı değişen bir alandır ve bu nedenle alandaki teknoloji ve ürünler çok hızlı bir şekilde değişime uğramaktadır. Bunun sonucu olarak da bu alanda yayınlanan standartların diğer sektörler için hazırlanmış standartlara göre çok daha hızlı güncellenebildiği unutulmamalıdır.

Bu çalışmada bilgi güvenliği ve siber güvenlik standartları aşağıda başlıkları verilen 3 temel kategoride gruplandırılmıştır. Bunlar:

- Sistem güvenliği standartları
- Ürün güvenliği standartları ve
- Bilgi güvenliği tetkik standartlarıdır.

3.2.1. Sistem Güvenliği Standartları

Sistem güvenliği standartları, kritik bilgilerin ve verilerin oluşturulduğu, işlendiği ya da saklandığı kurum ve kuruluşları tüm personeli, altyapısı, bilgi işleme olanakları ve sistemin işleyişi bağlamında bir bütün sistem olarak ele alan ve bilginin gizlilik, bütünlük ve erişebilirlik nitelikleri çerçevesinde alınması gereken güvenlik kontrollerini tanımlayan standartlardır. Sistem güvenliği ile ilgili yaygın olarak kullanılan standartlar aşağıda özetlenmiştir.

TS EN ISO/IEC 27001 Bilgi Teknolojileri - Güvenlik Teknikleri - Bilgi Güvenliği Yönetim Sistemi - Gereksinimler

Bilgi Güvenliği Yönetim Sistemi (BGYS) olarak ta bilinen bu standart ilk kez 2005 yılında yayınlanmış, sonrasında ise çeşitli reviz-

yonlardan geçirilmiş ve son yürürlükteki sürümü ise 2017 yılında yayınlanmıştır. Bu standart, bir kuruluş bünyesinde bilgi güvenliği yönetim sisteminin kurulması, uygulanması, sürdürülmesi ve gözden geçirilip iyileştirilmesi için uygulanması gereken prensip, şartlar ve kontrolleri kapsar. Burada ilgili prensip ve şartların belirlenmesi aşamasında kuruluşa özgü risklerin nasıl değerlendirip işleneceği de açıklanmaktadır. Standart oldukça genel bir yaklaşımla hazırlanmış olup tüm kuruluşlara uygulanabilirdir [5].

Bu standart birçok ülkede olduğu gibi ülkemizde de yaygın olarak bir belgelendirme standartı olarak kullanılmaktadır. Ülkemizde özellikle Elektronik Sertifika Hizmet Sağlayıcıları, Telekom operatörleri ve internet hizmet sağlayıcıları ve kişisel bilgilerin işlenip saklandığı Hastane Bilgi Yönetim Sistemi (HBYS) gibi alanlarda yazılım geliştiren yazılım firmaları gibi birçok firma/kuruluş bu standarta göre belgelendirilmiş durumdadır.

TS ISO/IEC 27002 Bilgi Teknolojileri - Güvenlik Teknikleri - Bilgi Güvenliği Yönetim Sistemi için Uygulama Prensipleri

Adından da anlaşılacağı üzere TS EN ISO/IEC 27002 standartı, bilgi güvenliği yönetim sistemlerinin uygulanması ile ilgili uygulama prensiplerini ve örneklerini içeren bir kılavuz standarttır. Bu bağlamda genel tavsiye niteliğinde bir standart olduğu söylenebilir. Standart kapsamında ilginin gizlilik, bütünlük ve erişilebilirlik özelliklerine yönelik riskleri karşılamak amacıyla bilgi güvenliğinin çeşitli alanlarına yönelik tavsiye niteliğinde bilgi güvenliği kontrolleri sunulmaktadır. Standartın özellikle ISO/IEC 27001 standartını esas alan bir Bilgi Güvenliği Yönetim Sistemi'ni kurmak isteyen kurum/kuruluşlar tarafından bir başvuru dokümanı olarak kullanılması tavsiye edilmektedir. Standart bir kılavuz standart olduğundan bu standart kapsamında belgelendirme çalışması yapılmamaktadır [6].

TS EN ISO/IEC 27005 Bilgi teknolojisi - Güvenlik teknikleri - Bilgi güvenliği Risk Yönetimi

Temel olarak TS ISO/IEC 27005, bilgi güvenliği risklerinin yönetimi için kılavuzluk sağlamak amacıyla hazırlanmış olup son sürümü

2018 yılında yayınlanmıştır. Bu standart ISO/IEC 27001 standartının genel kavramlarını destekleyecek şekilde hazırlanmış olup temel amacı bilgi güvenliğinin risk yönetimi tabanlı bir yaklaşım ile hayata geçirilmesini sağlamaktır. Bu bağlamda standartın ISO/IEC 27001 ve ISO/IEC 27002 standartları ile beraber ele alınması tavsiye edilmektedir [7]. Standart, TS ISO/IEC 31000 Bilgi teknolojisi - Güvenlik teknikleri - Risk Yönetimi standartından farklı olarak risk yönetimi yaklaşımı temelinde bilgi güvenliğinin uygulanmasını sağlar. Standart genel olarak hazırlanmış olup her türlü kuruluşa (kar amacı güden ticari işletmeler, devlet kurumları, kar amacı gütmeyen sivil toplum kuruluşları gibi) uygulanabilirdir.

Genel olarak incelendiğinde ISO/IEC 27001 serisi bir seri standart olup birbiri ile ilişkili birçok bölümden oluşmaktadır. Bu serinin temel amacı, kurum ve kuruluşlarda Bilgi Güvenliği Yönetim Sistemi'nin tasarlanması, uygulanması, kurulması, işletilmesi ve gözden geçirilmesi için dikkate alınması gereken zorunlu şartlar ile takip edilmesi gereken prensipleri içerir. Serinin önemli standartları yukarıda özetlenmiş olup tamamı burada verilmemiştir. Ayrıca serinin Bilgi Güvenliği Yönetim Sistemi Tetkikleri ile ilgili olan bölümleri tetkik standartları alt başlığı altında sunulmuştur.

3.2.2. Ürün Güvenliği Standartları

Ürün güvenliği standartları, bilgi teknolojileri ürünlerinin sağlaması gereken güvenlik özelliklerini belirleyen ve ürünün bu özellikleri taşıyıp taşımadığını ölçüp belgelendiren standartlardır. Burada bahsedilen ürün, bilgi üreten, işleyen ya da depolayan yazılım, donanım ya da hem yazılım hem de donanım içeren herhangi bir bilişim teknolojisi ürünü olabilir.

Her ne kadar bölümün alt başlığı ürün güvenliği standartları olsa ürün güvenliğine yönelik standart sayısı oldukça kısıtlıdır. Bu alanda değerlendirilebilecek uluslararası alanda kabul görmüş tek bir standart (Ortak kriterler standartı olarak da bilinen TS ISO/IEC 15408 serisi standart) ile ulusal bazda Türkiye'ye özgü Temel Seviye Güvenlik Belgelendirmesi bulunmaktadır. Bu standartların açıkları aşağıda sunulmuştur.

TS ISO/IEC 15408 1/2/3: 2005 - Bilgi teknolojisi - Güvenlik teknikleri - BT güvenliği için değerlendirme kriterler

Bilgi güvenliği ve siber güvenlik alanında ürün belgelendirmesi için kullanılan uluslararası kabul görmüş tek standart TS ISO/IEC 15408 serisi standartlardır. Bu standart serisi Ortak Kriterler standartı olarak da anılmaktadır. Serinin birinci bölümü giriş niteliğinde olup temel kavramlar ve Ortak Kriterler değerlendirme ve belgelendirme modelini içermektedir. Standartın ikinci bölümünde ürün güvenlik gereksinimleri belirlenirken kullanılacak güvenlik fonksiyonel gereksinimleri verilir. Üçüncü bölümünde ise ürünün iddia ettiği garanti iddiasının belirlenebilmesi için güvenlik garanti gereksinimleri yer almaktadır. Ortak kriterler kapsamında 7 farklı garanti seviyesi tanımlanmış olup bu garanti seviyeleri EAL (Evaluation Assurance Level) olarak ifade edilir. Burada birinci seviye en düşük garanti seviyesini, yedinci seviye ise en yüksek garanti seviyesini ifade eder [8].

Ortak Kriterler standartının yapısı gereği bir kurumun/kuruluşun Ortak Kriterler belgelendirme kuruluşu olabilmesi için Ortak Kriterler Konsorsiyonu tarafından bir dizi teste tabi tutulması ve bu testlerden başarı ile geçmesi gerekmektedir. Ülkemizde Türk Standardları Enstitüsü 2010 yılında bu testlerden başarı ile geçmiş ve belgelendirme kuruluşu olarak akredite edilmiştir. Bu kapsamda ülkemizde Ortak Kriterler belgelendirme çalışmaları Türk Standardları Enstitüsü tarafından yürütülmektedir.

Halihazırda Ortak Kriterler kapsamında erişim kontrol cihazları, veri tabanları ve veri koruma cihazları, akıllı kart sistemleri, ağ erişimi ile ilgili cihazlar vb alanlarda belgelendirme çalışmaları devam etmektedir.

Temel Seviye Güvenlik Belgelendirmesi

Ürün temelli tek uluslararası güvenlik belgelendirme standartı olan Ortak Kriterler standartının gerek değerlendirme sürecinin çok uzun ve zahmetli olması gerekse de belgelendirme maliyetlerinin çok yüksek olması nedeniyle daha hızlı ve efektif bir ulusal standarta ihtiyaç duyulmuştur. Bu kapsam Temel Seviye Güvenlik Belgelendirmesi (TSGB), ortak kriterlerin bir hafifletilmiş versiyonu ola-

rak Türk Standardları Enstitüsü tarafından geliştirilmiştir. TSGB, basit, hızlı ve etkin bir güvenlik değerlendirmesini hedefleyen bir değerlendirme programıdır [9].

TSGB, Ortak Kriterler standartında olduğu gibi ürünün güvenlik testlerinin yapılmasını ve elde edilen sonuçlara göre de belge verilip verilmemesi temeline dayanır. Burada güvenlik testleri bağımsız kuruluşlarca da yapılabilmekte, belgelendirme ise belgelendirme kuruluşu olan Türk Standardları Enstitüsü tarafından yapılmaktadır. TSGB'nin temel yaklaşımı, 35 adam-günde değerlendirmenin tamamlanması üzerine kurulmuştur.

3.2.3. Bilgi Güvenliği Tetkik Standartları

Bilgi güvenliği tetkik standartları, bilgi güvenliği tetkiklerine yönelik olarak Belgelendirme firmaları ve tetkikçiler tarafından uyulması gereken kuralları tanımlar ve kılavuzluk sağlar. Aşağıda bilgi güvenliği tetkikleri ile ilgili temel standartlar verilmiştir.

TS ISO/IEC 27006 Bilgi teknolojisi - Güvenlik teknikleri - Bilgi güvenliği yönetim sistemlerin tetkik ve belgelendirilmesini yapan kuruluşlar için şartlar

TS ISO/IEC 27006 ilk olarak 2007 yılında yayınlanmış ve sonrasında 2011 ve 2015 yıllarında revize edilerek güncellenmiştir. Bu standart, bağımsız BGYS tetkik ve belgelendirme hizmetleri veren kuruluşlar için gerekli olan şartları tanımlayarak bir kılavuzluk sağlar [10].

TS ISO/IEC 27007 Bilgi teknolojisi - Güvenlik teknikleri - Bilgi güvenliği yönetim sistemlerinin tetkiki için kılavuz

TS ISO/IEC 27007, TS ISO/IEC 27001 uyumluluğunun belgelendirilmesi dışında (bu husus TS ISO/IEC 27006 da kapsanmaktadır) farklı amaçlarla BGYS'lerinin tetkikini yapan kuruluşlar için kılavuzluk sağlar. Burada bahsedilen tetkikler, kurum içi tetkikler, dış tetkikler ya da yönetimin gözden geçirmeleri şeklinde olabilir. Ayrıca bu standart farklı büyüklükteki kuruluşlara uygulanabilir [11].

TS ISO/IEC 27008 Bilgi teknolojisi - Güvenlik teknikleri - Tetkikçiler için bilgi güvenliği kontrolleri kılavuzu

Tetkikçiler için bilgi güvenliği kontrollerinin denetiminin yapılması hazırlanmış kılavuz niteliğinde bir standarttır. 27008, bir kuruluş

tarafından uygulanan BGYS bağlamında teknik uyumun kontrolü de dâhil olmak üzere bilgi güvenliği kontrollerinin gözden geçirilmesi konularına odaklanır [12].

3.3. Sektörde Kullanılan Diğer Siber Güvenlik Standartları ve Yayımcı Kuruluşlar

Standart No.	Yayımcı kuruluş ve standartın açıklaması
NIST 800-53/SCF	ABD Ulusal Standartlar ve Teknoloji Enstitüsü (NIST)'nün 800-53 özel yayını, merkezi yönetim (federal) bilgi sistemleri için kontrolleri belirlemekle beraber, bu kontroller ticari birimler tarafından da kullanılabilmektedir. Merkezi yönetimin diğer bilgi güvenliği standartları ile uyumludur. Ücretsiz bir standartdır.
CIS 20	İnternet Güvenlik Merkezi (CIS) isimli kurum tarafından takip edilen ve orijinali SANS enstitüsü tarafından geliştirilmiş 20 adet güvenlik kontrolünü içermektedir. Ücretsiz bir standarttır.
ISACA-COBIT 5	Bilgi Sistemleri Denetleme ve Kontrol Ortaklığı (ISACA) kurumu tarafından düzenlenen Bilgi ve İlgili Teknolojiler Kontrol Hedefleri (COBIT) çerçevesi, siber güvenliğin tesisi için kontrol ve işlemleri de içermektedir. ISO 27000 serisi ve ISACA- Bilgi Güvenliği için İş Modeli (BMIS) standartları ile uyumludur. Standart ücretlidir.
ISF- Standard of Good Practice	Bilgi Güvenliği Formu (ISF)'nun düzenlemiş olduğu İyi Örnekler Standartı, mevcut ve gelişmekte olan teknoloji konularında kontrol yöntemleri ve rehberlik sağlamaktadır. Standart ve beraberindeki ISF Kıyaslamalı Ölçüm sistemi, ISO 27002, COBIT 5, CIS 20, NIS ve PCI-DSS standartları ile uyumludur. Dağıtım ve yayınlanması kontrollü, ücretsiz bir standarttır.
DISA	Savunma Bilgi Güvenliği Ajansı (DISA), Kontrol İlişki Göstergeleri (CCI), Güvenlik İhtiyaçları Rehberi (SRGs), Güvenlik Teknik Uygulama Rehberi (STIGs) ve mobil kodlama konularında güvenlik standartları yayımlamaktadır.

ITIL	Axelos firması tarafından geliştirilen, Bilgi Güvenliği Altyapısı Kütüphanesi (ITIL), ISO 27000 serisi ile uyumlu olarak, Bilgi Teknolojileri hizmet yönetimi düzenlemelerini içermektedir. Standart ücretlidir.
PCI-DSS	Büyük kredi kat firmalarının oluşturduğu, Ödeme Kartları Endüstrisi (PCI) kurumu güvenlik konseyinin Veri Güvenlik Standartı (DSS), kart işlemlerinin güvenliğini artırmak amacıyla politika ve işlemleri belirlemektedir. Uyumluluk kredi kartı firmaları tarafından zorunlu tutulmaktadır. Bazı ülke kanunları bu standarta referans vermekte veya standarttan alıntılar yapmıştır. Standart ücretsizdir.
OWASP	Açıl Web Uygulama Güvenliği Projesi (OWASP), OWASP ilk 10 listesini de içeren güvenlik artırıcı kaynakların kullanılmasını önermektedir. OWASP ilk 10 ücretsizdir.
BSIMM	Olgunluk Modelinde Güvenlik Tesisi (BSIMM) projesinde üretilen düzenleme, yazılım güvenliğine odaklanmıştır ve ticari kurum güvenlik inisiyatiflerini ölçme ve yönetmede yardımcı olan faaliyetlerin düzenlenmesinde kullanılan çerçeveyi tanımlamaktadır. Ücretsiz bir standarttır.
CSA- SGCAFCC 4.0	Bulut Güvenlik Birlikteliği (CSA) tarafından, bulut hesaplama teknolojilerinin benimsenmesi, güvenliğin artırılması ve risklerin yönetilmesi amacıyla Bulut Güvenliğine Odaklı Kritik Alan Güvenlik Rehberi (SGCAFCC) 4.0 yayımlanmıştır. Bu standart ücretsizdir.
CSA- CCM	Bulut Güvenlik Birlikteliği (CSA) tarafından yayımlanan Bulut Kontrol Matrisi (CCM) bulut listelerini kullanan organizasyonların bilgi güvenliğini en üst seviyeye çıkarması için yapılması gerekenleri içerir. Bu standart ücretsizdir.

ILTA	Uluslararası Hukuk Teknoloji Ortaklığı (ILTA) tarafından yayımlanan Hukuk Güvenliği (LegSEC) düzenlemesi, hukuk alanında risk-tabanlı bilgi güveliği programları için tavsiyeler içermektedir. Ücretsiz olarak bazı araçlara da bu ortaklık aracılığı ile erişmek mümkündür.
PAS 555	İngiliz Standartlar Enstitüsü (BSI) tarafından yayımlanan, Açık Erişim Tanımlamaları 555, üst seviye yöneticileri için kurumlarının siber güvenlik yetkinliklerinin karşılaştırılmasına imkan veren bir çerçevedir. Standart ücretlidir.

3.4. Değerlendirmeler

Bu bölümde siber güvenlik ve bilgi güvenliği ile ilgili gerek ulusal gerekse de uluslararası standartlar özetlenmiş, genel olarak kullanım alanları açıklanmıştır. Burada öncelikli olarak tüm standartlar için geçerli olan bir hususu belirtmekte fayda görülmektedir. Hazırlanan tüm standartlar ihtiyari nitelikte olup herhangi bir kurum/kuruluşça zorunlu kılınmadıkça belgelendirme ihtiyacı doğmayacaktır. Bu bağlamda bu standartların yayınlanmış olması sektörün ve son kullanıcıların ihtiyaçlarını karşılamamaktadır. Son kullanıcıların bilgi güvenliği anlamında mağdur edilmemesi için ilgili yasal otoritelerce bu standartların zorunlu hale getirilmesi ve belgelendirme süreçlerinden geçemeyen ürünlerin/sistemlerin piyasaya sürülememesi büyük önem arz etmektedir.

Siber güvenlik ve bilgi güvenliği standartları ile ilgili ikinci temel husus ise teknolojideki hızlı değişimler sonucu bu standartların içeriklerinin ve kullanım alanlarının hızla değişiyor olmasıdır. Standartların tarihçeleri incelendiğinde bu standartların birkaç yılda bir revize edildikleri görülmektedir. Son kullanıcıların ve ürünleri için standartları takip eden kuruluşların standartların son versiyonlarını ve hatta standart üzerinde revizyon çalışmalarının yapılıp yapılmadığını takip etmeleri önemle tavsiye edilmektedir.

Kaynaklar

[1] ISO (International Standardization Organization), www. iso.org.

[2] CEN (European Committee for Standardization), www.cen.eu

[3] CENELEC (European Committee for Electrotechnical Standardization), www.cenelec.eu

[4] Türk Standardları Enstitüsü Web Sayfası, www.tse.org.tr

[5] TS ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi Standardı, "https://www.tse.org.tr/IcerikDetay?ID=2311" adresinden 29.01.2019 tarihinde erişilmiştir.

[6] TS EN ISO/IEC 27002 Standardı, "https://intweb.tse.org.tr/Standard/Standard/StandardAra.aspx" adresinden 29.01.2019 tarihinde erişilmiştir. (TS No: alanına "TS EN ISO/IEC 27002" girilmelidir.)

[7] TS ISO/IEC 27005 standardı, "https://intweb.tse.org.tr/Standard/ Standard/StandardAra.aspx" adresinden 29.01.2019 tarihinde erişilmiştir. (TS No: alanına "TS ISO/IEC 27005" girilmelidir.)

[8] Ortak Kriterler Standardı serisi, "https://www.tse.org.tr/IcerikDetay?ID=950&ParentID=3295" internet adresinden 29.01.2019 tarihinde erişilmiştir.

[9] Temel Seviye Güvenlik Belgelendirmesi, https://www.tse.org.tr/IcerikDetay?ID=2061&ParentID=3312 internet adresinden, 29.01.2019 tarihinde erişilmiştir.

[10] TS ISO/IEC 27006 Standardı, "https://intweb.tse.org.tr/Standard/Standard/StandardAra.aspx" adresinden 29.01.2019 tarihinde erişilmiştir. (TS No: alanına "TS ISO/IEC 27006" girilmelidir.)

[11] TS ISO/IEC 27007:2011 Standardı, "https://intweb.tse.org.tr/Standard/ Standard/StandardAra.aspx" adresinden 29.01.2019 tarihinde erişilmiştir. (TS No: alanına "TS ISO/IEC 27007" girilmelidir.)

[12] TSE ISO/IEC TR 27008 Standardı, "https://intweb.tse.org.tr/Standard/Standard/StandardAra.aspx" adresinden 29.01.2019 tarihinde erişilmiştir. (TS No: alanına "TSE ISO/IEC TR 27008" girilmelidir.)

Siber Güvenlikte Askeri Standartlar Kapsamında AQAP İncelemesi

BÖLÜM 4

Seda YILMAZ

SİBER GÜVENLİKTE ASKERİ STANDARTLAR KAPSAMINDA AQAP İNCELEMESİ

Bu bölümde, savunma sistemlerindeki ürün/hizmetlerin ortak kalite standartlarını belirleyen Kuzey Atlantik Paktı'nın (NATO), müttefikleri için belirlediği standartlar ele alınacaktır. Bu standartlar ele alınırken en temel standartlar özetlenmiş, savunma sistemlerinin temelinde yer alan yazılım ürünleri/hizmetleri özelinde standartlar açıklanmıştır.

4.1. Giriş

Bilgi teknolojileri (BT) en temelde, dünyanın hemen her ülkesinde askeri amaçlı çalışmaların katkısı ve ihtiyaçlarıyla şekillenmiş, şekillenmeye de devam etmektedir. Ülkelerin, varlıklarını sürdürme ve savunma kaygıları arttıkça BT'ne yönelik yatırımları artmış ve giderek büyüyen siber dünya, yeni bir cazibe merkezi haline dönüşmüştür. Bu durumun doğal sonucu olarak siber dünyada da ülkelerin güvenliklerini sağlama gereksinimi ortaya çıkmıştır. İlgili gereksinimlerin karşılanmasındaki temel nokta, BT ürünlerinin bir standardizasyona sahip olmasıdır.

Mevcut endüstriyel standartlar, askeri alanda kullanılan BT ürünlerinin doğası gereği standardizasyon ihtiyacını karşılamakta maalesef yetersiz kalmaktadır. Başta Amerika Birleşik Devletleri (ABD), Avrupa Birliği (AB) ve NATO (North Atlantic Treaty Organization-Kuzey Atlantik Paktı) olmak üzere Dünya'nın önde gelen ülkeleri ve toplulukları siber güvenliğin ortak standartları konusunda henüz bir fikir birliğine varamamış olsalar da stratejiler yayınlayarak ve anlaşmalar yaparak temel bir yaklaşım belirlemeye çalışmaktadırlar.

Standardizasyon, "belirli bir çalışmanın, o çalışma ile ilgili bulunanların ve özellikle milli ekonominin yararına yapılabilmesi için tüm

tarafların katkı ve işbirliği ile belirli kurallar koyma ve bu kuralları uygulama işlemi" olarak tanımlanabilmektedir. Standart ise standardizasyonun oluşturulabilmesi için konunun somut örneklerini ifade etmekte olup herhangi bir özellik belirtiyor ise bu özelliğin deney metotlarının sağlanabildiğini göstermelidir [1].

Standardizasyonun tarihine bakıldığında, temelinin el sanatları kuralları, örf ve ananelere dayandığı görülmektedir. Modern anlamıyla standardizasyona en yakın örnekleri M.Ö.4500'lü yıllarda Mısır'da görmek mümkündür. Piramitlerin inşaatında kullanılan taşların boyutlarının belirlenmesinde birtakım kuralların uygulandığı yapılan çalışmalarla tespit edilmiştir. Benzer şekilde Eski Roma'da su kanallarından alınan vergilerin belirlenmesinde su kanallarının çapının kullanılarak hesaplamalarda bir standart oluşturulduğu tespit edilmiştir. Endüstriyel alandaki standardizasyonun temeli ise İngiltere sanayi devrimine dayanmaktadır [1].

Türklerin Anadolu'da bilinen ilk standardizasyon uygulaması, 1502 yılında Sultan II. Beyazıt tarafından Bursa'daki ticaretin usulünü düzenleyen ferman kabul edilmektedir. Ferman, satılan/işlenen ürünün hammaddesi, ebatları, paketleme ve fiyatlandırma gibi bileşenlerine dair esasları ve bu esaslara uyulmadığı durumdaki uygulanacak cezai yaptırımları içermekle birlikte güncel anlamda standardizasyon esaslarının dünyadaki ilk örnekleri arasındadır [2].

Ülkeler arasında sürekli bir etkileşim olması paylaşılan her unsurun bir standarda sahip olmasını zorunlu kılmaktadır. Ayrıca ülke içinde de genel kalitenin ve düzenin sağlanmasında standartların belirlenmesinin önemi büyüktür.

4.2. AQAP (Müttefik Kalite Güvence Yayınları - The Allied Quality Assurance Publications)

Kuzey Atlantik Paktı (North Atlantic Treaty Organization) olarak ifade edilen NATO'nun amacı, müttefik ülkeler arasında askeri işbirliği ve savunmayı sağlamaktır. Bu kapsamda müttefikler arasında kullanılan her türlü savunma sanayi ürün ve hizmetlerinin ortak standartlara sahip olması ülkeler arası işbirliğinin sağlanması için bir zorunluluktur. Savunma sistemlerinin kritik yapısı ve ihtiyaçlarının yapısal durumları nedeniyle Uluslararası Kalite Standartları

tarafından ortak standartların karşılanması şu an için çok mümkün görünmemekle beraber ISO-9000 ve DoD (Department of Defence - DoD) alanındaki gelişmeler gelecekte bu durumun büyük ölçüde değişeceğine işaret etmektedir.

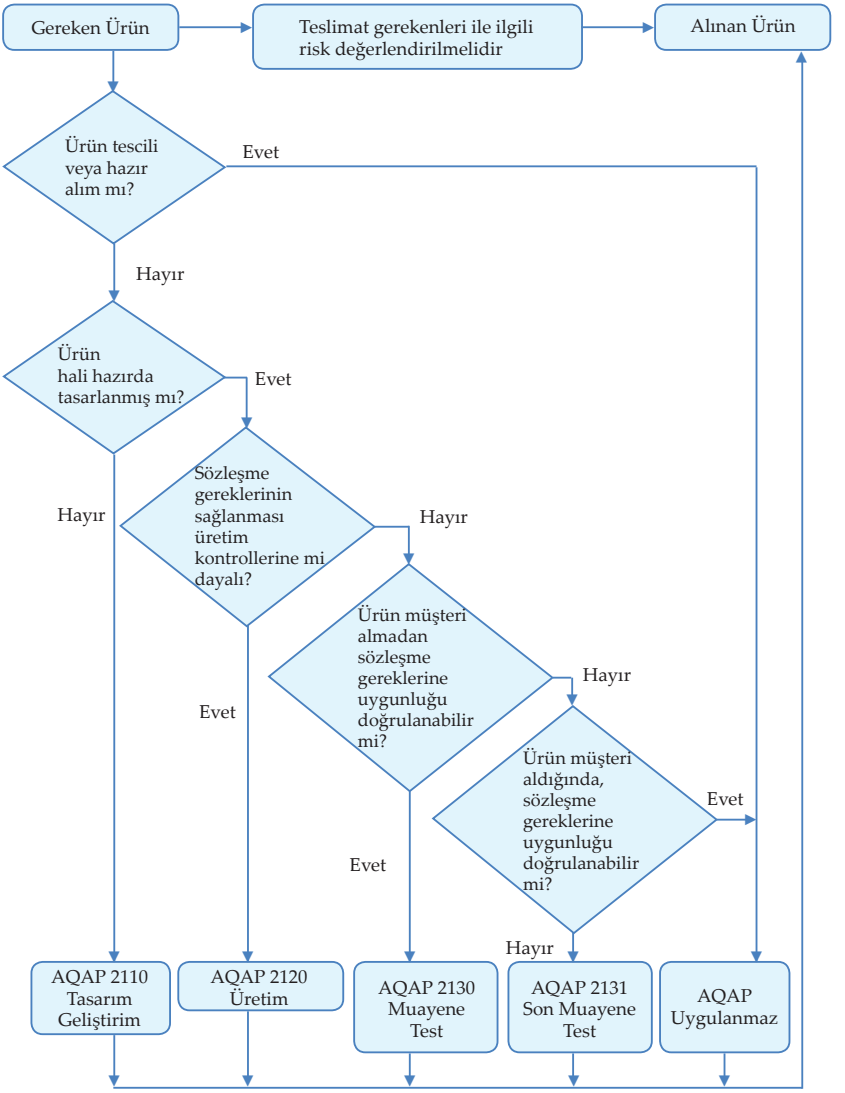
Müttefik Kalite Güvence Yayınları (The Allied Quality Assurance Publications-AQAP), 1968'de NATO üyesi ülkeler için askeri alandaki sistemlere yönelik kalite standartları olarak ortaya çıkmıştır. Savunma sistemlerinde kullanılan bütün yazılım ve donanım ürünleri ile üretim süreçlerine yönelik kalite yönetim politikalarını içermektedir. Temeli STANAG 4108 NATO standardizasyon anlaşmasına dayanmakta olup ABD Savunma Bakanlığı tarafından belirlenen standartlar ile uyumludur [3]. 1990'lı yıllardan sonra ISO-9000 serisindeki gelişmelerin ardından AQAP'lar 1993 yılından itibaren ISO-9000 serisi ile uyumlu hale getirilmiştir [7].

Ülkemizde 5201 sayılı kanun gereğince Milli Savunma Bakanlığı (MSB) tarafından belirlenen "Kontrole Tâbi Tutulacak Harp Araç ve Gereçleri ile Silâh, Mühimmat ve Bunlara Ait Yedek Parçalar, Askerî Patlayıcı Maddeler, Bunlara Ait Teknolojilere İlişkin Liste" dokümanı kapsamında üretim yapan ve/veya tedarik süreci yürüten firmaların, AQAP belgesinin olması zorunludur. Bu yayının yayınlandığı dönemde, firmanın ilgili standardı sağlayıp sağlamadığı MSB tarafından kontrol edilerek belgelendirilmektedir [4].

4.3. Ülkemizdeki Etkin Kullanılan AQAP'lar

Bu bölümde MSB tarafından, savunma sistemlerine ürün/hizmet üreten firmalardan talep edilen AQAP'lar ile temel referanslar arasında yer alan AQAP'lar incelenmiştir.

AQAP'lar diğer standartların aksine, ürün/hizmetin belirli bir aşamasındaki eksikliğin tespiti ve iyileştirilmesine yöneliktir. Genel olarak mevcut yapının standardize edilmesini değil ilgili aşamanın standardizasyonunu içerir. Bu şekliyle farklı alanlara hitap eden savunma sanayi ürün/hizmetlerinin modüler yapısı ile uyum sağlamaktadır. Firmanın hangi belgelendirmeye ihtiyacının olduğu belirlenirken tedarik edilecek ürün/hizmetin içeriği ve/veya firmanın genel yapısı incelenerek karar verilir. Şekil 4.1'de bu belirlemenin yapılmasında temel alınabilecek bir yol haritası verilmiştir [12].



Şekil 4.1. AQAP uygunluk belirleme şeması [12]

4.3.1. AQAP-110 NATO Tasarım, Geliştirme ve Üretim Kalite Güvencesi Koşulları

AQAP-110 dökümanı, tasarım, geliştirme ve üretim tabanlı standartları içerir. AQAP-1 standartları, ISO 9000 serisi ile uyumlu hale getirilme çalışmaları kapsamında AQAP-110 olarak değiştirilmiştir [7]. İlk olarak 1993 yılında yayınlanan standardın 1995 yılında

ikinci versiyonu (V.2) yayınlanmıştır. Hali hazırda V.2 referans alınmaktadır. Belgenin içeriği, genel olarak üretici ve yüklenicinin yerine getirmesi gereken şartları içermekte olup ISO 9001 standartlarına ek olarak NATO eklerine yer vermektedir. Bu koşulların genel hatları [5]:

- Üretim yapan endüstriyel şirketin, ürününden maksimum fayda sağlanması için üretimin her aşamasında planlama, kontrol, denetim ve güvence faaliyetlerine kalite yönetim süreçlerini izlemesi gerekmektedir.
- Yüklenici, sözleşmenin hüküm ve şartları ile geçerli şartnamedeki yükümlülükleri yerine getirmekten sorumlu olup bu şartlara uygunluk objektif bulgularla kontrol edilir.
- Yüklenicinin korunması için yüklenici tarafından gerekli kalite güvence koşullarının sağlanıp sağlanmadığı ihtiyaç duyulduğunda Devlet Kalite Güvencesi Temsilcisince kontrol edilir.
- Alıcı veya yetkili temsilcinin, ürünün istenen şartları sağlamaması durumunda süreci durdurma veya onaylamama yetkisi bulunmaktadır.

4.3.2. AQAP-120 NATO Üretim Kalite Güvencesi Koşulları

ISO 9000 serisi ile uyumlu olup üretim ve hizmet koşullarına yönelik standartları içerir. 1995 yılında ikinci versiyonu (V.2) yayınlanmış ve hali hazırda bu sürüm geçerliliğini korumaktadır. Üretim sürecinde uyulması gereken ISO 9002 standartlarına ek olarak NATO eklerine yer vermektedir. Bunlar [6]:

- Ana yüklenici, alt yüklenicileri de kapsamak üzere tasarım sürecinin ilk aşamasından itibaren bir konfigürasyon yönetim sistemi oluşturmalı ve bütün süreç bu sistemin uygun sürdürüldüğünden emin olmalıdır. Bu sistemin konfigürasyon tanımlaması, kontrolü, durum muhasebesi ve denetim prosedürleri belgelendirilmedir.
- Devlet Kalite Güvencesi Temsilcisine yüklenici tarafından gerekli konaklama ve inceleme şartları sağlanmalıdır. Kalite Güvence Temsilcisi, yüklenci ve/veya alt yüklenici tesislerinde tam erişim hakkına sahip olup sistemin prosedürlere uygunluğunu değer-

lendirmek ve ürünü sözleşme şartlarına uygunluğunu kontrol için sınırsız yetkiye sahiptir.

4.3.3. AQAP-130 NATO Muayene ve Test Kalite Güvencesi Koşulları

ISO 9003 Kalite Güvence Modeli ile uyumlu olup muayene ve test koşullarına yönelik standartları içerir [7].

4.3.4. AQAP-150 NATO Yazılım Geliştirme Kalite Güvencesi Koşulları

Savunma sistemlerinin kapsamında yer alan silah sistemleri, askeri iletişim sistemleri, ağ sistem ürünleri ve komuta-kontrol sistemleri gibi kritik ve karmaşık yapılarda kullanılan yazılımların güvenliği, askeri alandaki siber güvenliğin sağlanmasındaki en önemli unsurlardan biridir. Bu noktalardaki açıkların sonuçları maalesef ülke savunmasını doğrudan etkileyebilmektedir. Yazılımlardaki kalite eksikliklerinden kaynaklı olası problemlerin azaltılması ve önüne geçilmesi maksadıyla NATO üyesi ülkeler için yazılım kalite güvence standartları, AQAP-150 ile belirlenmektedir (Geçerli son versiyon 1997 yılında yayınlanmıştır). AQAP-150, AQAP-110 ve ISO/IEC 9126 standartlarını referans almakta ve AQAP-110 'a yazılım projeleri için ek gereksinimleri sağlamaktadır [8].

AQAP-150, yazılım projesinin genel yapısını hedef almaktadır. Herhangi bir yazılım geliştirme modeli ya da yöntemi önermemekte ve proje odaklı yönetimsel/teknik süreçleri ele almaktadır. Yazılım projesindeki her türlü yazılım geliştirme durumları, teslim edilmeyen ve ürün geliştirme aşamasında kullanılan yazılımlar, raf dışı yazılımlar, güvenlik duvarı yazılımları ile bakım/idame süreçleri de dâhil olmak üzere yazılım projesinin bütün unsurlarında uygulanması ön görülmüştür. Temelde, Yazılım Yaşam Döngüsü boyunca devam edecek bir Yazılım Kalite Sistemi (YKS) oluştulmasını, bu süreç adımlarının teslim ve bakım/idameyi de kapsayacak şekilde düzenlenmesini içerir. Standardın genel yapısı ve adımları [8]:

- (YKS), program yaşam döngüsü boyunca uygulanacak bir dizi kural ve prosedürleri içermekte olup olası riskleri en aza indirmeyi hedeflemektedir. Ayrıca sürecin kalite yönetimine uygun olarak tasarlanıp yürütüldüğünün kontrolünü sağlamaktadır.

- Yazılım Kalite Yönetim Faaliyetleri (YKYF), sözleşme şartları, YKS'nin kural ve prosedürleri ile özel proje gereksinimlerine dayanır. Bu faaliyetler;
  - Yazılım ürün ve ögelerinin gereksinimlerini tespit etmeyi
  - Geliştirme için yönetsel ve teknik süreçleri oluşturmayı ve uygulamayı
  - Ürünün kalitesinin tespiti ve onaylanması için ilgili prosedürlerin belirlenmesi ve uygulanmasını sağlamayı
  - Projeye dair potansiyel teknik, mali ve programsal risklerin tespit, analiz, önceliklendirme ve en aza indirilme / ortadan kaldırılması için prosedürleri belirlemeyi içeren eylemler ve yöntemler dizisi olarak tanımlanmaktadır.
- Yazılım Projesi Kalite Planı (YPKP), YKYF'lerini belgelendirmek için oluşturulmaktadır. Bu plan, yüklenici tarafından kalite sisteminin takip ve kontrolü için geliştirilen faaliyetlerin tanımlanması için kullanılmalıdır.
- Yazılım gereksinimleri, YPKP'ında yazılım geliştirme sürecinin başlangıç adımı olarak yer almaktadır. Bu gereksinimler alıcı tarafından da onaylanarak şartnameye dâhil edilmeli ve tasarım kısıtlamaları ile temel yazılım kalite özelliklerinin açık tanımlarını ifade etmelidir. Ayrıca YPKP'ında da gereksinimlerin formatı, içeriği, hangi standartları veya kılavuzların uygulanacağı net bir şekilde belirtilmelidir.
- Yazılım geliştirme süreci için;
  - Sürecin karmaşıklığını azaltacak ve kontrolü sağlayacak şeffaflığa sahip
  - Bilinen mühendislik uygulamalarını içeren
  - Önceki tasarımların geri bildirimlerine göre düzenlenmiş
  - Faaliyet adımlarını ve olası sonuçlarını açık bir şekilde belirten
  - Kritik görevlerin tanımlarının yapıldığı
  - Doğrulama kontrolünün yapılacağı noktaların kronolojik olarak tanımlandığı

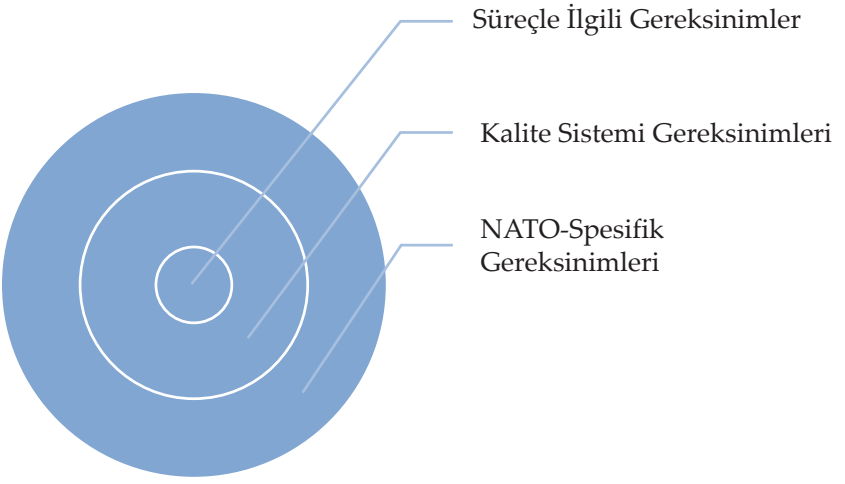
- Plan dışı durumların kontrol edilme adımlarını içeren
- Süreçlere dair başlangıç ve bitiş kriterlerinin belirsizliğini kaldıran
- Projeye özgü tüm kalite foksiyonlarının net ifade ve tahsis edildiği
- Doğrulanabilir ve nitel analitik kalite ölçümlerine sahip
- Geliştirme sürecinin etkinliği için kaliteli veri sağlayabilen
- Yazılım mühendisliği faaliyetlerinin planlama ve izleme etkinliğini içeren
- Geliştirme sürecine dâhil personelin hatalarından kaynaklı risklerin azaltılması ve tekrar eden faaliyetlerin kontrolü için bilgisayar kaynaklarının kullanımını içeren bir model oluşturulmalıdır.

- Sürecin kalitesini etkileyen faaliyetleri planlayan, yöneten, gerçekleştiren ve kontrol eden grupların, sorumlulukları, yetkileri ve unsurları ile grupların birbirleri ile ilişkileri net olarak tanımlanmalıdır. Yazılım ürünün bütünlüğü ve izlenebilirliği, kontrolsüz değişiklikleri önleyerek doğrulama, izleme ve kontrol için ön koşul olarak planlanmış ve yayınlanmış faaliyetleri içeren Yazılım Yapılandırma Yönetimi (YYY) tanımlanmalıdır. Ayrıca her bir sürece ait tüm verilerin kalite kayıtları tutularak proje dökümantasyonu yapılmalıdır.
- Yazılım geliştirme ve/veya bakım idame faaliyetleri için bilinmiş yazılım mühendisliği yöntem ve araçları kullanılmalıdır.

4.3.5. AQAP-160 NATO Yazılım Ömür Devri Boyunca Birleştirilmiş Kalite Gereksinimleri

Yazılım kalite yönetim sisteminin gereksinimlerinin belirlenmesi ve yürütülmesi esaslarını içermektedir. Yazılım yaşam döngüsü için bir çerçeve oluşturmayı hedeflemektedir. Daha çok ISO 9001:2000 ve ISO/IEC 12207 yi temel almaktadır. Kalite belgesinin modeli 3 aşamalı süreçten oluşmaktadır. Süreçler aşağıda açıklanmış ve Şekil 4.2'de gösterilmiştir [9]:

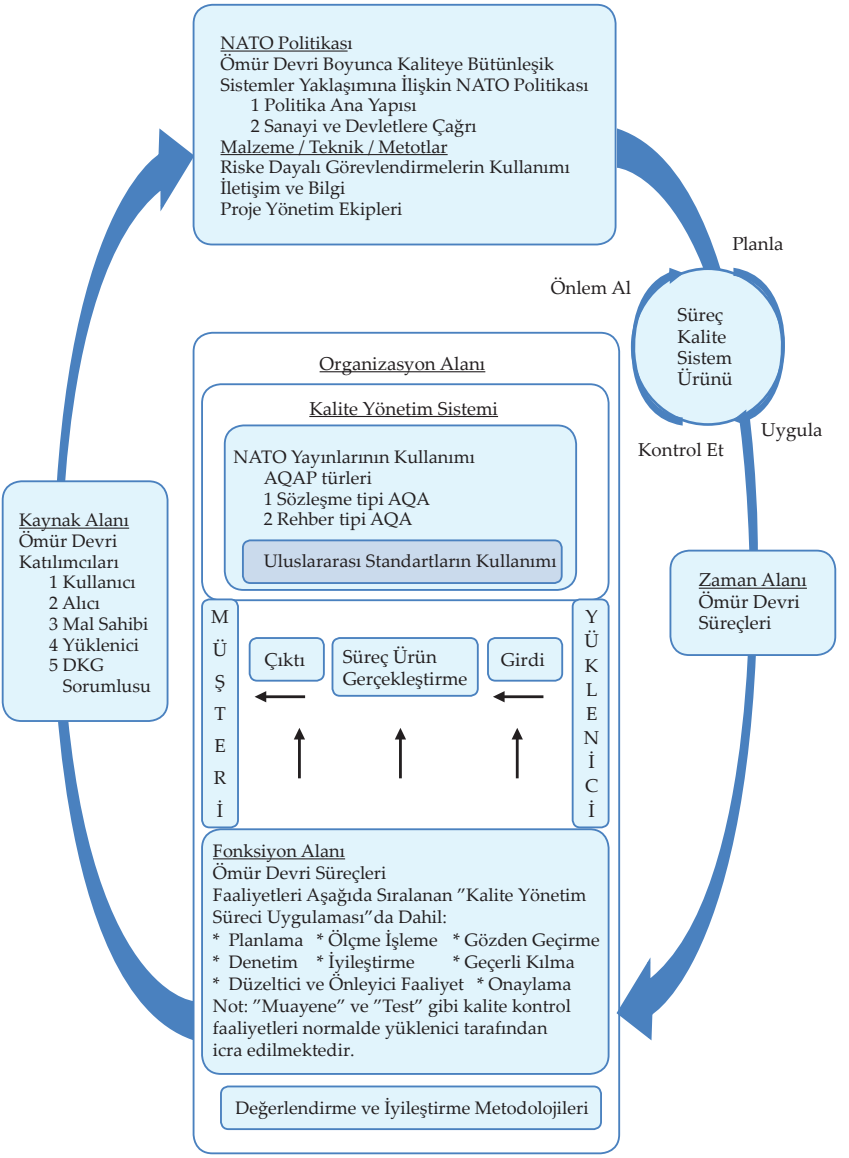
- Süreçle İlgili Gereksinimler: ISO 9001:1994/ISO 9001:2000 gereksinimlerini temel alarak savunma sanayi ile ilgili ilave hususları içerir. Ayrıca ISO/IEC 12007'de açıkça belirtilmeyen hususları ele alır.
- Kalite Sistemi Gereksinimleri: ISO 9001:1994/ISO 9001:2000'e dayalı tedarikçiye yüklenen organizasyonel gereksinim ve destekleyicileri içerir.
- NATO-Spesifik Gereksinimleri: Tedariğin NATO üyesi bir ülke için yapılmasından doğan NATO temel gereksinimlerini içerir.



Şekil 4.2. AQAP-160 modeli [9]

4.3.6. AQAP-2000 Ömür Devri Boyunca Kaliteye Bütünleşik Sistemler Yaklaşımına İlişkin NATO Politikası

Yazılım, donanım, tesis, insan ve temel süreçlerden oluşan savunma sistemlerinin kalite yönetimine yönelik teknik ve idari yaklaşımları içerir. En geniş kapsamlı politikalardandır. Politikanın etkinlik alanları ve bileşenler arasındaki bağlantıları birbirini takip eden ürün yaşam süresi döngüsüne sahiptir. Bu döngü Şekil 4.3'de gösterilmiştir [10].



Şekil 4.3. AQAP-2000 serisi etkinlik alanları ve bileşenler arası bağlantılar [10].

AQAP-2000 serisinin politikası 5 ana unsurdan oluşmaktadır. Bu unsurlar [10]:

- Her kuruluş hedeflerinin belirlenmesi ve bu hedeflere ulaşılması için süreç oluşum, yönetim ve yürütme politikasına sahip olmalıdır.

- Sistem içindeki bütün disiplinler uyumlu olmalıdır.
- Tarafların ihtiyaçları, uygun fonksiyonel ve teknik gerekliliklere dönüştürülebilmelidir.
- Sistemin devamlılığı için ortak altyapı ve terminoloji oluşturulmalıdır.
- Faaliyetler süreklilik arz etmelidir.

AQAP-2000 politikasının 5 temel unsurunun gerçekleştirilmesinde aşağıdaki başlıklar doğrultusunda hareket edilmektedir [10]:

- Ömür Devri Safhaları: Başlangıçtan teslime kadar her bir durum safhalara bölünerek kontrol edilir.
- Ömür Devri Süreçleri: Her bir organizasyonun etkin ve ekonomik süreçleri olmalı, bu süreçler dokümante edilmeli, idamesi ve iyileştirilmesi sağlanmalıdır. Bu kapsamda uygulanan kalite yönetim süreci, planlama, gözden geçirme, tetkik, ölçüm ve izleme, onaylama, düzeltici ve önleyici faaliyetleri içerir.
- Ömür Devri Katılımcıları: Ömür devri boyunca süreçler ve bunlarla ilgili işlemlere katılan her bir katılımcıyı ifade eder. Kalite, ortak bir sorumluluk olduğu için tek bir paydaşın değil bütünün (kullanıcı, alıcı, mal sahibi, yüklenici, kaliteden sorumlu personel) yüklenmesi gereken bir yükümlülüktür.
- Riske Dayalı Görevlendirme Kullanımı: Devlet Kalite Güvence personeli tarafından proje ekibinin bulunduğu tesis ve yüklenicinin sağladığı kalite yönetim sistemi kontrol edilmelidir.
- İletişim ve Bilgi: Ömür devrinin her safhasında gerek sonradan çıkacak sorunların önüne geçilmesi gerekse maliyet analizinin sağlıklı yapılabilmesi için bütün paydaşların paylaşımında bulunması önemlidir.
- Proje Yönetim Ekipleri: Kalite yönetim yaklaşımının sağlıkla yürütülmesi, projenin amaç ve performans hedeflerinin karşılanma durumunun takibi ve ortak yaklaşımların oluşturulabilmesi için en erken safhada proje yönetim ekipleri oluşturulmalıdır.
- Kalite Yönetim Sistemi: Maksimum etkinliğe ulaşmak için tüm katılımcıların, etkin ve ekonomik bir kalite yönetim sistemini

oluşturması, dokümante etmesi, değerlendirmesi ve iyileştirmesi gereklidir. Bu kapsamda;

- Gerekli süreçler tanımlanmalı
- Süreçlerin sırası ve birbiriyle ilişkisi belirlenmeli
- Gerekli kriterler ve yöntemler belirlenmeli
- Süreçlerin işleyişi ve izlenmesi için gerekli bilgi sağlanmalı
- Süreçlerin ölçümü, izlenmesi, analiz edilmesi, planlı sonuçlara ulaşımı ve sürekli iyileşmeyi elde edecek faaliyetler sürdürülmelidir.

- Uluslararası Standartların Kullanımı: ISO 9000 serisi gibi uluslararası standartların kullanımı NATO AC/250 ile düzenlenmiştir.
- NATO Yayınlarının Kullanımı: Savunma malzemeleri çok uluslu kullanıma sahip olduğundan bütün üye ülkelerde dâhil olmak üzere savunma ürünlerinde NATO standartları kullanılmalıdır. Bu standartlar rehber tipi ya da sözleşme tipi AQAP'lardır.

4.3.7. AQAP-2009 AQAP 2000 Serisinin Kullanımı İçin NATO Rehberi

NATO tarafından tek başına kullanılabilir olarak belirtilen yayınlar için bir rehber olarak hazırlanmıştır. Politika, rehber ve sözleşme tipi yayınları içerir [12].

AQAP dokümanları kullanım amacına göre şartname, rehber ve açıklama olarak kategorize edilebilir. **Şartname** tipi dokümanlar, ilgili tedarikçinin kurmak, uymak ve idare ettirmeye zorunlu olduğu sistemin temel niteliklerini adresleyen dokümanlardır. **Rehber** tipi olanlar, şartname tipi dokümanlardaki isteklerin açıklamasını içerir ve firma tarafından şartların ne ölçüde sağlandığını kontrol eder. **Açıklama** tipi dokümanlar ise terimler, yöntemler ve diğer hususlara ilişkin açıklamaları içerirler [3,12].

4.3.8. AQAP-2105 Devredilebilir Kalite Planları İçin NATO Gerekleri

Devredilebilir kalite planı yüklenici tarafından hazırlanan, ilgili her bir sürecin kimin tarafından ve ne zaman uygulanacağına dair prosedürleri ve ilgili kaynakları içeren dokümandır. AQAP 2105, bu

dokümanın nasıl hazırlanacağı ve neleri içereceğini düzenler. Dokümanın bileşenleri: [11]

- Planı oluşturma
- Onaylama ve sunuş
- Gerçekleştirme
- Gözden geçirme, düzeltme ve değişiklik kontrolü
- Plan içeriğinin düzenlenmesi
- Ürün gerçekleştirme faaliyetleri
- Ölçüm, analiz ve iyileştirme faaliyetleri

4.3.9. AQAP-2110 Tasarım, Geliştirme ve Üretim İçin NATO Kalite Güvence Gerekleri

Ürünün tasarım, geliştirme ve üretim ile ilgili kalite süreçlerini inceleyen yayındır. ISO 9000:2015 standartlarını temel alır. Dokümanda Kalite Yönetim Sisteminin (KYS) nasıl olması ve bileşenlerinin neler olması konusunda gerekli içerik sağlanmaktadır. ISO 9001:2015 de yer alan durumlara ek olarak NATO'ya özel gereklilikleri de içermektedir. Bu gereklilikler kapsamında;[13]

- Kurumsal görev, yetki ve sorumluklar başlığı altında üst yönetim tarafından atanacak yönetim temsilcinin yönetim ve Devlet Kalite Güvence Temsilcisi (DKGT) arasındaki görev ve sorumlukları ifade edilir.
- Planlama başlığı altında ISO 31000:2009 ilkelerine göre risk tanımlama, risk analizi, risk kontrolü ve risk azaltım süreçlerini içeren risk yönetim planı esasları ifade edilir.
- Destek başlığı altında altyapının, izleme ve ölçme kaynaklarının, personel yeterliliğinin ve farkındalığının sağlanmasının, dökümantasyonun esasları ifade edilmektedir.
- Operasyon başlığı altında planlama, kontrol, kalite planı ve esasları, konfigürasyon yönetimi, müşteri ilişkileri yönetimi, tasarım ve geliştirme süreçlerinin kontrolü gibi konulara dair esaslar ifade edilmektedir.

4.3.10. AQAP-2120 Üretim İçin NATO Kalite Güvence Gerekleri

Üreticinin sözleşmeye uygun ürünler sağlama kapasitesinin belgelendirildiği yayındır. ISO 9000:2008 standartlarını temel alır [14].

4.3.11. AQAP-2130 Muayene ve Test İçin NATO kalite Güvence Gerekleri

Son muayene ve test için süreçlere uygunluğu ve kalite yönetim gereksinimlerini içerir. ISO 9000:2008, ISO 9000:2005, ISO 10012:2003 standartlarını temel alır. Müşteri memnuniyeti odaklı gereksinimleri içerir. Diğer AQAP standartlarında olduğu gibi bu standartta da birinci öncelik Kalite Planın hazırlanmasıdır. Bu planda ürünün kalite gerekleri, ihtiyaç duyulan kaynaklar, doğrulama/izleme/muayene/test adımlarının esasları ve kabul kriterleri açıkça ifade edilmelidir. Standartta ayrıca sorumluluklar, kaynak yönetimi, müşteri ilişkilerinin süreçleri ve yönetimi ile ölçme/analiz/değerlendirme adımlarına dair esaslara yer verilmektedir [15].

4.3.12. AQAP-2210 AQAP 2110'a NATO Yazılım Kalite Güvence Gerekleri İlavesi

AQAP-2210, klasik olarak özel bir yazılım kalite sürecinden ziyade yazılım sürecindeki bütün organizasyonel yapıyı ve farklı yönetim seviyelerini hedef alır. AQAP-150 (V.2)'nin yeni ve geliştirilmiş versiyonu olarak ifade edilmektedir ve AQAP-2110 ile birlikte kullanılmak üzere tasarlanmış yazılım odaklı bir yayındır. Bu bağlamda yazılım projesi odaklıdır. Hareket noktası aşağıdaki durumların sağlanmasıdır [16]:

- Yazılım geliştirme prosedürlerinin açık olması
- Yazılım ömür devri içinde olası problemlerin en kısa sürede saplanması
- Etkin iyileştirme/düzeltme çalışmaları için kalite kontrol verilerinin elde edilmesi
- Yazılım geliştirme sırasında kalitenin doğrulanabilmesi
- Sözleşme kriterlerine uygunluğunun ve güvencesinin sağlanması

- Sözleşme kapsamında destek ve sistem mühendisliği faaliyetlerinin sağlanması ve
- Projenin gizlilik koşullarının belirtilmesidir.

İlgili durumların sağlanması için AQAP-150 yi temel alarak, yazılım kalite sisteminin oluşturulması, yazılım proje kalite planının oluşturulması ve bileşenlerinin belirlenmesi, yazılım gereksinimlerinin belirlenmesi, yazılım geliştirme süreçlerinin, organizasyonun, kullanılacak/teslim edilmeyecek yazılımlarının uyması gereken kriterlerin, dokümantasyon ve teslim aşamalarının belirlenmesi, değerlendirme ve doğrulama süreçleri ile bakım/idameye dair usul ve esasları yayında detaylı olarak ifade edilmiştir [16].

4.4. Değerlendirmeler

Siber savaşların arttığı son dönemde özellikle BT ürünlerinin etkin olduğu savunma sistemlerinde güvenliğin tam anlamıyla sağlanması büyük öneme sahiptir. Ülkelerin en kritik sistemlerinden birisi olan savunma sistemlerine yönelik ürün/hizmetlerin bir standardının olması hem güvenilirlik hem de sistemler üzerinde sağlıklı sonuçlar üretilmesi açısından kritiktir. NATO gibi birden çok müttefik bileşen arasında iletişim ve koordinasyonun sürekliliği olan organizasyonlarda ortak standartların bulunması daha da önem kazanmaktadır. Gerektiğinde birlikte çalışabilirliğin sağlanması ürünlerin birbiriyle sorunsuz iletişim kurmasına bağlıdır. Oluşacak bir iletişim kopukluğu ve/veya sistemin sağlıklı sonuçlar üretmesi konusundaki kuşku, kritik operasyonların bekasını tehlikeye sokabilmektedir. Bundan dolayı ortak standartların kullanılması gereklilik arz etmektedir. Bunun yanında AQAP'ların modüler olarak kullanılabilmesi hedefin belirlenmesi ve iyileştirmeleri kolaylaştırmakta ve tepki süresini kısaltmaktadır.

Savunma sanayisine hizmet/ürün gerçekleştiren firmaların sektördeki payı giderek artmaktadır. Firmaların birincil hedefleri her ne kadar bulundukları ülkenin savunma sistemlerine katkıda bulunmak olsa da sektörün hitap ettiği kitle uluslararası olma özelliğine sahiptir. Bu nedenle standartlara bağlı kalınarak geliştirilen ürünler hem ihracata imkân sağlamakta hem de ülkede kullanılan yabancı meşei ürünler ile entegrasyon problemlerini önlemektedir.

Dünya'daki savunma sanayisindeki gelişmeler, teknolojiye yatkın genç nüfusumuz ve giderek güçlenen bir savunma sanayimizin olduğu dikkate alındığında, hem ulusal hem de uluslararası düzeyde savunma sistemlerine yönelik ürün/hizmet üretiminde söz sahibi olmak ülkemizin temel hedefleri arasında olmalıdır. Bu aşamada, sistemlerin özellikle yerli tedarikçiler tarafından sağlanmasının teşvik edilmesinin yanı sıra uluslararası standartlara da katkıda bulunulacak akademik çalışmalar teşvik edilmeli, lisans/lisansüstü programlar ile eğitim desteği verilmeli ve yapılacak araştırmalara kaynak/imkân sağlanmalıdır.

Kaynaklar

[1] İnternet: Kocabaş C.(2013). *Kalite Güvence ve Standartları Ders Notları*. URL:http://www.webcitation.org/query?url=http://personel.klu.edu.tr/dosyalar/kullanicilar/erkan.tasdemir/dosyalar/dosya_ve_belgeler/kaliteGüvencevestandartları.pdf&date=2018-10-02, Son Erişim Tarihi: 02.10.2018.

[2] İnternet: TSE (2017). Türkiye'nin Bugünkü Manada İlk Standartı Bursa Belediye Kanunu (Kanunname-İ İhtisab-I Bursa). URL :http://www.webcitation.org/query?url=https://www.tse.org.tr/tr /icerikdetay/547/80/turkiyenin-ilk-standardı.aspx&date=2018-10-02, Son Erişim Tarihi: 02.10.2018.

[3] Gençler R. AQAP Allied qality assurance publication. NATO Müttefik Kalite Temin Yayınları. 205-211.

[4] İnternet: NATO Müşterek Siber Savunma Mükemmeliyet Merkezi (CCD COE). URL: https://ccdcoe.org/strategies-policies.html, Son Erişim Tarihi: 02.10.2018.

[5] İnternet: AQAP-110. NATO Quality Assurance Requirements For Design, Development And Productıon. URL: http://www.webcitation.org/ query?url=http://everyspec.com/NATO /NATO-AQAP/AQAP110e_346 &date=2018-10-02, Son Erişim Tarihi: 02.10.2018.

[6] İnternet: AQAP-120. NATO Quality Assurance Requirements For Productıon. URL: http://www.webcitation.org/query?url= http://everyspec.com/NATO/NATO-AQAP/AQAP_120_Ed-2_347&date=2018-10-02, Son Erişim Tarihi: 02.10.2018.

[7] İnternet: NATO Kalite Sistem Standartları AQAP-130. NATO Quality Assurance Requirements For Inspection and Test. URL: www.mbm.com.tr/aqap.asp Son Erişim Tarihi: 02.10.2018.

[8] İnternet: AQAP-150. NATO Quality Assurance Requirements For Software Development. URL: http://www.webcitation.org/query?url=https://www.difesa.it/SGD-DNA/Staff/DT/NAVARM/ Documents/NormeAQAP/AQAP150.pdf&date=2018-10-02, Son Erişim Tarihi: 02.10.2018.

[9] İnternet: AQAP-160. Integrated Quality Requirements for Software throughout the Life Cycle. URL: http://www.webcitation.org/query? url=https://www.difesa.it/SGD-DNA/Staff/DT/NAVARM/ Documents/NormeAQAP/aqap160e.pdf &date=2018-10-02, Son Erişim Tarihi: 02.10.2018.

[10] İnternet: AQAP-2000. NATO Policy On An Integrated Systems Approach To Quality Through The Life Cycle. URL: http://www.webcitation.org/query?url=http://www.difesa.it/SGD-DNA/Staff/DT/NAVARM/Documents/NormeAQAP/aqap2000e.pdf&date=2018-10-02, Son Erişim Tarihi: 02.10.2018.

[11] İnternet: AQAP-2105 URL: http://www.webcitation.org/query?url= http://nso.nato.int/nso/zPublic/ap/aqap-2105e(2).pdf&date=2018-10-02, Son Erişim Tarihi: 02.10.2018.

[12] İnternet: AQAP-2009. NATO Guidance On The Use Of The AQAP 2000 Series. URL: http://www.webcitation.org/query?url= http://www.difesa.it/SGD-DNA/Staff/DT/NAVARM/Documents/ NormeAQAP/aqap2009e.pdf&date=2018-10-02, Son Erişim Tarihi: 02.10.2018.

[13] İnternet: AQAP-2110. NATO Quality Assurance Requirements For Design, Development And Production. URL: http://www.webcitation.org/query?url=http://www.difesa.it/SGD-DNA/Staff/DT/NAVARM/Documents/ NormeAQAP/aqap2110e.pdf&date=2018-10-02, Son Erişim Tarihi: 02.10.2018.

[14] İnternet: AQAP-2120. NATO Quality Assurance Requirements For Production. Alıntı http://www.difesa.it/SGD-DNA/Staff/DT/ NAVARM/Documents/NormeAQAP/aqap2120e.pdf, Son Erişim Tarihi: 02.10.2018.

[15] İnternet: AQAP-2130. NATO Quality Assurance Requirements For Inspection And Test. URL: http://www.webcitation.org/query? url=http://www.difesa.it/SGD-DNA/Staff/DT/NAVARM/ Documents/NormeAQAP/aqap2130e.pdf&date=2018-10-02, Son Erişim Tarihi: 02.10.2018.

[16] [16] İnternet: AQAP-2210. AQAP 2210 Supplementary Software Quality Assurance Requirements URL: http://www.webcitation.org/query? url=http://nso.nato.int/nso/zPublic/ap/AQAP2210(A)(2).pdf&date=2018-10-02, Son Erişim Tarihi: 02.10.2018.

Yazılım Tanımlı Ağlar ve Siber Güvenlik

BÖLÜM 5

Sedef DEMİRCİ
Özgür YÜREKTEN
Mehmet DEMİRCİ

YAZILIM TANIMLI AĞLAR VE SİBER GÜVENLİK

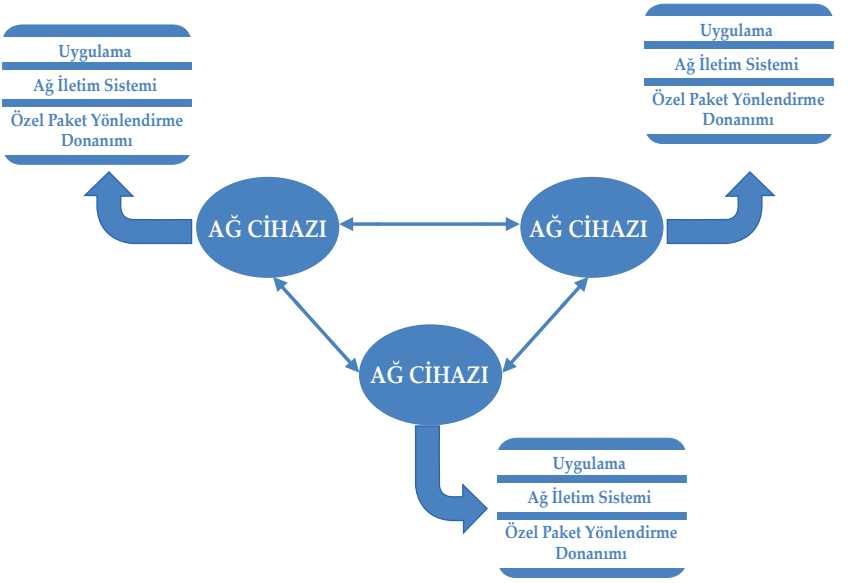
İnternet'e bağlı cihaz sayısının ve internet kullanımı gerektiren uygulama çeşitliliğinin artması beraberinde yüksek ölçeklenebilirlik, güvenilirlik, güvenlik ve hız gereksinimleri getirmiştir. Öte yandan, İnternet'in klasik mimarisi bu gereksinimler için yeterli esnekliğe sahip değildir. Günümüzde çok sayıda yeni servis ve uygulama (video aktarımı, bulut servisleri, VoIP vb.) tarafından üretilen büyük hacimli trafiğin karşılanmasında mevcut İnternet altyapısı gün geçtikçe yetersiz kalmaktadır [1, 2].

Yazılım tanımlı ağ (SDN) teknolojisi ile gelen programlanabilirlik ve merkezi kontrol, İnternet'teki sorunlara karşı pratik ve etkili çözümler üretmeyi kolaylaştırmaktadır. SDN, veri merkezlerinden servis sağlayıcı ağlarına kadar birçok alanda kullanılmakta ve hızla yaygınlaşmaktadır. SDN siber güvenlik açısında değerlendirildiğinde, hem güvenliği sağlamaya katkı yapan prensiplere hem de güvenlik risklerini arttıran özelliklere sahip olduğu görülmektedir. Bu bölümün 1. kısmında SDN'in temel felsefesi ve bileşenleri üzerinde durulmuştur. 2. kısımda SDN'in siber güvenliğe etkilerine değinilmiş, 3. kısımda ise SDN'de güvenliği sağlamak için önerilen somut çözümler işlevlerine göre sınıflandırılarak incelenmiştir. 4. kısımda, SDN ile dağıtık servis engelleme (DDoS) saldırılarının iki yönlü ilişkisi irdelenmiştir. 5. kısımda bölüm özeti ve araştırma önerilerine yer verilmiştir.

5.1. Yazılım Tanımlı Ağların Temelleri

Günümüzde kullanılan haliyle bilgisayar ağları, çok sayıda yönlendirici, anahtar, özel işleve sahip kutu (middlebox) ve bunlar üzerinde çalışan karmaşık protokollerden oluşmaktadır. Mevcut senaryo-

da bu cihazlar kendisine gelen paketi nereye ve nasıl yönlendireceğini hesaplamakta ve yönlendirme işlemini gerçekleştirmektedir. Şekil 5.1'de geleneksel bilgisayarın ağlarının nasıl çalıştığı gösterilmiştir. Bu mimarideki ağ cihazları dikey bütünleşmeye (vertical integration) sahip özelleşmiş kutulardır. Dikey bütünleşme, ağ cihazı içerisindeki donanım ve yazılımın yalnızca üreticisi tarafından sağlanabilmesi, üretici firma dışında kimse tarafından kapsamlı biçimde değiştirilememesi anlamına gelmektedir. Daha açık bir ifadeyle, bir cihaza kendi üreticisinden bağımsız bir şekilde farklı bir yazılım yüklenememekte ve müdahale edilememektedir [4]. Dolayısıyla ağ cihazları firmalara bağlı kaldıkça yeni fikirler rahatlıkla uygulanamamakta, yazılımda ve donanımda gelişmeler yavaşlamakta, esneklik yitirilmektedir.



Şekil 5.1. Geleneksel bilgisayar ağlarının çalışma prensibi [3]

İnternet mimarisine yitirilen esnekliği kazandırmak ve yeni servisler eklemeyi kolaylaştırmak amacıyla öne çıkan teknolojilerinden biri ağ sanallaştırmadır [5]. Fiziksel bir ağın üzerinde birden fazla mantıksal (sanal) ağın çalışmasını sağlayan soyutlama olarak tanımlanan ağ sanallaştırma ile düğümler, diskler, bağlar gibi ağ bileşenleri sanallaştırılmaktadır. Fakat ihtiyaç duyulan durumlarda dinamik bir şekilde sanal makine göçünün yapılması ve ağ yapılan-

dırması oldukça pahalı ve zaman alıcı işlemlerdir. Dolayısıyla büyük çaplı sanal ağların yönetiminin kolaylaştırılması da alt yapıda yer alan fiziksel ağın karmaşıklığının giderilmesine bağlıdır [6].

Yukarıda bahsedilen hususların etkilerinin en çok görüldüğü yerlerden biri veri merkezleridir. İnternet üzerinden erişilen servis ve uygulamaların kullanımına bağlı olarak ortaya çıkan büyük veri ile iletişim ağlarında tıkanıklık, ölçeklenebilirlik ve esneklik problemleri meydana gelmektedir. Bu da veri merkezlerindeki sunucu ve sanal makine sayılarının ve sunucular arasındaki iletişim trafiğinin muazzam bir şekilde artmasına neden olmaktadır. Dolayısıyla veri merkezlerinde yönetimin kolaylaşması ve sürdürülebilirliğin sağlanabilmesi için esnek, ölçeklenebilir ve çevik bir altyapıya ihtiyaç duyulmaktadır [6].

Ayrıca geleneksel bir ağ altyapısı üzerinde, değişen ağ şartlarını yönetebilmek için ağ operatörleri kısıtlı araç ve komutların kullanımı ile binlerce ağ cihazı için yüksek seviyeli kuralları manuel bir şekilde düşük seviyeli yapılandırma komutlarına dönüştürmek zorundadırlar. Dahası, ağa yeni bir cihaz veya servis eklenmesi gerektiğinde mevcut düğümlerin her biri yeniden yapılandırılmaktadır [6, 7]. Mevcut mimarideki bu tür kısıtlardan dolayı yeni bir yönlendirme protokolünün tasarlanması, test edilmesi ve kullanıma geçmesi 5 ila 10 yıl sürmektedir [8]. Dolayısıyla bu durum, hizmet kalitesi, güvenlik, güvenilirlik vb. amaçlı politikaların uygulanmasını ve yönetilmesini zorlaştırmakla birlikte maliyeti de artırmaktadır [2, 3].

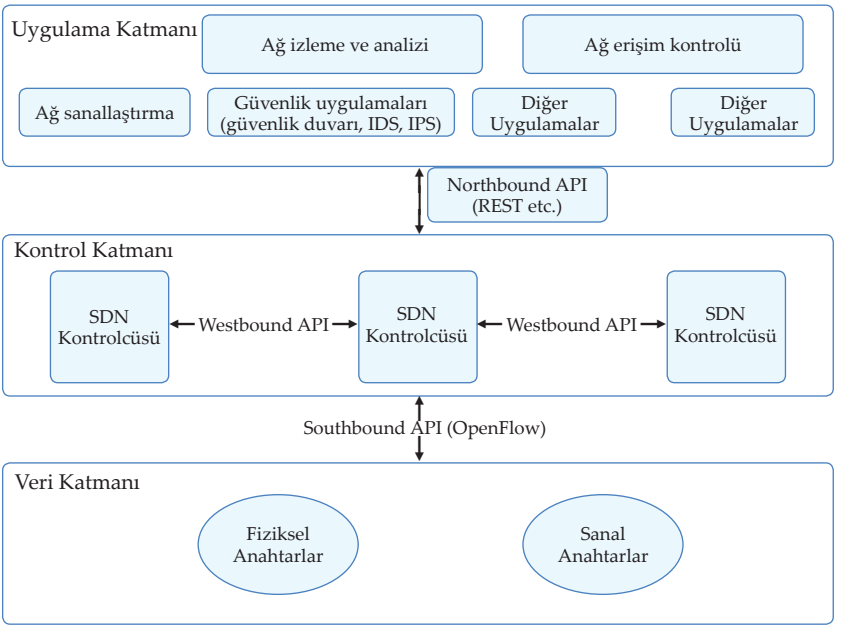
Geleneksel ağ mimarisi sahip olduğu kapalı kutu mantığından dolayı bilimsel araştırmaları da belirli ölçüde kısıtlamaktadır. Araştırmacılar yeni fikirler geliştirebilmek için gerçek dünya senaryoları üzerinde çalışmak yerine, genellikle kendi test ortamlarını yaratmak veya benzetim ortamlarında çalışmak zorunda kalmaktadır [9]. Diğer bir ifadeyle, donanım merkezli bir mimari üzerinde araştırma ve geliştirme yapmak oldukça maliyetlidir.

Sonuç olarak, mevcut ağ mimarisi üzerinde firmaya bağımlı ağ cihazlarının kullanımı ile esneklik yitirilmekte ve donanım bağımlı bir yapıdan dolayı gelişmeler yavaşlamaktadır [10]. Ayrıca ağ yönetimi ve yapılandırması gittikçe zorlaşmakta ve hatalara elverişli yapısından dolayı güvenlik açıklarına sebep olmaktadır [11]. Ya-

zılım Tanımlı Ağlar (Software Defined Networks), ağdaki kontrol birimini altyapıdaki yönlendirici ve anahtarlardan ayırarak, kontrolü mantıksal bir şekilde merkezileştiren, ağın merkezi bir yazılım birimi tarafından programlanmasına imkân sağlayan ve böylelikle yukarıda bahsedilen problemlere çözümler sunan yeni bir paradigmadır [8].

5.1.1. Kontrol ve Veri Düzlemlerinin Ayrılması

Yazılım Tanımlı Ağların (SDN) temel felsefesi kontrol katmanını veri katmanından ayırmaktır. Ağın beyni olarak da nitelendirilebilecek kontrol katmanı, yönlendirme kurallarını belirleyerek trafiğin nereye gönderileceğine dair kararları alan bir kontrol yazılımından oluşmaktadır. Söz konusu kararları icra eden veri katmanında ise kontrol yazılımının belirlediği kurallar dâhilinde yönlendirme yapan programlanabilir ağ cihazları bulunmaktadır. Uygulama katmanında, kontrolcünün üzerinde çalışan çeşitli ağ fonksiyonları (yük dengeleyici, güvenlik duvarı, saldırı tespit sistemi vb.) ile kullanıcı uygulamaları bulunmaktadır. Şekil 5.2'de SDN mimarisinin çalışma mantığı gösterilmektedir.



Şekil 5.2. SDN mimarisi [8]

Şekil 5.2'de ifade edilen çalışma prensibini daha detaylı açıklayabilmek için bu mimariyi oluşturan katmanlar, bunların birbirleriyle olan ilişkileri doğrultusunda aşağıdaki başlıklar altında anlatılmıştır.

5.1.2. Veri Katmanı

Altyapı katmanı olarak da bilinen bu düzlemde, geleneksel ağ mimarisine benzer şekilde paket anahtarlama ve iletiminden sorumlu yönlendirme elemanları bulunmaktadır. Geleneksel ağ cihazlarından farklı olarak bu katmandaki elemanlar kendi kontrol yazılımlarını içermediklerinden özerk kararlar alamazlar. Onun yerine bu katmandaki programlanabilir yönlendirici ve anahtarlar, kontrol katmanında çalışan kontrolcü yazılımının belirlediği kurallar doğrultusunda paket iletimi işlemini gerçekleştirmektedirler [12]. Switch Light, Open vSwitch, OpenFlow Reference, Pica8 SDN mimarisi için geliştirilmiş bazı programlanabilir anahtar örnekleridir [8].

5.1.3. Kontrol Katmanı

Bu katmanda ağın beyni olarak adlandırılabilecek bir veya daha fazla kontrolcü yazılımı bulunmaktadır. Kontrolcünün görevi, ağın hedefleri doğrultusunda önceden veya veri katmanındaki anahtarlar bir paketi nereye yönlendirileceğini sorduğunda, yönlendirme kuralları oluşturmak ve bunu güney arayüzü aracılığıyla anahtarların akış tablolarına yazmaktır [1]. Günümüzde farklı amaçlar için geliştirilmiş birçok kontrolcü yazılımı bulunmaktadır. NOX, POX, Floodlight, Beacon, DIFANE vb. bunlara örnek olarak gösterilebilir [8]. Kontrolcü seçimi yapılırken kullanım amacı, programlama dili kolaylığı ve performansı, öğrenme kolaylığı ve kullanıcı tabanı ve destek hizmetleri göz önünde bulundurulmalıdır.

5.1.4. Güney Arayüzü (Southbound API)

Bu arayüz, kontrolcünün veri katmanındaki yönlendirme elemanları ile iletişim kurmasını sağlamaktadır. Bu amaçla kullanılan en önemli protokol ONF (Open Networking Foundation) tarafından geliştirilen OpenFlow protokolüdür [13]. OpenFlow, kontrolcü ile anahtarlar arasında akan mesajların şeklini belirleyerek güvenli bir

biçimde iletişim kurulmasını sağlar. Kontrolcü, OpenFlow mesajları vasıtasıyla anahtara akış tablosunda değişiklikler yapmasını söyler [14]. OpenFlow protokolüne göre sırasıyla;

- Anahtar kendisine gelen paket için paketin başlıkları ile akış tablosundaki girdiler arasında eşleşme olup olmadığına bakar.
- Eşleşme varsa, daha önceden bu paketi nasıl yönlendireceğine dair kural kontrolcü tarafından akış tablosuna yazılmış demektir, dolayısıyla yapılması söylenen işlem gerçekleştirilir (paketi ilet, düşür, kuyruğa sok, başlık alanını değiştir vb.).
- Eşleşme yoksa anahtar ne yapacağını bilemediği için paketi OpenFlow protokolü aracılığıyla kontrolcüye gönderir.
- Kontrolcü paket ile ilgili kuralı hesaplar ve yine OpenFlow güvenli kanalı üzerinden anahtarın akış tablosuna yazar.

5.1.5. Uygulama Katmanı

Bu katmanda, ağ yönetimi, kontrolü ve operasyonunu sağlamak için gerekli olan yük dengeleme, güvenlik duvarı, trafik izleme, saldırı tespit sistemi, derin paket inceleme gibi farklı işlevleri olan uygulamalar bulunmaktadır [15]. Bu uygulamalardan her biri, kendi görevini gerçekleştirmesi için gereken politikaları tanımlar. Kuzey arayüzü tarafından kontrolcüye iletilen bu politikalar, sonrasında derlenip OpenFlow kurallarına dönüştürülerek veri katmanındaki anahtarların programlanmasında kullanılır [8].

5.1.6. Kuzey Arayüzü (Northbound API)

Kuzey arayüzü, uygulama katmanındaki uygulamaların kontrolcü ile haberleşmesinde kullanılan arayüzdür. Bir başka deyişle kuzey arayüzü, uygulamaların ağı programlamasına imkân veren yapıdır. Bu arayüz, geliştiricilere Python, Java, C++ vb. yüksek seviyeli diller kullanılarak uygulama geliştirme imkânı sunar. Ağ yöneticileri, servis sağlayıcıları ve araştırmacılar tarafından ağda karmaşık kurallar uygulamak için üst seviye bir dilde geliştirilen uygulamalar kuzey arayüzü tarafından derlenerek OpenFlow kuralları haline getirilmekte ve kontrolcüye iletilmektedir [14].

5.2. Yazılım Tanımlı Ağların Siber Güvenlik İçin Önemi

5.2.1. Siber Güvenliğin Sağlanmasına Ne Katkı Sağlar?

SDN; trafik kontrolü, saldırı tespiti, önlenmesi ve engellenmesi, güvenlik fonksiyonlarının geliştirilmesi, çalıştırılması, güncellenmesi ve adaptasyonu açısından birçok alanda ağdaki siber güvenliğin sağlanması ve sürdürülebilmesinde katkılar sağlamaktadır. Bu doğrultuda SDN'in siber güvenliğin sağlanmasındaki rolü ve sunduğu özellikler Tablo 5.1'de özetlenmiştir [16]. Ayrıca, tabloda sunulan özelliklerin her biri bu bölümde detaylandırılmıştır.

Tablo 5.1. Yazılım Tanımlı Ağların Siber Güvenliğe Katkısı

SDN'in sunduğu özellik	Açıklama	Siber Güvenliğe Katkısı	Savunmadaki Rolü
Dinamik trafik kontrolü	Trafiğin dinamik bir şekilde yönlendirilmesi, durdurulması vb.	Zararlı veya şüpheli ağ trafiğinin dinamik bir şekilde kontrol edilebilmesi ve normal trafikten ayırılabilmesi	Önleme, saldırıya cevap verme
Merkezi kontrol mekanizması	Ağ cihazlarının durumu ve ağa gelen trafiğin merkezi bir kontrolcü yazılımı tarafından izlenmesi ve yönetilmesi	Ağ çapındaki tüm güvenlik servislerinin izlenebilmesi, saldırıların veya anormal trafiğin daha etkin ve etkili bir şekilde tespit edilebilmesi	Tespit, saldırıya cevap verme
Ağın programlanabilir olması	Ağ fonksiyonlarının programlanabilmesi	Güvenlik fonksiyonlarının kolay bir şekilde geliştirilebilmesi ve güncellenebilmesi	Tespit, saldırıya cevap verme
Basitleştirilmiş veri katmanı	Kontrol mantığının veri katmanından ayrılarak merkezi bir kontrolcü yazılımına verilmesi	Yeni güvenlik servislerinin eklenmesi ve bunların diğer servislerle olan etkileşiminin kolaylaşması	Önleme, tespit, saldırıya cevap verme

Yazılım tanımlı ağların merkezi bir kontrol mekanizması ile trafik yönetimine izin vermesi ağ güvenliğinin sağlanmasına ciddi katkı sağlamaktadır. SDN'in sunduğu bu özellik sayesinde şüpheli veya zararlı olduğu tespit edilen trafik, ağa gelen normal trafikten dinamik bir şekilde ayırt edilebilmektedir. Bu trafiğin ağ üzerinde yönlendirmesinin durdurulması veya ilgili güvenlik fonksiyonlarına yönlendirilmesi ise oldukça kısa bir sürede ve birkaç komutla gerçekleştirilebilmektedir [16].

Öte yandan, SDN ağ çapında bir izleme mekanizması sunduğundan saldırıların tespit edilmesi ve bunlara karşı önlem alınması da daha kolay olmaktadır. Bütün ağ cihazlarının mevcut durumu ve ağa gelen trafik merkezi bir kontrolcü yazılımı tarafından izlenmekte ve yönetilmektedir. Böylelikle ağ çapındaki tüm güvenlik servisleri izlenebildiğinden saldırılar veya anormal trafik geleneksel ağlara göre daha etkin ve etkili bir şekilde tespit edilebilmektedir [16].

Bunlara ek olarak SDN ile birlikte gelen ağın programlanabilir olması özelliği sayesinde ağ üzerine yerleştirilecek olan güvenlik fonksiyonları çok daha kolay bir şekilde geliştirilebilmekte ve ağın ihtiyaçlarına göre bu fonksiyonların sunduğu özellikler güncellenebilmektedir. Bu da ağda güvenliğin sağlanmasını ve sürdürülebilmesini çok daha kolay bir hale getirmektedir [16].

Son olarak, SDN ile veri katmanının basitleştirilmesi ve karmaşık işleri yapan mantığın bu katmandan alınarak kontrol katmanında bulunan yazılıma verilmesi sayesinde ağa yeni güvenlik servislerinin eklenmesi ve bunların diğer servislerle olan etkileşiminin sağlanması çok daha kolay bir şekilde yapılabilmektedir [16].

5.2.2. Siber Güvenlik Açısından Ne Tür Yeni Zorluklara Yol Açar?

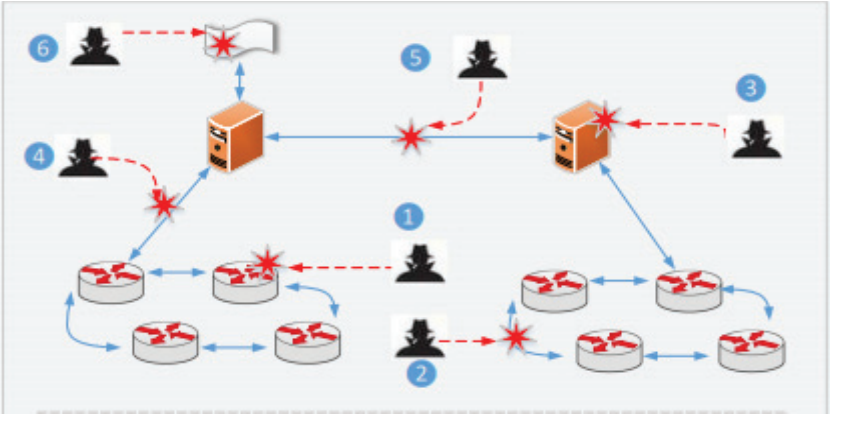
SDN siber güvenlik açısından birçok avantaj sağlasa da bu tür ağlara özgü bazı tehditler ile birlikte birçok yeni ve tehlikeli saldırı ortaya çıkabilmektedir. Shu ve arkadaşlarına göre [17] SDN'de karşılaşılan güvenlik problemleri ve zorluklar; "savunmasız kontrolcü", "açık kaynak programlanabilir arayüzlerden kaynaklanan riskler" ve "daha çok saldırı noktası" olmak üzere üç farklı başlık altında ele alınabilir.

Kontrolcü açısından bakıldığından ağdaki çoğu servisin (ağ yapılandırma, trafiğin yönlendirilmesi, ağ fonksiyonlarının yönetilmesi vb.)

bu yazılım üzerinde toplandığı görülmektedir. Dolayısıyla, kontrolcünün savunmasız olduğu durumda saldırılarının tek bir noktayı hedef alması dahi yeterli olmakta ve yalnızca kontrolcü hedef alınarak birçok servis için tehdit oluşturulabilmektedir. Saldırgan kontrolcüyü ele geçirdiğinde tüm ağ yönetimini de ele geçirmekte ve yapacağı bir saldırı ile tüm işleyişi felç edebilmektedir [17, 18].

Öte yandan, açık kaynak yapısından dolayı SDN güvenlik tehditlerine karşı daha elverişli bir platformdur. Çünkü kontrolcüdeki yazılım zafiyetleri ağı saldırganlara karşı savunmasız bir hale getirebilmekte ve saldırganların zafiyetin yapısına göre saldırı planlaması yapmasına olanak tanımaktadır. Ayrıca, kontrolcünün uygulama katmanında yer alan fonksiyonlar için çok sayıda programlanabilir arayüz imkânı sunmaktadır. Bu açıklık düzeyi; virüs, truva atı, arka kapı gibi zararlı kod parçacıklarının arayüze gömülmesi şeklinde kötüye kullanıma sebep olabilmektedir. Bu nedenle SDN kontrolcülerinin açık kaynak arayüzlerinin oldukça dikkatli bir şekilde değerlendirilmesi ve siber güvenlik açısından etraflıca incelenmesi gerekmektedir [17, 19].

Son olarak, SDN'de geleneksel ağlara göre daha çok saldırı noktası bulunmaktadır. Her bir katmandaki birimler ağın farklı bölgelerine dağılmış olsa bile bu birimler arasındaki iletişimin aksamadan devam etmesi gerekmektedir. Saldırganlar tarafından hedef alınan saldırı noktaları Şekil 5.3'de SDN mimarisi üzerinde gösterilmiştir.



Şekil 5.3. SDN mimarisi üzerindeki muhtemel saldırı noktaları [17]

Şekil 5.3'den de görülebildiği gibi, bir saldırgan SDN mimarisi üzerindeki (i) anahtarları, (ii) anahtarlar arasındaki yolları, (iii) kontrolcü yazılımını, (iv) kontrolcü ile anahtarlar arasındaki bağlantı noktalarını, (v) birden fazla kontrolcü olduğu durumda kontrolcüler arasındaki iletişim noktalarını ve (vi) uygulama katmanında yer alan fonksiyonları amacına yönelik saldırılar gerçekleştirmek üzere hedef alabilmektedir [17, 20].

5.3. Yazılım Tanımlı Ağlarda Siber Güvenlik Fonksiyonları

Geleneksel ağlarda güvenlik, markalar tarafından tescillenmiş özel donanım cihazları üzerine kurulu güvenlik duvarı, saldırı tespit/engelleme sistemleri, derin paket inceleme (DPI) gibi güvenlik fonksiyonları ile sağlanmaktadır [21]. Yazılım tanımlı ağlarda ise bu yaklaşımdan farklı olarak kontrol ve uygulama katmanlarındaki yazılım modülleri vasıtasıyla güvenliğin sağlanması tercih edilmektedir. Ağ fonksiyon sanallaştırma (network functions virtualization) kapsamında güvenlik fonksiyonlarının yazılım halinde ağda farklı bölgelerdeki sunuculara yerleştirilmesi giderek yaygınlaşmaktadır [22, 23]. Hu ve Ahn'a göre [21], sanallaştırılmış ağ güvenlik fonksiyonları, saldırı tespit, saldırı engelleme ve saldırı yakalama fonksiyonları olmak üzere üç başlık altında ele alınabilir. Bu bölümde güvenlik fonksiyonları bahsedilen üç başlık altında incelenecektir.

5.3.1. Saldırı Tespit Fonksiyonları

5.3.1.1. Saldırı Tespit Sistemi

Saldırı tespit sistemleri ağı izleyerek zararlı bir aktivite veya kural ihlali olup olmadığını tespit eden ve bunu sistem yöneticilerine raporlayan pasif güvenlik fonksiyonlarıdır [24]. Geleneksel ağ yapısı üzerindeki saldırı tespit sistemleri saldırıyı tespit edebilmek için imza tabanlı, istatistik tabanlı ve protokol analizi yaklaşımlarını kullanırlar. Fakat bu tür sistemlerin kullandıkları veri sistem kayıtları, servisler ve düğüm mesajlarından alındığı için sanal makinelere yapılan saldırıları tespit etmeleri oldukça zordur [25]. Bunu yapabilen sistem önerileri ise oldukça maliyetlidir [26]. Ayrıca ağ büyüdükçe ve karmaşıklığı arttıkça yapılması gereken analiz işlemi ve sonrasında trafiğin nasıl yönlendirileceği kararı performans açısından olumsuz sonuçlar doğurmaktadır [27]. SDN üzerinde

yapılandırılmış saldırı tespit sistemlerinde ise SDN'in merkezi ve yazılım tabanlı mimarisi sayesinde istatistikleri toplamak, anlamlandırmak ve trafiği uygun şekilde yönlendirmek çok daha kolay olmaktadır. Örneğin, Adrichem ve arkadaşları tarafından yapılan bir çalışmada [28] POX kontrolcü yazılımı üzerinde OpenNetMon adında bir saldırı tespit sistemi geliştirilmiştir. OpenNetMon ağdaki veri hacmi, paket kaybı ve gecikme metriklerine bakarak trafik mühendisliğine ile saldırı tespiti yapabilmektedir.

5.3.1.2. Zararlı Yazılım Tarayıcılar

Zararlı yazılım tarayıcılar, yerel ağı internetteki zararlı yazılımlardan korumak için geliştirilmiş olup genellikle ticari ürün olarak piyasada mevcutturlar. Bu güvenlik fonksiyonları yerel ağa gelen paketler içinde virüs, solucan, truva atı vb. taraması yaparlar. Ceron ve arkadaşları tarafından geliştirilen bir zararlı yazılım analiz sistemi, SDN'in sunduğu esneklikten faydalanarak dinamik biçimde gelişmiş zararlı yazılımları çözümlemekte ve geleneksel araçlara kıyasla daha yüksek oranda zararlı yazılım tespiti yapabilmektedir [29].

5.3.1.3. DDoS Tespit Sistemi

Ağ güvenliğini tehdit eden en önemli saldırı türlerinden biri de DDoS (dağıtık servis engelleme) saldırılarıdır. DDoS saldırılarında genellikle hedef bilgisayara dağıtık bir şekilde çok sayıda sahte istek gönderilerek gerçek istekleri işleyememesi ve böylelikle hizmet dışı bırakılması amaçlanmaktadır. Literatürde geleneksel ağlarda DDoS tespiti yapabilmek için önerilmiş yüzlerce çözüm mevcuttur [30]. Bu çözümlerde karşılaşılan en büyük problem çok sayıda paketin analiz edilmesi gereksinimidir. Bu durum hem tespit işleminin doğruluk seviyesini düşürmekte hem de işlem süresini uzatmaktadır [31].

Yazılım tanımlı ağlarda ise kontrolcü yazılımı ile çok sayıda anahtar eş zamanlı olarak kontrol edilebildiği için DDoS tespiti daha kısa sürede daha etkin bir şekilde yapılabilmektedir. Bu kapsamda Braga ve arkadaşları NOX kontrolcüsü üzerinde bir DDoS tespit fonksiyonu geliştirmişler ve NOX ile DDoS tespitinden sorumlu anahtarları ağa kolaylıkla ekleyip çıkarabildiklerini belirtmişlerdir. Ayrıca geliştirdikleri sınıflandırıcı ile yeni saldırı türlerini de kolaylıkla sisteme dâhil edebilmektedirler [31].

5.3.1.4. Derin Paket İnceleme

Derin paket inceleme (DPI), ağdaki trafik akışını ve kullanıcı aktivitelerini gerçek zamanlı olarak detaylı bir şekilde incelemeye olanak sağlayan bir araçtır. DPI ile paketin başlıklarının yanı sıra içerdiği veri kısmı da trafik türü, protokol uygunluğu ve zararlı yazılım içerip içermediği açısından kontrol edilmektedir. Paket içeriğinde şüpheli bir durum veya saldırı tehdidi algılandığında paket başka bir yere yönlendirilebilir veya başka bir güvenlik aracına durum raporlanabilir [32]. Böylelikle ağ performansının artırılması, bant genişliği maliyetinin azaltılması, tıkanıklık denetiminin yapılması, hizmet kalitesinin artırılması ve siber saldırılardan korunma amaçlanmaktadır [33].

Geleneksel ağlarda genellikle özel donanım cihazları üzerinde çalışan DPI araçları ağda belirli konumlara yerleştirilmektedir. Fakat SDN ve NFV kavramlarının ağ dünyasına girmesiyle birlikte DPI araçlarının sanallaştırılarak SDN mimarisinde uygulanması araştırmacıların üzerinde çalıştığı konular arasındadır [32, 34]. Bu doğrultuda yapılan bir çalışmada [35], DPI, SDN kontrolcüsü üzerinde bir fonksiyon olarak geliştirilmiş ve ağ performansında %67 iyileşme sağlandığı görülmüştür.

5.3.2. Saldırı Engelleme Fonksiyonları

5.3.2.1. Güvenlik Duvarı

Güvenlik duvarı, yerel ağ ile internet arasına yerleştirilerek yerel ağı internetteki güvenilir olmayan trafikten koruyan ilk seviye erişim kontrolü cihazıdır. Geleneksel ağlarda güvenlik duvarının yerleştirildiği konum ağın internete açıldığı kenar noktalarda olduğundan iç trafik görülmez ve denetlenmez. Yazılım tanımlı ağlarda ise bu güvenlik fonksiyonu, merkezi kontrolcü üzerinde bir uygulama olarak yapılandırılıp tüm trafik bu uygulamaya yönlendirilebilir veya güvenlik duvarı kuralları doğrudan ağdaki yönlendirme cihazlarına yazılabilir. Böylece, dış noktalarla iç noktalar arasındaki trafiğe ek olarak tamamen içeride kalan trafik de görülüp denetlenebilir. Ayrıca SDN'de güvenlik duvarının yalnızca paket filtreleme yapması yeterli değildir. Ağ şartları, yapılandırmalar ve akış kuralları dinamik bir şekilde değiştiği için güvenlik duvarı kurallarının akış kuralları ile olan uygunluğu da denetlenmektedir. Bunların

yanı sıra, güvenlik duvarını yerleştirme mimarisi (merkezi veya dağıtık) ve ağda hangi noktalara konumlandırılması gerektiği de dikkatli bir şekilde tespit edilmelidir [36].

Geleneksel ağlardaki güvenlik duvarları yaptıkları filtreleme işlemine göre durum denetlemesiz (stateless) ve durum denetlemeli (stateful) olarak ikiye ayrılırlar. Durum denetlemesiz güvenlik duvarlarında paket başlığındaki IP adres veya port numarası gibi alanlara bakılarak paketler filtrelenir, paketin meşruluğunu kontrol etmek için bağlantının durumu izlenmez. Durum denetlemelilerde ise gelen isteğin bağlantı kurulmak istenen IP olup olmadığına, iletişim kuralına, kaynak ve hedef porta bakılır. Daha basit bir ifadeyle, genellikle yalnızca öncesinde bağlantısı kurulmuş bir akış üzerinden gelen paketler kabul edilir [37]. SDN'deki güvenlik duvarları ise durum denetlemesiz filtreleme yapmaktadırlar çünkü OpenFlow kontrolcüye bağlantı hakkında oldukça kısıtlı bilgi sunmaktadır. Bu nedenle SDN güvenlik duvarlarının tamamen durum denetlemeli filtreleme yapması ele alınması gereken problemler arasındadır [36].

SDN'de güvenlik duvarı fonksiyonu geliştirme üzerine yapılmış çalışmalar literatürde mevcuttur [36, 38-41]. Bu kapsamda Hu ve arkadaşları tarafından yapılan bir çalışmada SDN için Flowguard adında bir güvenlik duvarı geliştirilmiştir. Flowguard tehditleri doğru bir şekilde tespit edebilmenin yanı sıra ağ şartları her değiştiğinde otomatik ve gerçek zamanlı olarak ihlalleri ayrıştırmaktadır [36].

5.3.2.2. Saldırı Engelleme Sistemi

Saldırı tespit sistemleri saldırıyı fark edip yalnızca raporladıkları için başlangıç aşamasında engelleyecek şekilde proaktif bir yapıya sahip değillerdir. Bu nedenle şüpheli ağ aktivitelerine karşı otomatik bir şekilde harekete geçmek için saldırı tespit sistemlerinin yanı sıra saldırı engelleme sistemlerine ihtiyaç duyulmuştur. Geleneksel saldırı engelleme sistemlerinin çoğu esnek bir şekilde genişletilebilir değildir. Açık kaynak kodlu yazılımlar olsa bile farklı kodlama stilleri, geliştirme ortamları ve arayüzleri bu sistemlerin her ortama yerleştirilmesini zorlaştırmaktadır. Ayrıca geleneksel ağ altyapısı üzerinde kurulu saldırı engelleme sistemlerinin değişen ağ şartlarına dinamik çözümler üretmesi de oldukça zordur [25].

Yazılım tanımlı ağlarda ise ağ mimarisinden dolayı saldırı engelleme sistemleri saldırı tespit ve engelleme işlemini daha çevik, az maliyetli ve dinamik bir şekilde yapabilmektedirler. Literatürde SDN için saldırı engelleme sistemi geliştirme üzerine yapılmış çalışmalar diğer güvenlik fonksiyonlarına göre sayıca daha azdır. Zhang ve arkadaşları tarafından yapılan bir çalışmada [42] SDN tabanlı bir saldırı engelleme sistemi önerilmiş ve ağa yerleştirilen bu yazılımlar üzerinde yük dengeleme yapılmıştır. Deney sonuçları geliştirilen sistemin daha kısa sürede saldırıları tespit edebildiği ve yapılan yük dengeleme ile gecikmeyi azalttığı yönündedir.

5.3.3. Saldırı Yakalama Fonksiyonları

Saldırıyakalama fonksiyonlarındar birisi olan bal küpü, bir ağa yapılan sızmaları ve saldırıları izleyebilmek, yöntemleri hakkında bilgi sahibi olmak ve yeni saldırı türlerini erken tespit edebilmek için saldırganlara önemliymiş gibi gösterilen tuzak sistemlere verilen addır. SDN'de ağ altyapısı yazılım ile kontrol edildiğinden bal küpü gibi dinamik öğrenme ve trafik yönlendirmesi gereken sistemlerde geleneksel ağlara göre daha iyi çözümler üretilebilmektedir [11].

Shin ve arkadaşları, içinde bal küpü fonksiyonunun da bulunduğu birçok güvenlik modülünden oluşan FRESCO adında bir çerçeve geliştirmişlerdir. FRESCO ile zararlı bir bağlantı isteği tespit edildiğinde ilgili trafik bal küpüne yönlendirilmektedir. Böylelikle saldırgan orijinal hedefi ile haberleştiğini sanarak sisteme zarar verememektedir [43].

5.4. Yazılım Tanımlı Ağlar ve DDoS

Servis engelleme (DoS) saldırıları, bilgisayar ağları üzerinden erişilen sistemlerin meşru kullanıcıları tarafından kullanılmasını engelleyen saldırılardır [44]. Dağıtık servis engelleme (DDoS) saldırıları da genellikle uzaktan kontrol edilen, iyi organize olmuş ve dağıtık zombi veya botnet bilgisayarların, aynı anda ve sürekli olarak hedef sisteme büyük bir trafik ve servis talebi göndermesiyle yapılmaktadır. Bu durum karşısında hedef sistem ya çok yavaş yanıt vermekte ya da yanıt veremez hale gelmektedir [44]. DDoS saldırılarının tespiti ve önlenmesi amacıyla çok fazla çalışma yapılmıştır. DDoS

saldırılarına karşı koymak için önerilen yöntemler çeşitli şekillerde sınıflandırılabilmektedir. Literatürdeki çalışmalarda DDoS savunma mekanizmaları için tanımlanan temel sınıflandırmalar Tablo 5.2'de yer almaktadır.

Tablo 5.2. DDoS Savunması için Sınıflandırmalar

DDoS Savunması İçin Sınıflandırma Türleri	**Açıklama**	**[44]**	**[45]**	**[46]**	**[47]**	**[48]**	**[49]**
Yapılan Faaliyete Göre Sınıflandırma	Önleme, tespit, karşı koyma, hedef tespiti, azaltma vb.	X		X	X		
Yerleştirildiği Yere Göre Sınıflandırma	Hedef ağ, kaynak ağ, ara ağ vb.	X	X	X			
Faaliyet Seviyesine Göre Sınıflandırma	Önleyici, düzeltici vb.		X				
İş birliği Seviyesine Göre Sınıflandırma	Bağımsız, otonom, işbirliği ile vb.		X			X	
Saldırılan Ağ Katmanına Göre Sınıflandırma	İletişim katmanı, uygulama katmanı vb.	X					
Uygulanan Tespit Yöntemine Göre Sınıflandırma	Anomali tespiti, kötüye kullanım tespiti, imza temelli tespit vb.		X	X			
Uygulanan Önleme Yöntemine Göre Sınıflandırma	Filtreleme, bant genişliği sınırlama, yetkinlik temelli, yapılandırma değiştirme, hedefin tespit edilmesi vb.		X			X	X

Bu bölümde yazılım tanımlı ağların DDoS saldırılarındaki rolü, DDoS saldırılarının tespitinde yazılım tanımlı ağ tabanlı çözümler ve yazılım tanımlı ağlarda gerçekleştirilen DDoS saldırılarının tespiti olmak üzere iki farklı başlık altında ele alınacaktır.

5.4.1. DDoS Saldırılarının Tespitinde Yazılım Tanımlı Ağ Tabanlı Çözümler

SDN ile DDoS saldırılarına sunulan çözüm önerileri, geliştirilen güvenlik fonksiyonları ve mimari önerileri olmak üzere tarafımızca iki farklı başlık altında sınıflandırılmıştır.

5.4.1.1. Güvenlik Fonksiyonu Çözümleri

Arins [50], internet servis sağlayıcısı tarafından SDN altyapısı kullanılarak bir güvenlik duvarı önermiştir. Önerilen yöntemde tanımlanan güvenli ağ üzerinden son kullanıcı ağındaki SDN kontrolcüsü internet servis sağlayıcının yönettiği yönlendirme tablolarına erişim sağlayabilmekte ve bu güvenlik duvarı ile iletişim kurarak DDoS saldırılarına karşı korunma sağlayabilmektedir.

Li ve ark. [51] ise SDN özelliklerinden faydalanarak DDoS saldırılarında da kullanılabilecek bir saldırı tespit ve önleme sistemi geliştirmişlerdir. Önerilen sistemin geleneksel yöntemlerle elde edilen performansı sağlayabildiği gibi geleneksel yöntemlerde ihtiyaç duyulan yazılım ve donanım maliyetlerini azaltabildiği ifade edilmiştir. Önerilen sistem DoS ve tarama saldırıları için test ortamında değerlendirilmiş ve sonuçları paylaşılmıştır.

Önerilen SDN temelli bir diğer saldırı tespit ve önleme sistemi de BroFlow [52, 53] adlı sistemdir. Bu sistem kaynakları dinamik olarak yönetebilmekte, ağ olayları için kural tanımlama programlama dili kullanılarak algoritma geliştirilebilmeyi sağlamakta, saldırılara anında karşılık verebilmekte ve saldırı tespiti için ağda dağıtık bulunan sensörleri yönetebilmektedir. Önerilen sistem için prototip geliştirilmiş olup sistemin normal trafiğin maksimum seviyede iletildiği, saldırıların %90'ının engellenebildiği ve normal güvenlik duvarlarına göre bant genişliğinin %50 daha fazlasının kazanıldığı belirtilmiştir.

DDoS'un yaygın bir türü olan sel (flood) saldırılarını tespit etmek için Chin ve ark. [54] tarafından Open Virtual Switch destekli İzleyici ve Denetleyici adı verilen bileşenler ile belirli imzaya sahip DDoS tehditlerini tespit edebilen bir yöntem önerilmiştir. Bu yöntemin DDoS tehditlerinin tespit edilmesinde veya başka sistemlerle tespit edilen tehditlerin doğrulanmasında kullanılabileceği belirtilmiştir.

Önerilen yöntem TCP SYN sel saldırıları için test edilmiş ve sonuçları paylaşılmıştır.

Yoon ve ark. [55] yazılım tanımlı ağların kabiliyetlerinden faydalanarak ve Floodlight SDN kontrolcüsünü kullanarak SDN mimarisinin uygulama katmanında yer alan dört farklı güvenlik fonksiyonu geliştirmiş ve test etmiştir. Önerilen çözümler; ağ içinde güvenlik çözümlerinden (güvenlik duvarı, saldırı önleme sistemi vb.), pasif güvenlik çözümlerinden (saldırı tespit sistemi vb.), ağ anormalliklerini tespit çözümlerinden (tarama ve DDoS tespit sistemi vb.) ve gelişmiş güvenlik çözümlerinden (hafızalı güvenlik duvarları, yansıtma ağları vb.) oluşmaktadır.

Ağ fonksiyonları sanallaştırma ve yazılım tanımlı ağ teknolojileri kullanılarak geliştirilen Bohatei [56] ise genişleyebilen, saldırılara cevap verebilen ve olumsuz durumlarda kendini iyileştirebilen bir güvenlik fonksiyonudur. Geliştirilen çözüm; tehdit belirleme, tehdit boyutunu kestirebilme, kaynakları yönetebilme ve ağ yönetimini sağlayabilme kabiliyetlerinin hepsine sahiptir. Bu çözüm bazı DDoS saldırılarına karşı uygulanmış olup çok yüksek oranda genişleyebilir olduğu, çok kısa sürede saldırılara karşılık verebildiği ve dinamik tehditlerde kendini iyileştirebildiği belirtilmiştir.

Son dönemde SDN'de DDoS tespiti için derin öğrenmeden faydalanan yaklaşımlar geliştirilmiştir [57]. SDN kontrolcüsünün merkezi konumu ve ağın tümünü takip edebilmesi sayesinde daha önce görülmemiş akışlara ait paketlerin başlık alanları üzerinde derin öğrenme modelleriyle analiz yapılabilmektedir. Kontrolcü tarafından yapılan bu analiz sonucunda saldırı olduğu tespit edilen akışlar için anahtarlara paket filtrelemeye yönelik kurallar kolaylıkla yazılabilmektedir.

Diğer bir çalışma kapsamında da [58] INSF (Interface to Network Security Functions) ve SDN kullanılarak merkezi güvenlik duvarı ve DDoS saldırıları karşı koyma servislerini de sağlayabilecek güvenlik servisi çatısı önerilmiştir. FRESCO [43] mimarisi kullanılarak tanımlanan bir başka DDoS saldırı önleme çatısında [59] bileşenler olarak betik programlama bileşeni, uygulama bileşeni ve ön tanımlı modüller yer almaktadır. Ağ yöneticileri betik programlama bileşeni ile değişik kurallar tanımlayabilmektedir. Tanımlanan betikler

uygulama bileşeni tarafından SDN anahtarların anlayacağı kurallara çevrilmekte ve SDN anahtarlarına yüklemektedir. Önerilen çatıda DDoS saldırılarının tespiti ve engellenmesi için modüller tanımlanmıştır.

5.4.1.2. Mimari Çözümleri

SDN ile DDoS saldırılarının tespiti ve önlenmesi amacıyla geliştirilen bir mimaride SDN kontrol katmanı ile veri katmanı arasında bir SDN güvenlik katmanı [60] önerilmiştir. Bu öneride, SDN anahtarları ile SDN kontrolcüsü arasındaki iletişim bu katman üzerinden gerçekleşmektedir. Önerilen yöntem için POX kontrolcüsü kullanılarak geliştirme yapılmış ve ICMP sel baskını saldırısı için testler gerçekleştirilmiştir. Önerilen yöntemin sisteme çok az ek yük getirdiği ve çok az bir yapılandırma ile hayata geçirilebildiği ifade edilmiştir.

Yazılım tanımlı ağlarda etkin ve genişleyebilir tehdit tespit ve karşı koyma mekanizması için Giotis ve ark. [61] tarafından önerilen yöntemde, ağ istatistiklerini toplamak için SDN kontrolcüsü devreden çıkarılarak sFlow izleme verisi kullanılmaktadır. Toplanan istatistik verileri entropi temelli olarak analiz edilmekte ve saldırıları önlemek için kullanılmaktadır. Çalışma kapsamında önerilen yöntem, OpenFlow protokolü vasıtasıyla yürütülen veri toplama süreci ile karşılaştırılmış ve önerilen yöntemin performansının yüksek olduğu belirtilmiştir.

Çok yüksek yoğunluklu trafiğin olduğu ağlarda DDoS saldırılarından korunmak için sunulan bir öneride [62], şüpheli ağın tespiti ve saldırının önlenebilmesi için yazılım tanımlı ağın kabiliyetleri kullanılarak ağ trafiği DDoS önleme cihazına (DDoS washing machine) yönlendirilmektedir. DDoS saldırılarının etkisini azaltmak için Belyaev ve Gaivoranski [63] tarafından sunucular ve ağ cihazları arasında SDN ağlarında daha kolay uygulanabilen yük dengeleme yöntemi önerilmiştir. Bu yöntemle DDoS saldırısı anında ağın ayakta kalma süresinin uzatılabildiği belirtilmiştir.

DDoS saldırılarına karşı kullanılan Remote Triggered Black-Hole (RTBH) yönlendirme yaklaşımı, yazılım tanımlı ağlarda da uygulanmış ve başarılı sonuçlar sağladığı belirtilmiştir [64]. Yürütülen

diğer bir çalışmada da [65] geleneksel ağlara OpenFlow protokolü destekli özel kutular ekleyerek aynı yöntemin DDoS saldırılarına karşı kullanılabileceği belirtilmiştir.

DDoS saldırısı anında servislerin esnekliğinin sağlanması, yükün dengelenmesi ve filtrelemelerin yapılabilmesi için kapasiteyi esnek olarak yönetebilecek, tanımlanan kara listeleri kullanabilecek ve normal trafik akışını öğrenebilecek bir mekanizma Kalliola ve ark. [66] tarafından önerilmiştir. Önerilen mekanizma ile saldırı anında servislerin %50-%80 oranında servis sunmaya devam ettikleri belirtilmiştir.

DDoS saldırılarını önlemek için Duan ve ark. [67] tarafından yapılan çalışmada rastgele yönlendirme mutasyonu adında çevik çok yollu yönlendirme yaklaşımı önerilmiştir. Diğer bir çalışmada da [68] yönlendirme için kısıt sağlama problemi ile ifade edilerek ve oyun teorisini de kullanarak geliştirilen bir yöntem önerilmiştir. Bu yaklaşımda öncelikle kullanılacak parametrelerin belirlenmesi için saldırgan ve hedef arasında oyun modeli oluşturulmaktadır. Ardından kısıt sağlama problemi optimizasyonu ile yönlendirme seçimi modellenmektedir. Son olarak tanımlanan algoritmalarla model ağda uygulanmaktadır. Yapılan çalışma tek yönlü yönlendirme yöntemleri ile karşılaştırılmış ve tek yönlü yönlendirmeden daha etkin bir sonuç sağladığı belirtilmiştir.

Saldırı olaylarının çevre SDN kontrolcüleri ile paylaşılabilmesini sağlayacak şekilde genişletilmesini ve SDNi (SDN interface) protokolünün kullanılmasını öneren bir çalışmada [69], saldırı ile ilgili olay kaydı diğer SDN ağlarına gönderilmektedir. Bu olay kaydı, kaynak olabilecek ağa doğru gönderilerek tehdidin kaynağında sonlandırılması için çalışılmaktadır. Önerilen yöntemde SDN ağları komşu ağların davranışlarını değerlendirerek güvenilirliklerini hesaplanmakta ve buna göre işlemler yapmaktadır.

DDoS saldırılarında sunucuların gerçek IP adresleri dinamik olarak güncellenip çok sayıda IP adresi arasında gizlenebilmekte ve gerçek trafik ile saldırı trafiği dağıtılabilmektedir. IP Fast Hopping olarak adlandırılan bu yaklaşımda [70] sunucuların DDoS saldırılarında kaynaklarını tüketmeleri engellenmektedir.

SDN kontrolcüsü ile sunuculara sanal IP adresi verilerek gerçek IP adresini yetkili olmayan sistemlerden gizleme de bir diğer DDoS engelleme yöntemidir. Bu doğrultuda Jafarian ve ark. [71] tarafından önerilen OF-RHM (OpenFlow Random Host Mutation) isimli yöntemde, OpenFlow ile hareketli hedef savunma stratejisi oluşturulmaktadır. DNS sunucularında ağdaki bilgisayarların internet adresleri için sanal IP adresleri saklanmakta ve bu sanal IP adresleri SDN kontrolcüsü tarafından gerçek IP adreslerine dönüştürülerek hedef sunuculara erişim sağlanabilmektedir. Sanal IP adresleri sürekli değiştirilerek sunucuların mantıksal anlamda hareketli olması sağlanmaktadır. Önerilen yöntemin gizli taramalara, bilgisayar solucanlarının yayılımına ve diğer tarama temelli saldırılara karşı etkili olduğu gösterilmiştir.

Yazılım tanımlı ağların özellikleri kullanılarak DDoS saldırılarından korunmanın bir diğer yolu ise birbirleriyle işbirliği yapan otonom ağlar oluşturmaktır [72]. Bu mantığa dayalı ajan temelli ağ kontrol sistemi olan AgNOS tarafından ağa bir saldırı olduğuna karar verildiğinde bu durum SDN kontrolcüsüne ve diğer AgNOS ajanlarına iletilmektedir. Ajanlar birbirleri ile etkileşimde bulunarak saldırıyı işbirliği ile engellemeye çalışmaktadır. Wang ve ark. [73] tarafından önerilen yöntemde ise DDoS saldırılarından korunmak için IP ağ altyapılarının üstüne bulut bilişim ve yazılım tanımlı ağların özellikleri kullanılmaktadır. Ağ trafiği üç ağdan geçecek (kaynağa yakın ağ, çekirdek ağ ve hedefe yakın ağ) şekilde yönetilmektedir. Bu mimari, uygulama katmanında kimlik doğrulama ve kayıt modülü, erişim kontrol modülü, denetim modülü, kural yönetim modülünden oluşmaktadır.

5.4.2. Yazılım Tanımlı Ağlarda Gerçekleştirilen DDoS Saldırılarının Tespiti

SDN'de gerçekleştirilen DDoS saldırılarının tespiti için yapay sinir ağları, Bayes ağları, destek vektör makinesi, genetik algoritma ve bulanık mantık gibi yöntemler kullanan çözümler geliştirilmiştir [74]. Örneğin, Li ve ark. [75] tarafından önerilen yöntemle çapraz doğrulama genetik algoritması ve destek vektör makinesi (SVM) sı-

nıflandırıcı kullanılarak DDoS saldırıları tespit edilmeye çalışılmaktadır. [76] nolu çalışmada da DDoS saldırılarının tespiti için benzer şekilde AVL ağacı ile optimize edilmiş destek vektör makinesi kullanılmıştır.

DDoS saldırılarının tespit edilebilmesi için ağ trafiğinin ve trafik yoğunluğunun etkin şekilde izlenebilmesi gerekmektedir. Wang ve ark. [77] tarafından yapılan çalışmada ağdaki trafik yoğunluğunun ve saldırı yoğunluğunun tespit edilebilmesi için bulanık mantık ve istatistik teorisine dayalı yöntem önerilmiştir. Yöntemde trafik, normal trafik davranışı ve normal ağ yoğunluğu davranışı ile sürekli karşılaştırılmaktadır. Önerilen yöntem SDN ağlarına uyarlanmış ve yapılan değerlendirmelerde DDoS saldırılarına karşı %95 önleme sağlandığı ifade edilmiştir. Trung ve ark. [78] ise kesin karar eşik değerleri ve bulanık çıkarım sistemleri kullanan bir çoklu kriter temelli saldırı önleme mekanizması önermişlerdir. Mekanizmada, saldırı tespit edildikten sonra SDN kontrolcüsü ile iletişime geçilerek saldırı engellenmeye çalışılmaktadır. Aynı amaçla Xu ve Lu [79] tarafından geliştirilen sistemde DDoS saldırılarını tespit etmek için yazılım tanımlı ağlardan akış hacmi (flow volume) ve akış oranı asimetrisi (flow rate asymmetry) istatistikleri için bilgi toplanmaktadır. Önerilen yöntemde potansiyel saldırganları ve hedefi bulmak için SDN anahtarlarından toplanan bilgilerin ayrıntı seviyesi adaptif olarak hem ardışık ve hem de eş zamanlı olacak şekilde değiştirilmektedir. Çalışmada, önerilen yöntem farklı parametre değerleri ile test edilmiş ve elde edilen sonuçlar paylaşılmıştır.

Wang ve ark. [80] tarafından önerilen yöntemde ise ağ trafiğindeki kaynak-hedef IP adresi çifti ile tarihsel olarak gerçek kaynak-hedef IP adresi veritabanı oluşturulmaktadır. Yeni gelen trafik parametrik olmayan CUSUM (cumulative sum control chart) algoritması ile analiz edilmekte ve DDoS saldırıları hızlı şekilde ve belirli kesinlikte tespit edilmeye çalışılmaktadır. Anormal durum tespit edildiğinde akış ağdaki bir özel cihaza yönlendirilerek saldırının ayrıntılı biçimde analiz edilmesi sağlanmaktadır. Yapılan deneyler sonucunda yöntemin SDN üzerindeki DDoS saldırılarında iyi bir performans sergilediği belirtilmiştir.

5.5. Değerlendirmeler

Yazılım Tanımlı Ağlar (SDN) ağdaki kontrol birimini altyapıdaki yönlendirici ve anahtarlardan ayırarak merkezi bir yazılım birimine veren ve kontrolcü adı verilen bu birim tarafından ağın programlanmasına imkân sağlayan yeni bir teknolojidir. SDN, bu özellikleri sayesinde geleneksel ağlara kıyasla daha esnek ve yönetilebilir ağlar oluşturma fırsatı sunmaktadır.

SDN'de siber güvenliğin sağlanması için saldırı tespiti yapan (saldırı tespit sistemi, zararlı yazılım tarayıcılar, DDoS detektörü ve derin paket inceleme), engelleyen (güvenlik duvarı, saldırı engelleme sistemi) ve saldırı yakalayan (balküpü) güvenlik fonksiyonlarının sanallaştırılarak ilgili sunucular üzerinde çalıştırılması yöntemi giderek yaygınlaşmaktadır.

SDN ağ güvenliğinin sağlanmasında birçok kolaylığı beraberinde getirmektedir. Merkezi kontrolcü yazılımı tarafından trafiğin dinamik bir şekilde izlenmesi ve denetlenmesi, saldırıların daha başarılı bir şekilde önlenmesini ve tespit edilmesini sağlamaktadır. Ayrıca programlanabilir ağ mantığı sayesinde siber güvenlik fonksiyonlarının çok daha kolay bir şekilde geliştirilebilmesi, ağa yerleştirilmesi, güncellenebilmesi ve diğer fonksiyonlarla etkileşiminin sağlanması sürdürülebilir bir güvenlik sağlanmasında etkin rol oynamaktadır.

Fakat SDN'in sunduğu bu özellikler yüzde yüz güvenlik sağlamadığı gibi sunulan bu yeni mimari mantığı birçok yeni saldırı türünü de beraberinde getirmektedir. Kontrolcünün güvenliğinin sağlanmadığı durumda saldırıların yalnızca bu yazılımı hedef alması bile yeterli olmakta ve tüm ağ işleyişini bozacak etkiler yaratabilmektedir. Öte yandan açık yapısından dolayı saldırganlar kontrolcü veya uygulama yazılımlarına kötü niyetli kod parçacıkları enjekte ederek ciddi tehditler oluşturabilmektedirler. Ayrıca, yazılım tanımlı ağlarda desteklenen protokollerin çeşitliliği ve farklı görevleri olan yazılımların sanallaştırma yoluyla aynı fiziksel sunucularda yer alabilmesi, bu mimaride geleneksel ağlara göre daha çok saldırı noktası ortaya çıkarmaktadır.

Sonuç olarak yazılım tanımlı ağlar ve siber güvenlik konuları bir arada değerlendirildiğinde;

- uygulama-veri katmanı işlem güvenliğinin sağlanması,
- güvenli ağ haritasının oluşturulması ve yönetilmesi,
- hareketli hedef savunması için SDN kullanımı,
- güvenlik değerlendirme çatıları,
- servis olarak ağ güvenliği hizmetleri ile
- ağ fonksiyonu sanallaştırma

konularının önem kazandığı görülmektedir.

Ayrıca yazılım tanımlı ağlarda DDoS vb. saldırıların tespiti ve önlenmesi amacı ile aşağıdaki konularda daha çok araştırmaya ihtiyaç duyulmaktadır. Bunlar:

- Düşük yoğunluklu DDoS ve mobil saldırılara karşı mücadele yöntemleri
- Birden fazla noktadan savunma ve işbirliği yöntemleri
- Yazılım tanımlı ağlarda bütün protokol katmanlarını içerecek şekilde ağ trafiğinin analiz edilebilmesi ve trafik analizlerinin savunma olarak kullanılması ve
- DDoS saldırılarına toleranslı sistemlerin geliştirilmesidir.

Son olarak yazılım tanımlı ağlarda siber saldırıların önlenmesi için büyük verinin, ağ fonksiyonu sanallaştırmanın ve bilgi merkezli ağların kullanılabileceği ifade edilmekte ve yakın gelecekte bu konulardaki araştırmaların artacağı değerlendirilmektedir.

Kaynaklar

[1] Hu, F., Hao, Q., & Bao, K. (2014). A survey on software-defined network and openFlow: from concept to implementation. *IEEE Communications Surveys & Tutorials*, 16(4), 2181-2206.

[2] Hakiri, A., Gokhale, A., Berthou, P., Schmidt, D. C., & Gayraud, T. (2014). Software-defined networking: Challenges and research opportunities for future internet. *Computer Networks*, 75, 453-471.

[3] Dhamecha, K., & Trivedi, B. (2013). SDN Issues-A Survey. *International Journal of Computer Applications*, 73(18).

[4] Ranjan, P., Pande, P., Oswal, R., Qurani, Z., & Bedi, R. (2014). A Survey of Past, Present and Future of Software Defined Networking.

International Journal of Advance Research in Computer Science and Management Studies, 2(4).

[5] Bronzino, F., Maheshwari, S., Seskar, I., & Raychaudhuri, D. (2019). NOVN: named-object based virtual network architecture. *20th International Conference on Distributed Computing and Networking*, 90-99.

[6] Jammal, M., Singh, T., Shami, A., Asal, R., & Li, Y. (2014). Software defined networking: State of the art and research challenges. *Computer Networks*, 72, 74-98.

[7] Nunes, B. A., Mendonca, M., Nguyen, X. N., Obraczka, K., & Turletti, T. (2014). A survey of software-defined networking: Past, present, and future of programmable networks. *IEEE Communications Surveys & Tutorials*, *16*(3), 1617-1634.

[8] Kreutz, D., Ramos, F. M., Esteves Verissimo, P., Esteve Rothenberg, C., Azodolmolky, S., & Uhlig, S. (2015). Software-defined networking: A comprehensive survey. *Proceedings of the IEEE*, 103(1), 14-76.

[9] Farhady, H., Lee, H., & Nakao, A. (2015). Software-defined networking: A survey. *Computer Networks*, 81, 79-95.

[10] Xie, J., Guo, D., Hu, Z., Qu, T., & Lv, P. (2015). Control plane of software defined networks: A survey. *Computer Communications*, 67, 1-10.

[11] Ali, S. T., Sivaraman, V., Radford, A., & Jha, S. (2015). A survey of securing networks using software defined networking. *IEEE Transactions on Reliability*, 64(3), 1086-1097.

[12] Jarraya, Y., Madi, T., & Debbabi, M. (2014). A survey and a layered taxonomy of software-defined networking. *Communications Surveys & Tutorials,* IEEE, 16(4), 1955-1980.

[13] Open Networking Foundation, "OpenFlow Specifications", URL: https://www.opennetworking.org/software-defined-standards/specifications/, Son Erişim Tarihi: 30.03.2019.

[14] Demirci, M. "Yazılım Tanımlı Ağlar ders notları", URL: https://websitem.gazi.edu.tr/site/mdemirci/posts/view/id/124767, Son Erişim Tarihi: 30.03.2019.

[15] Ahmad, I., Namal, S., Ylianttila, M., & Gurtov, A. (2015). Security in software defined networks: a survey. *IEEE Communications Surveys & Tutorials*, 17(4), 2317-2346.

[16] Shin, S., Xu, L., Hong, S., & Gu, G. (2016). Enhancing network security through software defined networking (SDN). *25th International Conference on Computer Communication and Networks*, 1-9.

[17] Shu, Z., Wan, J., Li, D., Lin, J., Vasilakos, A. V., & Imran, M. (2016). Security in software-defined networking: Threats and countermeasures. *Mobile Networks and Applications*, 21(5), 764-776.

[18] Zarca, A. M., Bernabe, J. B., Trapero, R., Rivera, D., Villalobos, J., Skarmeta, A., & Gouvas, P. (2019). Security Management Architecture for NFV/SDN-aware IoT Systems. *IEEE Internet of Things Journal*.

[19] Yan, Q., Yu, F. R., Gong, Q., & Li, J. (2016). Software-defined networking (SDN) and distributed denial of service (DDoS) attacks in cloud computing environments: A survey, some research issues, and challenges. *IEEE Communications Surveys & Tutorials*, 18(1), 602-622.

[20] Scott-Hayward, S., O'Callaghan, G., & Sezer, S. (2013). SDN security: A survey. *IEEE SDN for Future Networks and Services*, 1-7.

[21] Hu, H., & Ahn, G. J. Virtualizing and Utilizing Network Security Functions for Securing Software Defined Infrastructure.

[22] Jarraya, Y., Shameli-Sendi, A., Pourzandi, M., & Cheriet, M. (2015). Multistage OCDO: Scalable Security Provisioning Optimization in SDN-based Cloud, 2015 *IEEE 8th International Conference on Cloud Computing*, 572-579)

[23] Krishnaswamy, D., Kothari, R., & Gabale, V. (2015). Latency and policy aware hierarchical partitioning for NFV systems, 2015 *IEEE Conference on Network Function Virtualization and Software Defined Network*, 205-211.

[24] Hande, Y., Jadhav, A., Patil, A., Zagade, R. (2014). Software Defined Networking with Intrusion Detection System, *International Journal of Engineering and Technical Research*, , 2(10), 19-21.

[25] Xiong, Z. (2014). An SDN-based IPS Development Framework in Cloud Networking Environment (*Doctoral dissertation*, Arizona State University).

[26] Modi, C., & Patel, D. (2018). A feasible approach to intrusion detection in virtual network layer of Cloud computing. *Sādhanā*, 43(7), 114.

[27] Benkhelifa, E., Welsh, T., & Hamouda, W. (2018). A Critical Review of Practices and Challenges in Intrusion Detection Systems for IoT: Toward Universal and Resilient Systems. *IEEE Communications Surveys & Tutorials*, 20(4), 3496-3509.

[28] Van Adrichem, N. L., Doerr, C., & Kuipers, F. A. (2014). Opennetmon: Network monitoring in openflow software-defined networks. *IEEE Conference on Network Operations and Management Symposium*, 1-8.

[29] Ceron, J. M., Margi, C. B., & Granville, L. Z. (2016). Mars: An sdn-based malware analysis solution. *IEEE Symposium on Computers and Communication*, 525-530.

[30] Yusof, A. R. A., Udzir, N. I., & Selamat, A. (2019). Systematic literature review and taxonomy for DDoS attack detection and prediction. *International Journal of Digital Enterprise Technology*, 1(3), 292-315.

[31] Braga, R., Mota, E., & Passito, A. (2010). Lightweight DDoS flooding attack detection using NOX/OpenFlow. *IEEE 35th Conference on Local Computer Networks,* 408-415.

[32] De La Torre, G., Rad, P., & Choo, K. K. R. (2019). Implementation of deep packet inspection in smart grids and industrial Internet of Things: Challenges and opportunities. *Journal of Network and Computer Applications*.

[33] Sun, X., Li, H., Zhao, D., Lu, X., Hou, K., & Hu, C. (2019). COIN: A fast packet inspection method over compressed traffic. *Journal of Network and Computer Applications*, 127, 122-134.

[34] Bouet, M., Leguay, J., Combe, T., & Conan, V. (2015). Cost-based placement of vDPI functions in NFV infrastructures. *International Journal of Network Management*, 25(6), 490-506.

[35] Bremler-Barr, A., Harchol, Y., Hay, D., & Koral, Y. (2014). Deep packet inspection as a service. *International on Conference on emerging Networking Experiments and Technologies,* 271-282.

[36] Hu, H., Han, W., Ahn, G. J., & Zhao, Z. (2014). FLOWGUARD: building robust firewalls for software-defined networks. *Workshop on Hot topics in software defined networking,* 97-102.

[37] François, J., Dolberg, L., Festor, O., & Engel, T. (2014). Network security through software defined networking: a survey. *Conference on Principles, Systems and Applications of IP Telecommunications*, 6.

[38] Suh, M., Park, S. H., Lee, B., & Yang, S. (2014). Building firewall over the software-defined network controller. *16th International Conference on Advanced Communication Technology*, 744-748.

[39] Hu, H., Ahn, G. J., Han, W., & Zhao, Z. (2014). Towards a reliable SDN firewall. *Open Networking Summit 2014*.

[40] Morzhov, S., Alekseev, I., & Nikitinskiy, M. (2016). Firewall application for Floodlight SDN controller. *International Siberian Conference on Control and Communications,* 1-5.

[41] Kartheek, D. N. (2013). Towards Secured Firewalls for Software Defined Networks, *ACM SIGCOMM workshop on Hot topics in software defined networking*. 55-60.

[42] Zhang, L., Shou, G., Hu, Y., & Guo, Z. (2013). Deployment of intrusion prevention system based on software defined networking. *15th IEEE International Conference on Communication Technology,* 26-31.

[43] Shin, S., Porras, P., Yegneswaran, V., Fong, M., & Gu, G., (2013). "FRESCO: Modular Composable Security Services for Software-Defined Networks", *Network and Distributed System Security Symposium,* 1-16.

[44] Zargar, S. T., Joshi, J., & Tipper, D. (2013). "A Survey of Defense Mechanisms Against Distributed Denial of Service (DDOS) Flooding Attacks", *IEEE Communications Surveys and Tutorials*, 5(4), 2046-2069.

[45] Mirkovic, J., & Reiher, P. (2004). "A Taxonomy of DDoS Attack and DDoS Defense Mechanisms", *ACM SIGCOMM Computer Communication Review*, 34(2), 39-53.

[46] Douligeris, C., & Mitrokotsa, A. (2004). "DDoS Attacks and Defense Mechanisms: Classification and State-of-the-Art", *Computer Networks*, 44(5), 643-666.

[47] Peng, T., Leckie, C., & Ramamohanarao, K. (2007). "Survey of network-based defense mechanisms countering the DoS and DDoS problems", *ACM Computing Surveys*, 39(1) 3.

[48] Shameli-Sendi, A., Pourzandi, M., Fekih-Ahmed, M., & Cheriet, M. (2015). "Taxonomy of Distributed Denial of Service Mitigation Approaches for Cloud Computing", *Journal of Network and Computer Applications*, 58, 165-179.

[49] Sahay, R., Blanc, G., Zhang, Z., & Debar, H. (2015). "Towards Autonomic DDoS Mitigation using Software Defined Networking", *NDSS Workshop on Security of Emerging Technologies*, 1-7.

[50] Arins, A., "Firewall as a Service in SDN OpenFlow Network", (2015). *IEEE 3rd Workshop on Advances in Information, Electronic and Electrical Engineering,* 1-5.

[51] Le, A., Dinh, P., Le, H., & Tran, N. C. (2016). "Flexible Network-Based Intrusion Detection and Prevention System on Software-Defined Networks", *International Conference on Advanced Computing and Applications*, Ho Chi Minh City, Vietnam, 106-111.

[52] Lopez, M. A., & Duarte, O. C. M. B. (2015). "Providing Elasticity to Intrusion Detection Systems in Virtualized Software Defined Networks", *IEEE International Conference on Communications*, 7120-7125.

[53] Lopez, M. A., Ferrazani Mattos, D. M., & Duarte, O. C. M. B. (2016). "An Elastic Intrusion Detection System for Software Networks", *Annals of Telecommunications*, 1-11.

[54] Chin, T., Mountrouidou, X., Li, X., & Xiong, K. (2015). "An SDN-Supported Collaborative Approach for DDoS Flooding Detection and Containment", *IEEE Military Communications Conference*, 659-664.

[55] Yoon, C., Park, T., Lee, S., Kang, H., Shin, S., & Zhang, Z. (2015). "Enabling Security Functions with SDN: A Feasibility Study", *Computer Networks,* 85, 19-35.

[56] Fayaz, S. K., Tobioka, Y., Sekar, V., Bailey, M., & Bailey, M. (2015). "Bohatei: Flexible and Elastic DDoS Defense", *24th USENIX Security Symposium*, 817-832.

[57] Li, C., Wu, Y., Yuan, X., Sun, Z., Wang, W., Li, X., & Gong, L. (2018). "Detection and Defense of DDoS Attack Based on Deep Learning in OpenFlow-Based SDN," *International Journal of Communication Systems*, 31(5) e3497.

[58] Kim, J., Firoozjaei, M. D., Jeong, J. P., Kim, H., & Park, J.S. (2015). "SDN-Based Security Services Using Interface to Network Security Functions", *International Conference on Information and Communication Technology Convergence*, 526-529, 2015.

[59] Luo, S., Wu, J., Li, J., & Pei, B., (2015). "A Defense Mechanism for Distributed Denial of Service Attack in Software-Defined Networks", *9th International Conference on Frontier of Computer Science and Technology*, 325-329.

[60] Hussein, A., Elhajj, I. H., Chehab, A., & Kayssi, A. (2016). "SDN Security Plane: An Architecture for Resilient Security Services", *IEEE International Conference on Cloud Engineering Workshop*, 54-59.

[61] Giotis, K., Argyropoulos, C., Androulidakis, G., Kalogeras, D., & Maglaris, V. (2014). "Combining OpenFlow and sFlow for an Effective and Scalable Anomaly Detection and Mitigation Mechanism on SDN Environments", *Computer Networks*, 62, 122-136.

[62] Seeber, S., Stiemert, L., & Rodosek, G. D. (2015). "Towards an SDN-Enabled IDS Environment", *IEEE Conference on Communications and Network Securit*y, 751-752.

[63] Belyaev, M., & Gaivoronski, S. (2014). "Towards Load Balancing in SDN-Networks During DDoS-Attacks", *International Science and Technology Conference (Modern Networking Technologies)*, 1-6.

[64] Giotis, K., Androulidakis, G., & Maglaris, V. (2014). "Leveraging SDN for Efficient Anomaly Detection and Mitigation on Legacy Networks", *3th European Workshop on Software Defined Networks*, 85-90.

[65] Giotis, K., Androulidakis, G., & Maglaris, V. (2016). "A Scalable Anomaly Detection and Mitigation Architecture for Legacy Networks via an OpenFlow Middlebox", *Security and Communication Networks*, 9(13), 1958-1970.

[66] Kalliola, A., Lee, K., Lee, H., & Aura, T. (2015). "Flooding DDoS Mitigation and Traffic Management with Software Defined Networking", *IEEE 4th International Conference On Cloud Networking*, 248-254.

[67] Duan, Q., Al-Shaer, E., & Jafarian, H. (2013). "Efficient Random Route Mutation Considering Flow and Network Constraints", *IEEE Conference on Communications and Network Security*, 260-268.

[68] Jafarian, J. H., Al-Shaer, E., & Duan, Q. (2013). "Formal Approach for Route Agility Against Persistent Attackers", *Lecture Notes in Computer Science*, 8134, 237-254.

[69] Giotis, K., Apostolaki, M., & Maglaris, V. (2016). "A Reputation-Based Collaborative Schema for the Mitigation of Distributed Attacks in SDN Domains", *IEEE/IFIP Network Operations and Management Symposium*, , 495-501.

[70] Krylov, V., Kravtsov, K., Sokolova, E., & Lyakhmanov, D. (2014). "SDI Defense Against DDoS Attacks Based on IP Fast Hopping Method", *International Science and Technology Conference (Modern Networking Technologies)*, 1-5.

[71] Jafarian, J. H., Al-Shaer, E., & Duan, Q. (2012). "Openflow Random Host Mutation: Transparent Moving Target Defense Using Software Defined Networking", *1st Workshop on Hot Topics in Software Defined Networks*, 127-132.

[72] Passito, A., Mota, E., Bennesby, R., & Fonseca, P. (2014). "AgNOS: A Framework for Autonomous Control of Software-Defined Networks", *IEEE 28th International Conference on Advanced Information Networking and Applications*, 405-412.

[73] Wang, X., Chen, M., & Xing, C. (2015). "SDSNM: A Software-Defined Security Networking Mechanism to Defend against DDoS Attacks", *9th International Conference on Frontier of Computer Science and Technology*, 115-121.

[74] Ashraf, J., & Latif, S. (2014). "Handling Intrusion and DDoS Attacks in Software Defined Networks Using Machine Learning Techniques", *National Software Engineering Conference*, 55-60.

[75] Li, X., Yuan, D., Hu, H., Ran, J., & Li, S. (2015). "DDoS Detection in SDN Switches Using Support Vector Machine Classifier", *Joint International Mechanical, Electronic and Information Technology Conference*, 10, 344-348.

[76] RT, K., Selvi, S. T., & Govindarajan, K. (2014). "DDoS Detection and Analysis in SDN-Based Environment Using Support Vector Machine Classifier", *International Conference on Advanced Computing*, 205-210.

[77] Wang, B., Zheng, Y., Lou, W., & Hou, Y. T. (2015). "DDoS Attack Protection in the Era of Cloud Computing and Software-Defined Networking", *Computer Networks*, 81, 308-319.

[78] Trung, P. Van, Huong, T. T., Tuyen, D. Van, Duc, D. M., Thanh, N. H., & Marshall, A. (2015). "A Multi-Criteria-Based DDoS-Attack Prevention Solution Using Software Defined Networking", *International Conference on Advanced Technologies for Communications*, 308-313.

[79] Xu, Y., & Liu, Y. (2016). "DDoS Attack Detection Under SDN Context", *35th Annual IEEE International Conference on Computer Communications*, 1-9.

[80] Wang, X., Chen, M., Xing, C., & Zhang, T. (2016). "Defending DDoS Attacks in Software-Defined Networking Based on Legitimate Source and Destination IP Address Database", *IEICE Transactions on Information and Systems*, E99D(4), 850-859.

Web Uygulama Zafiyetleri ve Önlemler

BÖLÜM 6

Onur AKTAŞ
Prof. Dr. Şeref SAĞIROĞLU

WEB UYGULAMA ZAFİYETLERİ VE ÖNLEMLER

Bu bölümde; web uygulamalarında kullanılan teknolojiler, servisler ve http protokolü hakkında bilgiler sunulmuş; siber güvenliğin temel yaklaşımları, bilgi güvenliği kavramları, karşılaşılan tehditler, güvenlik testlerinin saldırganlardan ve siber güvenlik uzmanları tarafından kullanılan bilgi toplama aşaması incelenmiş; web uygulamalarındaki zafiyetler ve çözüm önerilerine yönelik çalışmalara yönelik bilgiler sunulmuş; kelime listesinin oluşturulması ve bilgi toplama aşamasında kullanılması ele alınmış; senaryolar üzerinden zafiyet içeren sistemler oluşturulmuş ve bilgi toplama sonrasında oluşabilecek zafiyetler incelenmiş; elde edilen sonuçlar sunulmuş ve önerilerde bulunulmuştur. Bu kitap bölümü [83] nolu kaynakta verilen tezin bir kısmı alınarak oluşturulmuş ve özetlenmiştir.

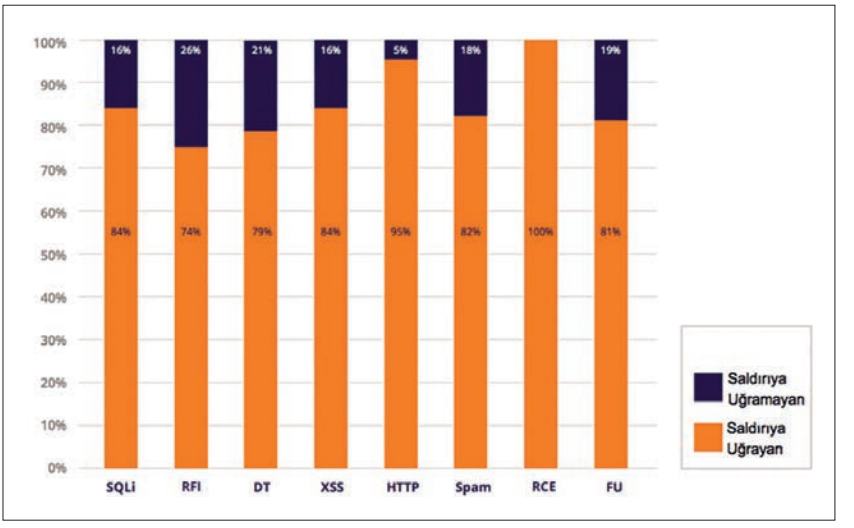
6.1. Web Uygulamaları ve Tehditler

Web uygulamaları insanların günlük hayatının neredeyse ayrılmaz bir parçası haline gelmiştir. Kullanıcıların internet üzerinden eriştikleri web uygulamaları dünyanın en büyükleri arasına girebilen firmalara dönüşmüştür. Oldukça fazla sayıda içerikten oluşabilen ve kullanıcıların içerikleri ile büyüyen web uygulamaları önemli birer bilgi kaynağı haline gelmiştir. E-ticaret uygulamaları büyük cirolar ile işlem yapabilecek kadar büyümüş ve yüz binlerce kişiye hizmet verebilecek kapasiteye erişmiştir [1].

Yalnızca büyük firmalar tarafından değil kamu kurumları, küçük ve orta ölçekli firmalar tarafından da web uygulamaları birçok farklı amaç için kullanılmaktadır. Kamu kurumları insan kaynağı edinimi, çeşitli konularda duyuru veya bilgilendirme yayınlama, güncel haberleri iletmek, e-posta listelerini yönetmek, iletişimi kolaylaştırmak ve daha birçok farklı amaç için web uygulamaları kullanmak-

tadır. Bunların yanında kamu kurumları arasındaki bilgi paylaşımı ve kullanıcılara sunulan hizmetler yine web uygulamaları tarafından sağlanmaktadır. Küçük ve orta ölçekli firmalar ise ürün/hizmet tanıtımı, iletişim bilgilerini iletmek, müşteri çekmek veya insan kaynağını yönetimi gibi farklı farklı amaçlar doğrultusunda web uygulamaları kullanabilmektedirler.

Web uygulamalarında kullanılan bilginin farklı nedenlerden dolayı siber saldırganlar tarafından hedef olmaktadırlar. Bu nedenle web uygulamalarında bilgi güvenliğinin sağlanması önem arz etmektedir. Şekil 6.1'de [2] nolu kaynakta yayınlanan seçilmiş bazı web uygulamalarına yönelik saldırıların incelenmesi sonucu oluşturulan grafik yer almaktadır. Grafikte web uygulamaların çok büyük oranının farklı türdeki siber saldırılara maruz kaldığı görülmektedir.



Şekil 6.1. Web uygulama saldırılarının dağılımı [2]

Siber saldırıların artması alınması gereken önlemleri de beraberinde getirmektedir. Siber güvenlik uzmanları tarafından gerçekleştirilen güvenlik testleri veya zafiyet analizlerinin amacı saldırganlarda önce ilgili sistemlerdeki zafiyetleri tespit ederek oluşabilecek maddi veya manevi zararların engellenmesidir. Web uygulamalarına yönelik güvenlik testlerinde zafiyet tarama araçları sıklıkla kullanılmaktadır [3]. Bu zafiyet tarama araçları ilgili web uygulamaları otomatik olarak belirli kurallara göre tarayarak zafiyetleri tespit etmeye yönelik işlemler

gerçekleştirmektedir. Otomatik olarak zafiyetlerin tespiti ve daha az zaman ve kaynak ile daha fazla güvenlik anlamına gelmektedir [4]. Zafiyet tarama araçlarının başarısı sahip oldukları imza veri tabanları ve kullandıkları siber saldırı yöntemlerine göre değişmektedir. Zafiyet tarama araçları, siber saldırı yöntemleri ve bu saldırıların tespitine yönelik çalışmaların literatürde yer almaktadır [5-9].

Zafiyet tespit aşamasında kullanılan tarama araçları web uygulamalarında tespit edebildikleri tüm sayfalara erişip gerekli kontrolleri yapmaktadır. Fakat web uygulamaları içerisinde bağlantı verilmemiş ve dolayısıyla otomatik araçlar tarafından tespit edilemeyen sayfalar zafiyet taramalarının dışarısında kalmaktadır. Zafiyet kontrollerinden geçmeyen bu sayfaların saldırganlar tarafından tespit edilmesi durumunda güvenlik ihlalleri ortaya çıkabilir. Bu gizli sayfalar bir kelime listesinin web uygulama bağlantısında sürekli olarak denenmesi ile tespit edilebilir. Tespit edilen yeni bağlantı içerisinde bir zafiyet olması durumunda bu zafiyet saldırganlar tarafından sömürülebilir (Bkz. Şekil 6.2).

Şekil 6.2. Gizli kalmış bağlantılar

Gizli kalmış bağlantıların tespiti için bir kelime listesinin web uygulamasındaki bağlantıya otomatik olarak deneyen ve bağlantının varlığı tespit eden birçok açık kaynak yazılım bulunmaktadır [10-15]. Bu yazılımların tamamın denediği kelime listelerinin içerisinde yalnızca İngilizce kelimeler bulunmaktadır. Fakat Türkçe web sayfalarındaki bağlantılarda Türkçe kelimeler kullanılabilmektedir. Bir web uygulamasında yönetim ara yüzüne erişim için 'ornek.com/admin' yerine 'ornek.com/yönetim-paneli' kullanılması durumunda açık kaynak yazılımların mevcut kelime listeleri bağlantıyı tespit edemeyecektir. Bu da ileride oluşabilecek güvenlik ihlallerinin riskini arttırmaktadır.

Web uygulamaların dışarıdan bağlantı verilmeyen özel sayfalarına erişim için Türkçe kelimelerin kullanılması bilgi toplama veya zafiyet tarama amacıyla kullanılan araçların bağlantıyı tespit edememesine neden olacaktır. Tespit edilmesini sağlamak için Türkçe bir kelime listesinin güvenlik testlerinde kullanılan yazılımlara girdi olarak sağlanması gerekmektedir. Ülkemizde sızma testlerine yönelik milli yazılımlar ve yöntemlerin geliştirilmesi ülkemizde yapılan kurumsal bilgi güvenliği alanında yapılan ilk çalışmanın sonuç ve öneriler bölümünde yer almaktadır [16].

Web uygulamalarındaki güvenlik açıklıklarının önceden tespit edilmesi ve engellemesi giderek daha fazla önemli hale gelmektedir. Güvenlik testleri ve zafiyet analizleri güvenlik açıklıklarının saldırganlardan önce tespit edilip kapatılması için etkili yöntemlerdir. Her iki yöntemde de bilgi toplama aşamasında atak yüzeyinin doğru ve tam şekilde tespit edilmesi zafiyetlerin bulunma oranını arttıracaktır. Bu bölümde, Türkçe web uygulamalarının bağlantılarında kullanılabilecek kelime listesi belirlenerek, web uygulamalarında daha fazla atak yüzeyinin tespit edilmesi, tespit sonrası oluşabilecek zafiyetlerin incelenmesi, zafiyetlerin giderilmesine yönelik çalışmalar yapılması ve dolayısıyla daha fazla zafiyetin siber saldırganlardan önce tespit edilip giderilmesi amaçlanmıştır. Web uygulamalarında kullanılan Türkçe kelimelerin listesini belirlemeye yönelik ilk çalışma olduğundan dolayı hem literatüre hem de güvenlik testlerinde kullanılan yazılımlara girdi olmasıyla siber güvenlik uzmanlarına katkı sağlayacağı değerlendirilmektedir.

Oluşturulan Türkçe kelime listesinin saldırganlar tarafından kullanılarak oluşabilecek zararların önüne geçilmesi için Türkçe kelime listesi öncelikle Ulusal Siber Olaylara Müdahale Merkezi ile paylaşılacak, kritik kurumlar ve kamu kurumlarının bilgilendirilmesi sonrasında siber güvenlik uzmanlarına açılarak güvenlik testlerinde kullanılması sağlanacaktır.

6.2. Web Uygulamalarını Anlamak

Web uygulamaları yeni istekleri karşılamak için gelişmekte ve sürekli olarak yenilenmektedir. Bu yeni istekler gittikçe yönetimi ve geliştirilmesi karmaşık hal alan gelişmiş web uygulamaların ortaya

çıkmasına sebebiyet vermiştir. Böylece farklı teknolojiler ve yöntemler web uygulamalarına dahil olmuştur. Web uygulamalarının popülaritesi arttıkça web uygulamalarına yönelik siber tehditlerde artmıştır [17]. Web uygulamalarına gelen siber tehditleri daha iyi anlaşılması için uygulamaların alt yapılarının ve ilgili sistemlerin doğru anlaşılması gerekmektedir.

6.2.1. Web Uygulama Geliştirilmelerinde Kullanılan Diller ve Bağlantı Yapıları

Hypertext Markup Language (HTML) tarayıcılar tarafından yorumlanarak görsel öğelere dönüştürülen bir programlama dilidir. Bu dil kullanıcılara internette gezinme imkanı tanıyarak günümüzdeki web teknolojilerinin oluşmasını mümkün kılmıştır [18]. HTML statik bir dildir. Dinamik işlemler için web sunucularında başka programlama dilleri kullanılmaktadır. PHP, ASP.NET, Java, ColdFusion, Ruby, JavaScript, Perl, Python, Erlang gibi geliştirme dilleri en çok kullanılan web yazılımı geliştirme araçlarıdır [19]. PHP yazılım dili açık kaynak olup yorumlanan bir yazılım dilidir. Web sunucu tarafından PHP yorumlayıcısı kullanılarak web sayfalarının yorumlanıp, çıktısı kullanıcılara gösterilir.

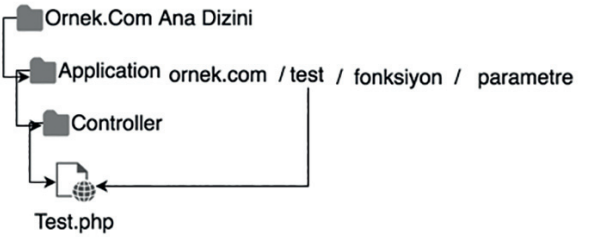
ASP.Net Microsoft firması tarafından geliştirilen dinamik web sayfaları oluşturan ve birçok özelliği içerisinde barındıran web uygulama geliştirme teknolojisidir. Java çalıştırılması için Java Sanal Makinasına ihtiyaç duyan ve desteklediği farklı teknolojiler ile web platformlarına aktarılabilen bir yazılım dilidir. Hem ASP.Net hem de Java dilinde geliştirilen uygulamaların sunucu üzerinde çalıştırılmadan önce derlenmesi gerekmektedir.

JavaScript yazılım dili genellikle istemci tarafından çalışan, istemci tarafında birçok özel işlemin yapılmasına olanak tanıyan bir dil olsa da JavaScript dili ile sunucu tarafında çalışan uygulamalar da geliştirilmiştir. JavaScript dili çerez erişimleri, HTML objelerinin değiştirilmesi, http isteklerinin gönderilmesi, form verilerinin değiştirilmesi gibi siber güvenlik açısından önemli işlemler gerçekleştirilmesine olanak tanımaktadır.

Web uygulamanın geliştirildiği teknoloji web uygulama sayfalarının uzantısını belirlemektedir. Genellikle PHP ile geliştirilmiş web

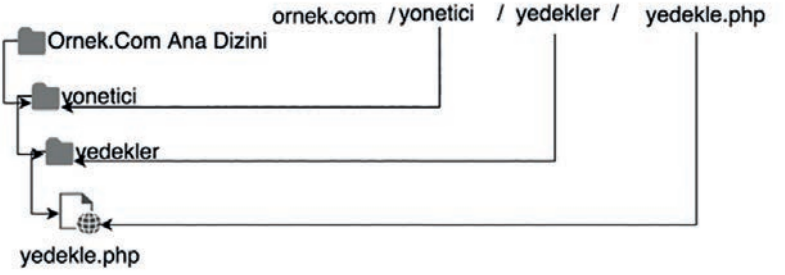
uygulamaları .php uzantılı web sayfalarına ASP.NET ile geliştirilmiş web uygulamaları ise '.aspx' uzantılı sayfalara sahip olmaktadır. Bu uzantılar web uygulamaların bağlantılarında da yer alabilir. Fakat web sunucularında yapılan ayarlar ile bu uzantılar gizlenebilir veya istenilen bir değer ile değiştirilebilir.

Web uygulamalarda geliştirmelerin hızlanması, güvenliğin sağlanması, farklı geliştiricilerin birlikte çalışabilmesi gibi nedenlerden dolayı web uygulama çatıları oluşturulmuştur. Bu çatıların çoğunda klasör ve dosya yapısı belirli kurallara bağlı olmakla birlikte bağlantı yapısı yazılım geliştiricileri tarafından belirlenmektedir. Şekil 6.3'de PHP ile geliştirilmiş açık kaynak bir çatı olan CodeIgniter'ın bağlantı yapısı gösterilmektedir [20].



Şekil 6.3. CodeIgniter'ın bağlantı yapısı

Bağlantı yapısında görülebileceği üzere dosya sistemi üzerindeki klasör yapısına bağlı olmaksızın bağlantı yapısı oluşturulabilir. Web sunucuları varsayılan olarak dosya sistemi üzerindeki klasör ve dosyaları bağlantı yapısı ile eşleştirmektedir. Şekil 6.4'de dosya sistemindeki web uygulama dosyasına ait dizin yapısının bağlantıda da kullanıldığı görülmektedir.

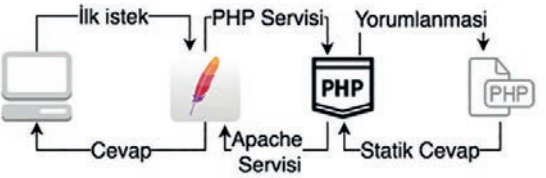


Şekil 6.4. Dosya yolu ve bağlantı yapısı

Bağlantı yapıları dizin veya kullanılan çatılardan bağımsız olarak web sunucularında URL yeniden yazma yöntemleri ile tamamıyla değiştirilebilir. Kullanılan bu yöntem ile bağlantı yapıları yazılım geliştiricilerin istediği şekilde dosya ve dizinlerden bağımsız olarak yapılandırılabilirler.

6.2.2. Web Sunucuları ve Veri Tabanları

Web uygulamaları HTTP protokolü üzerinden çalışmaktadırlar. Web sunucuları HTTP isteklerini işleyen sistemler veya servis olarak çalışan yazılımlar olarak tanımlanabilirler. Web sunucuların görevi gelen isteğe uygun cevabın ayarlanması ve bu cevabın karşı tarafa iletilmesidir. İletilen cevap içerisinde genellikle HTML kodları, resimler, betik kodları (Java Script) ve CSS kodları bulunmaktadır. Web sunucuları desteklediği programlama dilleri ile birlikte web uygulamalarına dinamik özellik sağlamaktadırlar. Bu sayede bir web sunucusu aldığı isteği, yazılım dilinin yorumlayıcısı ile birlikte çalışarak işlemekte ve yazılım dillerinin gücü web uygulamalarında kullanılabilmektedir. Şekil 6.5'de en çok kullanılan web sunucusu olan Apache yazılımının PHP programlama dili ile birlikte çalışması gösterilmektedir.



Şekil 6.5. Apache ve PHP'nin birlikte çalışması

Verilerin işlenmesi ve saklanması için veri tabanları bulunmaktadır. İlişkisel veri tabanları verilerin organize bir şekilde tablolara ve alanlara bölünebildiği içerisinde ilişkili verilerin saklana bildiği yapılardır. Web uygulamaları içerisinden bu yapılarda bulunan veriler sorgulanarak işlemektedir. Sorgular sırasında ekleme, silme veya düzenleme gibi çeşitli işlem yapılmaktadır. Stuctured Query Languages (SQL) ilişkisel veri tabanlarında sorgu yapmak için kullanılan özel bir dildir. Bu dil web uygulamanın geliştirildiği programlama dillinin içerisinde ilişkisel veri tabanlarında işlem yapmak için kullanılmaktadır.

Veri tabanları web sunucularından ayrı bir fiziksel sunucuda olabileceği gibi aynı sunucu içerisinde iki ayrı servis olarak da çalışabilirler. Veri tabanı sunucularının çalıştığı yetkileri, kullanılan servisin yazılımı, veri tabanında saklanan veriler ve veri tabanı kullanıcıları gibi bilgiler siber güvenlik açısından önem arz etmektedir. Yüksek yetki ile çalışan veri tabanı servisi, şifrelenmeden saklanan kritik veriler, yüksek yetkili veri tabanı kullanıcıları hem web uygulama hem de veri tabanı sunucusunda ciddi güvenlik ihlallerine yol açabilmektedir.

6.2.3. HTTP Protokolü

Tarayıcılar üzerinden erişilen web uygulamaları Hyper Text Transfer Protocol (HTTP) adı verilen bir protokol üzerinden çalışmaktadır. TCP/IP protokolü üzerinde uygulama seviyesinde çalışan HTTP protokolü Web'in çalışma altyapısını oluşturmaktadır [12]. Metin tabanlı olan bu protokol üzerinden yapılan istekler web sunucuya iletilmekte ve web sunucu tarafından dönen cevap tarayıcı tarafından yorumlanarak kullanıcıya gösterilmektedir. İstemci (web tarayıcıları) web sunucularına web sayfaları ve resimler gibi web elementlerine erişim istekleri göndermektedirler [21]. HTTP ile alakalı tüm kurallar Internet Engineering Task Force (IETF) ve World Wide Web Consortium (W3C) tarafından oluşturulup yönetilmektedir [22-23].

Web uygulamalarına erişim için HTTP standartlarına uygun bir istek ilgili sunucuya iletilmelidir. Bu isteği alan web sunucusu isteğin özelliklerine bakarak gerekli cevabı oluşturmalı ve son olarak cevabı göndermelidir. Gönderilen ve alınan tüm mesajlarda HTTP metotları veya durum kodlarının yanında başlık bilgileri bulunmaktadır. HTTP üzerinden işlenen diğer tüm veriler mesajların gövde bölümündedir. Yapılan istekler için HTTP metotları kullanılmaktadır. Bu metotlar web sunucunun gelen isteği nasıl işleyeceğini belirlemektedir. Çizelge 6.1'de HTTP metotları verilmektedir.

Çizelge 6.1. HTTP metotları

GET	HEAD	POST	PUT	DELETE
TRACE	OPTIONS	CONNECT	PATCH	

Çizelge 6.1'de belirtilen HTTP metotlarından GET metodu ile yapılan istekler yalnıza web sunucusu üzerinden istenilen sayfanın bilgisini alma amaçlı kullanılmaktadır. Tarayıcı tarafından herhangi bir web uygulama sayfasına GET isteği yapıldığında, istek yapılan sayfanın içeriği kullanıcıya geri döndürülmektedir. HEAD metodu ise GET ile benzer çalışmakla birlikte bu metotla yapılan isteklere cevabın gövdesi eklenmez. Sunucu tarafından yalnızca HTTP başlıkları iletilir. POST metodu genellikle bir kaynağı sunucu tarafına iletmek için kullanılmaktadır. GET metodu ile yapılan isteklerde veriler bağlantının içerisinde yer alırken POST isteklerinde bilgiler isteğin gövdesinde yer almaktadır. PUT metodu sunucu tarafında kaynağın yer değiştirilmesi veya oluşturulması, DELETE metodu silinmesi, PATCH metodu ise belirli düzenlemeler yapılması amacıyla kullanılmaktadır. CONNECT metodu bir proxy işlemleri, TRACE ileti döngüsü testi OPTIONS ise kullanılabilir metotları listelemek için kullanılmaktadır. Yapılan isteklere uygun olan cevaplar HTTP cevap kodları ile birlikte iletilmektedir. Web sunucularına yapılan her istek için, web sunucudan gelen cevap içerisinde bir HTTP cevap kodu bulunmaktadır. Cevap kodları toplam 3 haneli rakamlardan oluşmakta ve toplam beş farklı cevap kodu türü bulunmaktadır. Cevap kodlarındaki ilk rakam cevabın türünü belirtmektedir. Çizelge 6.2'de cevap kodları ve türü gösterilmektedir.

Çizelge 6.2. HTTP cevap kodları

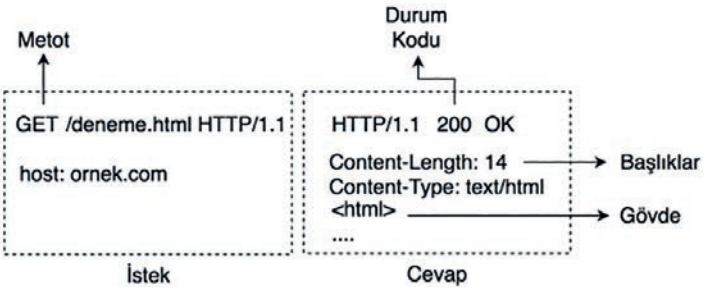
Kod	Anlamı
1xx	Bilgi
2xx	Başarılı
3xx	Yönlendirme
4xx	İstemci Hatası
5xx	Sunucu Hatası

Web sunucusu tarafından iki ile başlayan bir cevap kodu dönmesi, cevabın başarılı bir şekilde istemciye iletildiği anlamına gelmektedir. Üç ile başlayanlar iletilen mesaj sonrası yönlendirme isteklerinin yapılması gerektiği anlamını taşımaktadır. Dört ile başlayanlar

yapılan istekler istemcide bir hata olduğunu, beş ile başlayanlar ise sunucu tarafında bir hata olduğunu belirlemektedir.

Web uygulamalarında kullanılan bir bağlantının karşılığı olup olmadığı sunucudan dönen cevap kodları incelenerek tespit edilebilmektedir.

Hem istek hem de cevap mesajlarının içerisinde HTTP başlıkları bulunmaktadır. HTTP başlıkları başlık adı sonrasında iki nokta üst üste karakteri ve sonrasında değer bilgisi içermektedir. HTTP standartları içerisinde başlık bilgileri bulunmakla birlikte başlıklar yazılım geliştiricileri tarafından da düzenlenebilmektedir. Şekil 6.6'de örnek bir istek ve cevap mesajları görülmektedir.



Şekil 6.6. HTTP istek ve cevabı

6.2.4. Robots Exclusion Protokolu

Arama motorları erişilebilir web uygulamalarını düzenli olarak inceleyip içeriklerinin aranmasını sağlayarak son kullanıcılara hizmet sağlayan yapılardır. Google günümüzde en popüler arama motoru olarak bilinmektedir. Arama motorları sayfa içeriğinde yer alan bağlantıları takip ederek bir web uygulamasının tüm sayfalarını otomatik olarak gezerek kayıt etmektedir. Bazı sayfaların arama motorları tarafından kayıt edilmesi yazılım geliştiricileri veya uygulama sahipleri tarafından istenmeyebilir. Yönetici sayfaları, tema sayfaları, ön bellek klasörleri genellikle arama sonuçlarında çıkması istenmeyen sayfalardır. Bu durumda arama motorlarının otomatik olarak kayıt etme işlemi sunucu tarafında robots.txt dosyası içerisinde Robots Exclusion Protokolu kullanılarak limitlenebilir [24]. Google, Yandex, Bing gibi arama motorları tarafından kullanılan ve sürekli olarak interneti gezen sistemler web uygulamaların ana

dizindeki robots.xt dosyasına erişim yaparak indekslenmesine izin verilen ve izin verilmeyen dizinleri belirlerler. Bu işlem için robots.txt dosyası içerisinde dizin / sayfa bilgileri girilmesi gerekmektedir. Özel olarak arama motorları tarafından kayıt edilmesi istenmeyen sayfalar, arama motorları üzerinden yapılan arama sonuçlarında görünmemektedir. Fakat robots.txt dosyası tüm kullanıcılara açıktır. Bu da aslında arama motorlarından gizlenmek istenen sayfa veya dizinlerin kolaylıkla öğrenilmesi anlamını taşımaktadır.

Web uygulamalarında kullanılan teknolojiler sistemlere zarar vermek isteyen siber saldırganlar için birer bilgi kaynağı haline gelebilmektedir. Her ne kadar bu bilgiler sistemler üzerinde yapılan yapılandırmalar ile belirlense de siber saldırganlar bilgi toplama aşamalarında bu bilgileri gerçekleştirecekleri siber saldırıların hazırlık aşamalarında kullanabilmektedirler.

6.3. Web Uygulama Güvenliği

Günümüzde hızla gelişen teknoloji ve ihtiyaçlar siber dünyada işlenen bilginin niceliği ile birlikte niteliğini de arttırmaktadır. E-ticaretten, sağlık uygulamalarına kadar birçok alanda kullanılan web uygulamaları günlük hayattın ayrılmaz parçalarıdır. Büyük miktarda önemli veriler web uygulamaları tarafından kayıt edildiğinden saldırganlar tarafından önemli bir hedef haline gelmekte dolayısıyla web uygulamaları daha fazla gelişmiş saldırılara maruz kalmaktadır [25]. Siber saldırganlar tarafından gerçekleştirilen saldırılar web uygulamalarında güvenlik ihlalleri oluşturabilirler.

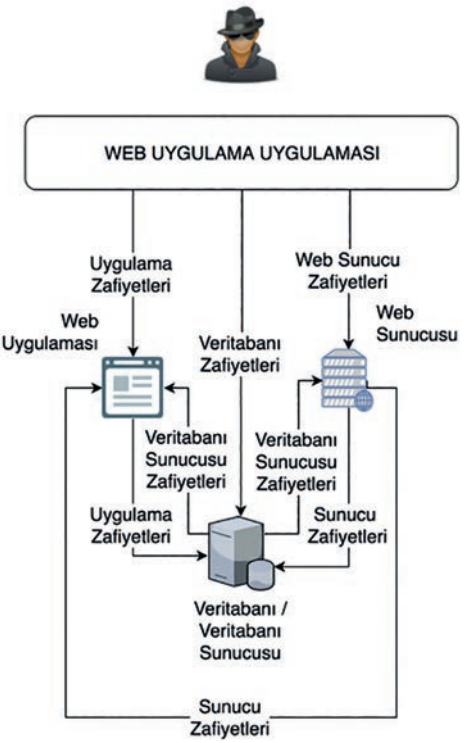
6.3.1. Siber Güvenlik Tanımları

Ağ yapıları, son kullanıcı cihazları, sunucular, servisler, etkileşimli bir şekilde birbirine bağlı tüm bilişim sistemleri ile birlikte siber dünyayı oluştururlar. Siber dünya içerisinde kritik öneme sahip, ele geçirilmesi durumunda maddi veya manevi zarar verebilecek birçok bilgi sürekli olarak kayıt edilmekte ve işlenmektedir. Siber saldırganlar kayıt edilen ve işlenen bu bilgilerin güvenliğini tehdit etmektedirler. Bilgi güvenliğinin gizlilik, bütünlük ve verinin kullanılabilirliği (erişilebilirliği) olmak üzere üç temel amacı vardır [26]. Siber dünyadaki bilgilerin gizliliği, erişilebilirliği veya bütünlüğü yapılan siber saldırılar tarafından tehlikeye girebilir. Gerçekleştiri-

len siber saldırıların türüne göre bu üç temel bileşenden biri veya birden fazlasının tehlike girmesi mümkün olabilmektedir. Gizlilik yalnızca yetkili erişimlerin olması gerektiği anlamını taşımaktadır. Bilgiye yetkisiz olarak yapılan ve istenmeyen tüm erişimler gizlilik bileşenini tehlikeye sokar. Erişilebilirlik istenilen zamanda ve istenilen şekilde bilgiye ulaşılabilmesi anlamını taşımaktadır. Bütünlük ise bilginin bir parçasının veya tamamın zarar görmemesini, yetkisiz bir şekilde değiştirilmemesi demektir. Bu üç temel bileşenin tamamının sağlanması siber güvenlik açısından önemlidir. Her ne kadar temel bileşenler birbirlerine yakın gözükse de gerçek hayatta birini uygulamak bir diğerinden uzaklaşmak anlamına gelebilmektedir. E-postalara her yerden erişmek için farklı istemciler ve farklı yerel ağlar (ev, restoran, vb) üzerinden e-postaları okumak erişilebilirliği arttırsa da gizlilik için bir risk oluşturabilir.

Bilişim sistemlerin güvenilir bir şekilde çalışması için üç temel bileşen arasında denge kurmak gerekmektedir. Bu denge risk değerlendirilmesine göre yapılabilmektedir. Risk istenmeyen bir olay veya sonuçlarından dolayı oluşabilecek kayıp veya zararların potansiyeli olarak tanımlanmaktadır [27]. Yapılan risk değerlendirmesi sonucu risk kabul edilebilir, kaçınılabilir azaltılabilir veya aktarılabilir [28]. Riskin kabul edilmesi herhangi bir işlem yapılmadan riskin olduğu gibi kabul edilmesidir. Riskten kaçınmak risk oluşturulan faaliyetlerinin yapılmasını engellemektedir. Riskin azaltılması yapılan çeşitli işlemler ile risk seviyesinin düşürülmesi demektir. Riskin aktarılması ise risk içeren sistem veya işleyişin bir başkasına aktarılarak riskin başkasına ait olması veya sigorta edilmesi anlamını taşımaktadır. Siber dünyada kullanılan varlıklar siber saldırganlar tarafından sürekli tehdit altındadır. Güvenlik ihlallerini önleme için, iş yönetiminde zafiyetlere açık varlıklar belirlenerek, farklı tehditlerden korumak büyük önem taşımaktadır [29]. Risk ve tehdidin ortak özelliği, sürekli izlenerek kontrol altında bulundurulma zorunluluğudur. Tehdit, varlığa zarar verme noktasına geldiğinde mutlaka müdahalede bulunulur, yönetilemez duruma gelen risk ise, tehdit kategorisine yükseltilerek varlığa zarar vermemesi için tedbirler alınmalıdır [30]. Gerekli tedbirler alınmadığı takdirde siber saldırganlar farklı atak vektörleri kullanarak zarara yol açabilirler. Bilişim sistemlerini oluşturan varlıkların (sunucular, istemciler, yazı-

lımlar) zafiyet oluşturan tüm alanları siber saldırganlar tarafından birer atak vektörü olarak kullanılabilmektedirler. Bilişim varlıklarına olan erişimlerin tamamı bir veya aha fazla atak vektörlerine dönüşebilirler. Standart bir web uygulamasına yönelik birden fazla atak vektörleri saldırganlar tarafından kullanılabilir (Bkz. Şekil 6.7).



Şekil 6.7. Dışarıdan erişim ile web uygulamasına gelebilecek atak vektörleri

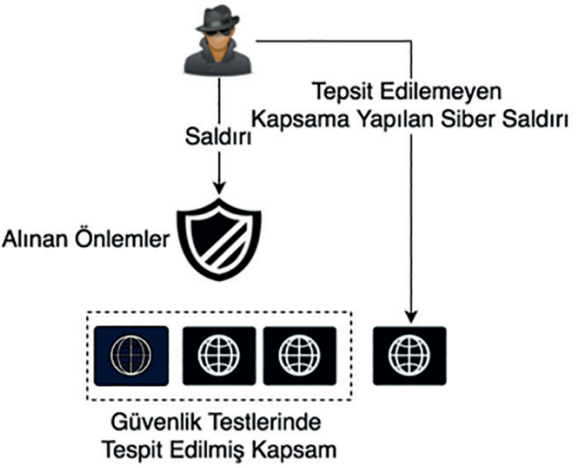
İlgili atak vektöründeki zafiyeti giderilmesi, atak vektörlerinin önceden bilinip gerekli çalışma yapılmasını gerektirir. Güvenlik testleri veya zafiyet analizleri güvenlik risklerin tespit edilip giderilmesi amacıyla gerçekleştirilmektedir.

6.3.2. Güvenlik Testi ve Zafiyet Analizi

Zafiyetlerin tetiklenmesi sonucu oluşabilecek bilgi güvenliğini ihlallerini önceden tespit etmek ve önlemek amaçlı iyi niyetli siber güvenlik uzmanla tarafından ilgili varlık üzerinde siber güvenlik testleri (sızma testi) gerçekleştirilmektedir. Gerçekleştirilen güvenlik

testleri belirlenen kapsam içerisindeki tüm varlıkları siber saldırgan gözüyle zarar vermeden incelenip raporlanmasını kapsamaktadır. Zafiyet analizi iletişim altyapısında, ağlarda veya bilgisayarlardaki zafiyetleri tanımlayan, belirleyen ve kategori eden bir süreçtir [31]. Zafiyet analizlerinde zafiyetin tespit edilmesine yönelik çalışmalar yapılırken, güvenlik testlerinde bu çalışmaya ek olarak zafiyetin sömürülmesi ve oluşabilecek ihlallerin test edilmesi de yer alır. Uzun zamana yayılı bir güvenlik testi izin verilmesi durumunda zafiyet analizine göre çok daha fazla alandaki (sosyal mühendislik, fiziksel erişim) testleri de kapsamaktadır [32]. Güvenlik testleri kendi içerisinde zafiyet analizini kapsarken, zafiyet analizleri daha çok otomatik araçlar ile ilerlenen ve derinlemesine inceleme gerektirmeyen bir süreci oluşturmaktadır.

Güvenlik testlerinin ilk aşaması bilgi toplamadır [33]. Aynı durum siber saldırganlar içinde geçerlidir. Siber saldırganlar veya güvenlik uzmanları hedef hakkında ne kadar çok bilgi toplayabilirse o kadar doğru bir değerlendirme yapabilirler. Güvenlik uzmanları tarafından tespit edilemeyen bilgilerin siber saldırganlar tarafından tespit edilmesi halinde bilgi güvenliği ihlalleri ortaya çıkabilir (Bkz. Şekil 6.8).



Şekil 6.8. Tespit edilemeyen kapsam ve güvenlik ihlali

Tespit edilemeyen kapsam güvenlik testleri veya zafiyet analizleri sırasında bilgi toplama aşamasında toplanan bilgilerin eksikliğinden kaynaklanabilmektedir.

6.3.3. Aktif ve Pasif Bilgi Toplama

Bilgi toplama sızma girişim öncesinde veya güvenlik testleri sırasında hedef hakkında aktif veya pasif olarak bilgi edinmeyi kapsamaktadır. Bilgi toplama aşaması güvenlik testlerinin veya sızma girişiminin ilk aşamadır ve her ne kadar daha az teknik bir aşama olsa da başarıyı doğrudan etkilemektedir [34]. Aktif bilgi toplama aşaması hedef sistemde iz bırakan, hedef sisteme paket göndererek yapılan bilgi toplamayı anlatırken, pasif bilgi toplama aşaması açık kaynaklardan elde edilen bilgileri kullanarak direk hedefe bağlantı sağlamadan bilgi toplama anlamına gelmektedir [35]. Bir web uygulamasında bilgi toplama aşaması pasif olarak aşağıdaki adımlar ile sağlanabilir:

- Alan adı / IP kayıt bilgileri (whois)
- Sitelerin geçmişini kayıt eden servisler ile yapılan incelemeler
- Arama motorlarının kullanımı ve özel aramalar
- E-posta adreslerinin tespit edilmesi (hedefin dışında)
- DNS sorguları

Alan adı / IP kayıt bilgileri hedef sistem hakkında IP aralığı, e-posta, adres, telefon bilgileri gibi bilgileri verebilir. Sitelerin geçmişini tutan hizmetler önceki tasarımlar, bağlantılar, kullanılan teknolojiler, alt alan adları gibi konularda bilgi verebilirler. Bu bilgilerin geçerli olup olmadığı testlerin veya sızma girişimlerin sonraki adımlarında kontrol edilmelidir. Arama motorlarında ise özel aramalar kullanılarak (site, inurl, filetype) daha önceden arama motorları tarafından hedef sistem içerisinde kayıt edilmiş bağlantılar, alt adları, dosyalar ve benzeri bilgilere ulaşılabilir. Hedef sistemdeki alan adlarına ait e-posta adreslerini bulmak için açık kaynak yazılımlar kullanılabilmektedir. TheHarvester adlı yazılım alan adına göre internetteki belirli web uygulamalarını tarayarak e-posta adreslerini tespit etmektedir [36]. Tespit edilen e-posta adresleri sonraki aşamalarda sosyal mühendislik saldırılarından, kaba kuvvet saldırılarına kadar birçok alanda kullanılabilirler. DNS sorguları web uygulamalarına ait alt alan adları, yeni IP adresleri gibi kapsamı genişletmek amacıyla kullanılmaktadırlar. Aktif bilgi toplama ise aşağıdaki şekilde toplanabilmektedir.

- Servis bilgileri edinme
- Port tarama
- DNS kaba kuvvet saldırıları ve
- Bağlantı tespitidir.

Aktif bilgi toplamda servis bilgileri ve port tarama hedef sisteme gönderilen ağ paketleri ile hedef sistemde çalışan servislerin sürümleri ile açık portları hakkında bilgi edinmeyi kapsamaktadır. DNS kaba kuvvet saldırıları DNS sunucusundan dönen cevapları kullanarak hedef sistemdeki alt alan adlarını veya farklı alan adlarını tespit etme işlemidir. Web uygulamalarında bağlantı tespiti ise bu çalışmanın konusunu oluşturmaktadır.

Bağlantı tespiti için arama motorları, web sitesindeki bağlantılar veya zafiyet tarama araçları gibi farklı yöntemler kullanılmaktadır. Zafiyet tarama araçları otomatik olarak web uygulamalarını gezerek zafiyetleri tespit etmeden önce hedef hakkında bilgi toplarlar. Silverlight, Java Applet, Ajax gibi web uygulamalarında kullanılan teknolojiler otomatik olarak tespit edilen bağlantıların sayısını olumsuz yönde etkilemektedir [37]. Eğer herhangi bir sayfa arama motorlarında, otomatik zafiyet tarama araçlarında veya web sitesi içerisinde gezinerek bulunamıyorsa tespit edilmesi için tahmin saldırıları yapılmaktadır. Dizinlere yapılan kaba kuvvet olarak da bilinen dosya/dizin tahmin saldırıları bir kelime listesinin web uygulamalarındaki dizinlere erişim için kullanılarak sunucudan dönen cevabı incelemek için kullanılmaktadırlar.

Gizli kalmış, tespit edilemeyen bağlantıların kaba kuvvet yöntemi ile tespit edilmesi durumunda yeni atak vektörleri oluşabilir. Yeni tespit edilen bağlantılar güvenlik zafiyetleri içeriyorsa saldırganlar tarafından bu zafiyetler istismar edilebilirler. Tespit için kullanılan kaba kuvvet yönteminde kullanılan kelime listesi içerisindeki kelimeler tespitin başarını oranını doğrudan etkilemektedir. Yeni bağlantı tespiti için kullanılan yazılımlarda İngilizce kelime listesi bulunmaktadır [10,15]. Bu kelime listesi Türkçe uygulamalarında test edildiğinde gizli kalmış Türkçe bağlantılar tespit edilememektedir. Zira Türkçe uygulamalardaki bağlantılarda İngilizce kelimeler yerine Türkçe karşılıkları (‘administrator’ yerine ‘yonetici’, ‘user’ yerine

'kullanici' gibi) kullanılabilmektedir. Şekil 6.9'da gizli kalmış sayfalar ve bağlantı yapısı örnek olarak gösterilmiştir.

Şekil 6.9. Gizli kalmış bağlantılar

Kapsamı belirleyen bilgi toplama aşaması hem saldırganlar hem de siber güvenlik uzmanları açısından önem arz etmektedir. Toplanan bilgiler daha fazla atak vektörünü belirlemek için kullanılmalıdır. Yeni atak vektörleri yeni zafiyetlere neden olabilir. Gizli kalmış bağlantıların tespiti sonrası oluşabilecek zafiyetler sonraki bir sonraki detaylı olarak incelenmiştir.

6.4. Web Uygulama Zafiyetleri ve Çözüm Önerileri

Siber saldırganlar tarafından toplanan bilgiler saldırılarda kullanılmaktadır. Toplanan her bir bilgi yeni zafiyetlere sebebiyet verebilir. Bu çalışma web uygulamaları üzerinde oluşabilecek zafiyetler ile ilgili olduğundan yalnızca web uygulama zafiyetleri ile bilgiler eklenmiştir.

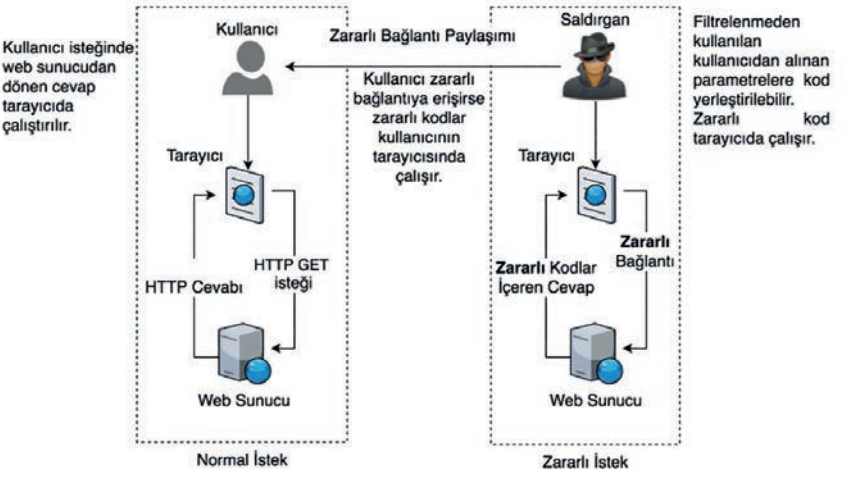
6.4.1. Siteler Arası Betik Çalıştırma Zafiyeti

JavaScript web uygulamalarına kullanılan tarayıcı tarafında yorumlanan ve genellikle yalnızca tarayıcı tarafında çalışan bir programlama dilidir ve çerez bilgilerine erişimden, web sitelerindeki verilere erişime kadar birçok işlem gerçekleştirebildiğinden dolayı siber saldırganlar tarafından zararlı amaçlar için kullanılabilmektedir. Saldırganların tarafından hedef sistem üzerinde JavaScript kodu çalıştırmasına olanak tanıyan zafiyetler Siteler arası betik çalıştırma zafiyeti (Cross Site Scripting, XSS) olarak bilinirler. Siteler arası betik çalıştırma zafiyeti günümüzdeki web uygulamalarında en çok tespit edilen zafiyetlerden biridir [38].

XSS zafiyetleri kullanıcıdan alınan verilerin web uygulamalarında doğru şekilde filtrelenmemesinden dolayı ortaya çıkan zafiyetlerdir. Zafiyetlerin tetiklenme türüne gürüne göre, yansıtılmış, depolanmış ve DOM tabanlı olarak üç ana başlık altında toplanabilmektedir.

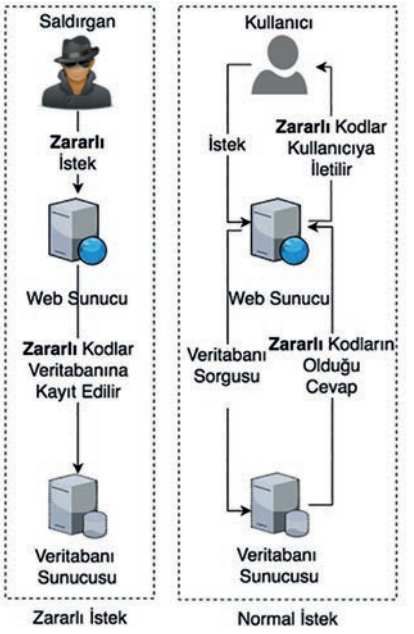
Yansıtılmış XSS saldırıları HTTP isteklerindeki parametreler ile zararlı değerlerin gönderilmesi vasıtasıyla tetiklenirler [39]. Diğer XSS zafiyet türü olan DOM tabanlı zafiyet türü ile birlikte kalıcı olmayan XSS saldırıları olarak değerlendirilmektedir. Kalıcı olmayan XSS zafiyetleri HTTP isteklerinde zararlı kodların gönderilmesi ve ayıklanmadan web uygulama tarafından geri yansıtılması ile oluşmaktadır [40].

Web uygulamalarında bazı durumlarda kullanıcıdan alınan veriler işlendikten sonra kullanıcıya yeniden sunulurlar. Herhangi bir web uygulamasına kullanıcı tarafından gönderilen isteklerin okunması ve tekrar kullanıcıya gönderilmesi yansıtılmış XSS türüne örnek olarak gösterilebilir. Bu tür XSS zafiyetleri arasında en çok karşılaşılan türdür. Zararlı kodlar kalıcı olarak kayıt edilmez fakat hemen kullanıcıya gösterilir [41]. Saldırgan tarafından zararlı kodlar içeren bağlantının sosyal mühendislik yöntemleri kullanılarak hedefe gönderilmesi ile kurbanın tarayıcısında çalıştırılabilir. Şekil 6.10'da yansıtılmış XSS zafiyeti gösterilmektedir.



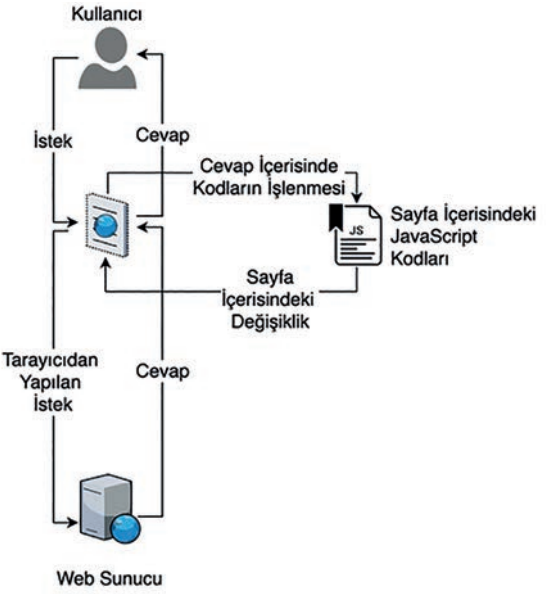
Şekil 6.10. Yansıtılmış XSS zafiyeti

Depolanmış XSS saldırılarında zararlı betikler saldırılan sistemdeki veri tabanı, mesaj alanları, yorum alanları ve benzeri alanlara kayıt edilmektedir [42]. Bu tür zafiyetlerde gönderilen zararlı kodlar hedef uygulama tarafından kayıt edilir ve tekrar kullanıcıya gösterilir. Uygulama içerisindeki zafiyet içeren bağlantıya erişen herkesin tarayıcısında zararlı kodlar çalışacaktır. Kalıcı türdeki XSS zafiyetleri sömürü kodları ilgili sayfaya erişen tüm ziyaretçileri etkileyecektir [43]. Şekil 6.11'de kalıcı türdeki XSS zafiyeti gösterilmektedir.



Şekil 6.11. Depolanmış XSS Zafiyeti

Belge Nesnesi Modeli (DOM) web ortamında yaygın şekilde kullanılan, özellikle HTML belgelerinde nesnelerle etkileşimde bulunmak için bir modeldir [44]. DOM tabanlı XSS zafiyetinde zararlı kodlar sayfa içerisinde başka JavaScript kodları kullanılarak eklenir. Bu zafiyetler istemci tarafında çalışan JavaScript kodları ve kullanıcıdan alınan girdilerin filtrelenmeden kullanılması ile oluşmaktadır [45]. Yansıtılmış XSS zafiyetinde zararlı kodlar sunucu tarafında işlenip gönderilen cevaba eklenirken, DOM tabanlı zafiyetlerde hedefin tarayıcısında zararlı kodlar eklenir ve çalıştırılır. Şekil 6.12'de DOM tabanlı XSS zafiyeti gösterilmektedir.



Şekil 6.12. DOM tabanlı XSS zafiyeti

XSS zafiyeti en tehlikeli 25 yazılım hataları sıralamasında dördüncü sırada bulunmaktadır [46]. XSS zafiyetleri ile hedef üzerinde veri okumaktan, hedef sistemi tamamıyla ele geçirmeye kadar birçok farklı saldırı gerçekleştirilebilmektedir. Bu zafiyetin önlenmesi için doğru filtreleme mekanizmaları kullanıcıdan alınan tüm girdiler için kullanılmalıdır. Kullanılan filtrelerin bazıları saldırganlar tarafından farklı yöntemler ile atlatılabilmektedir. Bazı kontrolleri atlatmanın birden fazla yolu olduğu için, web uygulama geliştiricileri uygulamaları zafiyetlerden korumak için ek koruyucu önlemler almalıdır [47]. Eğer uygulama kullanıcıdan alınan verileri doğru filtrelenmezse, saldırganlar çerezleri çalma, hesap ele geçirme, özel bilgileri transfer etme, servis dışı bırakma, sayfa içeriğini değiştirme gibi zararlı aktiviteleri gerçekleştirebilirler [48]. XSS zafiyetlerinin türlerine göre önleme yönelik çalışmalar 2004'den günümüze devam etmekte ve yeni çalışmalar hala günümüzde yayınlanmaya devam etmektedir [42].

Saldırganlar tarafından kullanılan zararlı Javascript kodları son kullanıcı üzerinden tehlikeli siber saldırılara yol açabilirler. Javascript ile XSS zafiyetinin sömürülmesi amacıyla kullanılan açık kaynak bir yazılım olan Beef çatısı içerisinde tarayıcı sömürülerini tetikleyen, bilgi-

leri çalan, zararlı istekler yapan, sosyal mühendislik saldırıları gerçekleştiren örnekler bulunmaktadır [49]. Bu zafiyetin sömürü kodlarının yapabilecekleri tarayıcılarda çalışan kodların yetenekleri dahilindedir.

XSS kullanıcıdan alınan girdileri doğru filtrelenmeden dolayı oluştuğundan dolayı, doğru filtreler uygulamak XSS zafiyetleri için en iyi yöntemdir [50]. Girdileri filtrelemek için yer değiştirme, silme, tarayıcı tarafından özel olarak yorumlanan karakterlerden kaçınma ve beyaz liste uygulaması olarak 4 farklı yöntem bulunmaktadır [51]. Çoğu çalışma önlemeyi istemci ve tarayıcı arasında önlenmesi üzerine olsa da [41,50,52] tarayıcı tarafında kritik bilgilerin dışarı çıkmaması önlemeyerek zafiyetlerin sömürülmesini engelleyen çalışmalar bulunmaktadır [53].

Zafiyetin varlığını anlamak için uygulamanın kaynak kodunun incelenmesi (statik) veya uygulamanın kullandığı parametreler üzerinde istekler yapılarak analiz edilmesi (dinamik) gerekmektedir [54].

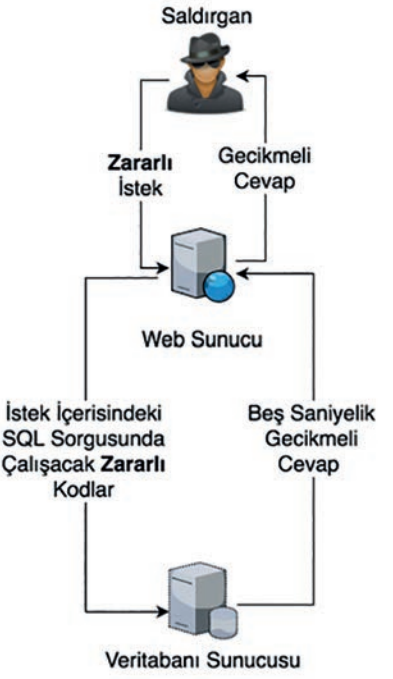
6.4.2. SQL Enjeksiyonu Zafiyeti

Web uygulamalarındaki dinamik sayfalarda çoğunlukla kullanıcıya sunulan bilgiler veri tabanlarından okunarak servis edilir. Veri tabanından okuma işlemi veri tabanına özel kurallar çerçevesinde gerçekleştirilir. Web uygulamalarında kullanıcıdan alınan değerler SQL sorgularına dahil edilebilir. Yazılımcıların, kullanıcıdan aldığı parametreleri SQL sorgularına kullanması ile oluşan sorgulara dinamik SQL sorgularıdır [55]. Saldırganların dinamik sorgulara müdahale ederek hedef sistemde çalışan SQL kodlarını değiştirerek yaptığı saldırılar SQL enjeksiyonu saldırıları olarak adlandırılmaktadır. Bu saldırıda saldırgan, dinamik olarak oluşturulan SQL sorgulara zararlı kodlar enjekte ederek sorguları kendi amacı doğrultusunda kullanmaktadır. SQL enjeksiyonu saldırılarında, saldırganlar tarafından hedefe zararlı istekler gönderilerek, veri tabanı hakkında bilgi sahibi olma, veri tabanı yöneticim parolaları ele geçirme, verileri silme, ele geçirme, veri tabanında kod çalıştırma hatta işletim sistemine komut çalıştırmaya kadar birçok farklı zararlı işlem gerçekleştirilebilir [56].

SQL enjeksiyonu zafiyeti kullanıcıdan alınan girdilerin doğru şekilde filtrelenmeden SQL sorgularında kullanılması ile ortaya çıkan zafiyetlerdir. Bu zafiyetlerin belirli çalışmalarda [57,58] farklı türlerle (line

comment, logical query, inference) bölünmüştür. SQL enjeksiyonu zafiyetlerini tessit eden ve sömürmekte kullanılan SQL Map adlı açık kaynak zafiyet tarama aracı bu zafiyetleri, körlemesine mantıksal tabanlı (boolean-based blind), körlemesine zaman tabanlı (time-based blind), hata tabanlı (error-based), birleştirilmiş sorgu tabanlı (union query-based) ve yığın sorgular (stacked queries) türleri olarak beşe ayırmıştır ve diğer çalışmalardakileri de kapsamaktadır [58,59,60].

Körlemesine (blind) SQL enjeksiyonu zafiyetlerinde saldırganlar hedef sistem üzerine herhangi bir veri direk olarak okunmamaktadır. Saldırganlar veriyi sayfada gösterecek SQL girdileri kullanmak yerine, hedef sistem üzerindeki SQL sorgularına yaptıkları müdahaleleri, sunucudan dönen cevabı geciktirme (zaman tabanlı) veya dönen cevap içerisindeki bazı davranışları analiz edebilecek (doğru/yanlış) hale çevirerek kullanmaktadırlar. Şekil 6.13'de körlemesine SQL enjeksiyonu türündeki zafiyet gösterilmektedir.



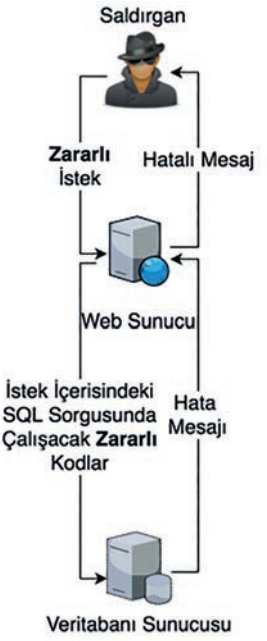
Şekil 6.13. Körlemesine zaman tabanlı SQL enjeksiyonu zafiyeti

Birleştirilmiş SQL sorgularında iki farklı sorguyu birleştirerek tek bir cevap dönmesini sağlayan bir özel bir ifadedir. Birleştirilmiş SQL

enjeksiyonu saldırılarında asıl sonuç ile zararlı kodlar ile oluşmuş sonucu birlikte birleşip tek bir cevap olmasını sağlayan sorgular kullanılmaktadır [56]. Birleştirilmiş cevapların saldırgana dönmesi ile saldırgan hedef sistemde ver olan SQL enjeksiyonu zafiyetini tetikleyebilmektedir.

Yığın tabanlı (stacked, piggy-backed) SQL enjeksiyonu zafiyetinde ise saldırgan hedef sisteme bağımsız bir sorgu göndererek, hedef sistemde var olan ilk sorgunun çalışmasından sonra kendi sorgusunun çalışmasını sağlar [61]. Bu tarz zafiyetler her veri tabanı ve web uygulamasında çalışmayabilir. Sıralı olarak birden fazla SQL sorgusunun tek seferde çalıştırılması varsayılan olarak bazı web uygulamalarında kullanılan veri tabanı sınıfları içerisinde kapalı olarak gelmektedir.

Hata tabanlı SQL enjeksiyonu saldırılarında saldırgan hedef sisteme veri tabanı satırlarında hata oluşturacak girdileri gönderir. Oluşan hata, dönen cevap içerisinde gövde de veya başlıklarda bir iz bırakır. Saldırgan bu ize bakarak hedef sistem üzerinde gerekli bilgileri toplayabilir. Şekil 6.14'de hata tabanlı SQL enjeksiyonu zafiyet gösterilmektedir.



Şekil 6.14. Hata tabanlı SQL enjeksiyonu

SQL enjeksiyonu zafiyetlerinde saldırganlar yönetici hesapları saldırganlar tarafından saldırıya maruz kalabilir, saldırganlar bağlantılardaki GET parametresi gibi basit kaynakları kullanarak bu saldırıları gerçekleştirebilirler [57]. SQL enjeksiyonu zafiyetini sömüren saldırganlar veri tabanı üzerinde tam yetkiye sahip olabilirler, veri tabanı sunucusunu ele geçirebilirler ve uzaktan komut çalıştırmak, ziyaretçilere yönelik saldırılar gerçekleştirmek, bilgileri almak, değiştirmek gibi birçok zararlı aktivite gerçekleştirebilirler. Bu türdeki zafiyetlerini önlemek için uygulama katmanında ve veri tabanı katmanında birçok çalışma yapılmıştır [58]. Ayrıca günümüzde kullanılan web uygulama güvenlik duvarları ağ katmanında SQL enjeksiyonu zafiyetlerini engellemek için kullanılmaktadır. Uygulama katmanı dışında statik kod analizi, kara-kutu test (tüm girdi değerlerinin taranarak tespit edilmesi) gibi ek yaklaşımlarda bulunmaktadır [56]. Bu tarz saldırı önlemek için kullanıcıdan alınan değerlerin bir kara listeden geçirilerek engellenmesi yerine yalnızca izin verilen girdiler oluşan bir beyaz listenin kullanılmasının başarıyı arttıracağı yapılan çalışmalarda yer almaktadır [55]. Yapılan saldırıların tespit edilmesi için paket analizi ve örnek eşleşme algoritmasının kullanıldığı araştırmalar literatürde yer almaktadır [62].

6.4.3. Sitelere Arası İstek Sahteciliği

Web uygulamaları kullanıcıları hem tarayıcının kendisinde (çerez) hem de sunucu içerisinde tuttuğu (oturum bilgisi) bazı özel değerler ile tanımaktadır. Bu değerler sayesinde üyelik işlemleri, alışveriş sepeti gibi kişiye özel işlemler web sitesinde bir tarayıcı üzerinden gerçekleştirilmektedir. Tarayıcıda tutulan bilgiler otomatik olarak tarayıcı tarafından yapılan her istekte gönderilmektedirler. Sunucu tarafında alınan bu bilgiler gerekli kontrollerden geçtikten sonra işlemler yapılmaktadır. Yeni oturum bilgileri sunucu tarafından oluşturulup, HTTP başlıkları ile tarayıcıya gönderilmektedir. Oturum bilgileri web uygulamalarında mesajlar, yorumlar, alışveriş sayfası, üyelik paneli, üye işlemleri gibi özel alanlara erişim için kullanılmaktadır. Saldırganlar hedef sistemdeki tarayıcıların oturum bilgilerini kendi çıkarları için kullanarak web uygulamalarında başka kullanıcıymış gibi işlem yapabilirler. Siteler arası istek sahteciliği (Cross-Site request forgery, CSFR) web kullanıcılarına yönelik,

saldırganın kurbanın tarayıcısı ile güvenilir bir web uygulamasına istenmeyen bir istek yapması ile oluşan saldırılardır [63]. OWASP tarafından 2013 yılı içerisinde yayımlanan en çok karşılaşılan zafiyetler listesinde CSRF zafiyeti sekizinci sırada bulunmaktadır [64].

CSRF zafiyeti web uygulamasına yapılan her isteğin yalnızca ilgili web uygulaması içerisinden yapılıp yapılmadığının kontrol edilmemesi ile oluşmaktadır (Bkz. Şekil 6.15).

Şekil 6.15. CSRF zafiyeti

Güvenilir web sitesinde oturum bilgisi ile işlem yapan kullanıcı, içerisinde zararlı kodların olduğu başka bir sayfayı ziyaret edebilir. Bu durumda zararlı web sitesi içerisinden güvenilir web sitesine, kullanıcının oturum bilgisinin de içerisinde olduğu bir istek iletilebilir. Bu istek kullanıcının tarayıcısı tarafından gönderilmektedir. Yapılan istek içerisinde oturum bilgisi yer aldığından dolayı saldırgan sanki kullanıcıymış gibi güvenilir web sitesinde özel işlemler gerçekleştirebilmektedir.

CSRF saldırılarına karşı gelen isteklerin doğrulu kontrol edilmelidir. Bu zafiyetler genellikle HTTP çerezlerinin oturum bilgisi içeren (session token) değerlerin gönderilmesinde kullanılması ile oluşur [65].

Aynı kök politikası (same origin policy) çözümü günümüzde kullanılan birincil çözümlerden biridir [66]. Bu zafiyetin engellenmesi için web sunucularına yapılan isteğin doğru kaynaktan yapıldığı kontrol edilmelidir. Her sunucu ya yapılan istekte değişen değerlerin istemcide saklanması ve tekrar sunucuya iletilerek kontrol

edilmesi bilinen yöntemler arasındadır. Rastgele değer üreten algoritmaların kullanılması CSRF zafiyetlerinde önemli derece etki göstermektedir [67].

6.4.4. Basit Parola Denemeleri ve Kaba Kuvvet Saldırıları

Kimlik bilgisini doğrulamak için günümüzde en çok kullanılan mekanizmalardan biri kullanıcı adı ve parola bilgisidir. Bu bilgiler web uygulamalarında kullanıcı kimliğini tanımak için kullanılır. Bilgilerin doğru olması durumunda kişiye özel alanlara erişim yapılabilir. Kötü niyetli kullanıcılar web uygulamaların kimlik doğrulama sayfalarına (genellikle üye giriş ara yüzleri) kullanıcı adı ve parola denemeleri gerçekleştirebilirler. Doğru kombinasyonu tespit etmeleri halinde kullanıcı yetkilerinde web uygulamalarında işlem yapabilirler. Genellikle kullanıcı adları web uygulamaları içerisinde herkese açık olduğundan kimlik doğrulama için kullanılan ilk öğe olan kullanıcı adı parametresi saldırganlar tarafından kolaylıkla ele geçirilebilir. Yönetim paneli gibi özel alanların en yetkili kullanıcı isimleri ise admin, administrator, yonetici vb. kelimelerden oluşabilir. Bu durumlarda saldırgan kullanıcı adını tespit edemese de dahi kolayca tahmin edebilir. Parola bilgisinin de kolay tahmin edilebilir olması durumunda saldırganlar ilgili web uygulamasında kimlik doğrulama aşamasını geçebilirler. Kullanıcılar farklı farklı web uygulamalarına üyelik açtığı halde aynı parolayı tekrar kullanma eğilimindedirler. Bu da zaman geçtikte parolaların tekrar kullanımın oranını arttırmaktadır [68]. Web sitelerine ait kullanıcı bilgilerinin ele geçirilmesi aynı parolaların tekrar kullanılmasını daha tehlikeli bir hale getirmektedir. Bazı web uygulamalarında saldırganların denemelerini önlemek için kimlik doğrulama denemelerine belirli bir limit getirilmektedir. Her ne kadar parola denemeleri için limit olsa da saldırganlar tarafından ele geçirilen önceki sızmış parola bilgileri, deneme sayısı limiti içerisinde parolanın doğru şekilde tespit edilmesi için kullanılabilir [69].

Basit, tahmin edilmesi kolay kullanıcı adı ve parola ikililerinin kimlik doğrulama yöntemlerinde tercih edilmesi siber saldırganlar tarafından kolaylıkla tespit edilebilir önemli bir zafiyettir. Siber saldırgan tarafından doğru şekilde tahmin edilen kullanıcı adı ve parola ikilileri saldırganların sistem üzerinde ilgili kullanıcının yetikleri ile işlem yapmasına olanak tanımaktadır.

Kaba kuvvet saldırıları anlık olarak oluşturulan değerler ile yapılabileceği gibi daha önceden oluşturulmuş bir listedeki kelimelerin (liste saldırısı) denenmesi ile de gerçekleştirilebilir. Sistem üzerinde kullanıcı adı ve parola ikililerinin kontrolleri sırasında kaynak kullanımı yüksek ise bu saldırılar ile sistemler servis dışı kalabilirler.

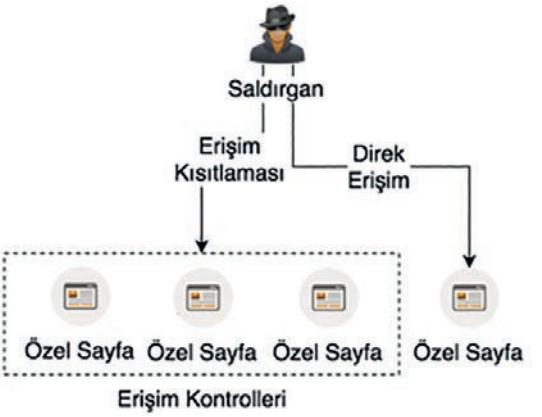
Güvenlik kodu kullanılması her seferinde doğrulama isteyeceğinden dolayı kaba kuvvet saldırılarını büyük oranda durduracaktır. Fakat basit parola denemeleri otomatik araçlar kullanılmadan el ile denenebileceğinden dolayı güvenlik kodları kolay tahmin edilebilir basit parolalar için etkili birer önleme yöntemi değildirler.

Kullanıcılar her farklı kimlik doğrulama sistemi için farklı bilgiler kullanmalıdır. Fakat kullanıcıların seçtiği parola bilgileri kullanıcıların bilgileri limitli olduğundan doğal olarak zayıftırlar [70]. Bunun önüne geçmek parola yazılımları kullanılmalıdır. Ek olarak tek seferlik kod üreten mekanizmalar kimlik doğrulama sistemlerinin içerisinde kullanılması sistemin güvenliğini arttıracaktır [71]. Yazılım geliştiriciler web uygulamalarında güvenilir parola politikaları uygulamalı ve parola deneme işlemlerini kısıtlamalıdırlar.

6.4.5. Yetkisiz Erişim Zafiyeti

Kullanıcılar, uygulamalar içerisinde farklı yetkilere sahip olabilirler. Web uygulamalarında bu yetkiler belirli alanlara yazma, belirli alanlardan okuma veya belirli alanları silme gibi farklılıklar gösterebilir. Erişim kontrolleri web uygulamalarında veriye (okuma ve yazma) ilgili kullanıcının yetkileri dahilinde kısıtlanmasıdır [72]. Yetkiler genellikle kimlik doğrulama mekanizmaları sonrasında ilgili kullanıcıya atanmaktadır. Yetkisiz erişim doğru bilgilere (kullanıcı adı, parola, tek girişlik parola, vb.) sahip olmadan yetkili bir kullanıcı haklarının bir kısmına veya tamamına sahip olmaktır.

Kimlik doğrulama mekanizmaları sonrasında atanan yetkiler genellikle kullanıcının tarayıcısından web uygulamasına gönderilen oturum bilgileri ile tutulmaktadır. Bu oturum bilgileri yetkilerin kontrol edilmesi gereken her sayfada kontrol edilmelidir. Kontrol edilmediği durumlarda saldırganların erişim yapması bazı bilgilerin dışarıya çıkmasına sebebiyet verebilir (Bkz. Şekil 6.16).



Şekil 6.16. Yetkisiz erişim kontrolleri

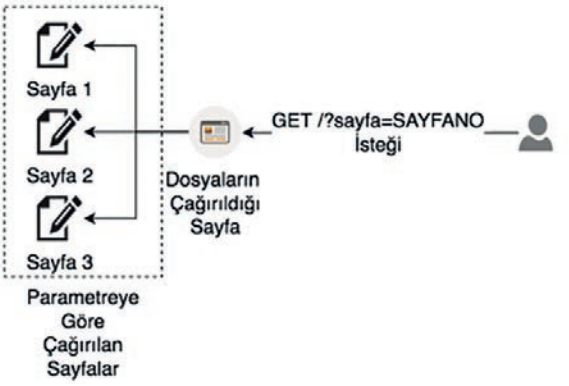
Yetkisiz erişimler erişim kontrolleri olmayan ayrı sayfaları test edilerek tespit edilebileceği gibi web sayfalarına giden ağ trafiği üzerinde değişiklik yapılarak da test edilebilir.

Yetkisiz erişim zafiyetlerinin tetiklenmesi kullanıcı oturumu gerektiren sayfalarda veya alanlara yetkisiz olarak siber saldırganların erişmesi ile oluşmaktadır. Saldırganın istemciden sunucuya giden tüm istekleri değiştirilebileceği düşünülerek gerekli kontrollerin web uygulama yazılım geliştiricileri tarafından sağlanması önemlidir. Özellikle kullanıcıya ait özel tekil değerlerin (id), oturum alanlarının istemciden sunucuya gittiği alanlar web uygulamalarında yetkisiz işlemlerin kontrol edilmesi gereken alanlardır.

6.4.6. Dosya Çağırma

Uygulamalarda yer alan kodlar içerisinde bazı durumlarda uzaktaki veya uygulama ile aynı alandaki (yerel) sistemlerden dosya çağıran kod parçaları bulunur. Bu kod parçaları web uygulaması içerisinde yapılması gereken işlerin bir kısmını veya tamamını yerine getirmek için kullanılabilir. Çağırılan dosyaların türüne göre komut çalıştırmaktan, dosya içerisindeki komutları kullanmaya kadar birçok farklı alanlarda web uygulamalarına dışarıdan dosya çağırılabilmektedir. Bazı çalışmalar internet sitesi, dizinler veya aynı disk üzerindeki gibi farklı bir yerde bir kısım kodları çağırılmasına uzaktan dosya çağırma (remote file inclusion, RFI) zafiyeti olarak

tanımlamıştır [73]. Bazı çalışmalarda ise doğru kontrollerin yapılmadığı sistemlerde, web uygulama ile aynı sunucuda olan dosyaları çağıran zafiyetlere yerel dosya çağırma (local file inclusion, LFI) zafiyetleri olarak , uzaktan aynı sunucu üzerinde olmayan dosyaların çağırıldığı zafiyetlere ise uzaktan dosya çağırma (remote file inclusion, RFI) zafiyetleri denmektedir [74]. Daha güncel çalışmalar içerisinde ve OWASP'da yerel dosya çağırma zafiyeti, uzaktan dosya çağırma zafiyeti olarak iki farklı zafiyet olarak incelenmektedir [75,76]. Şekil 6.17'de dosya çağırma zafiyeti gösterilmektedir.

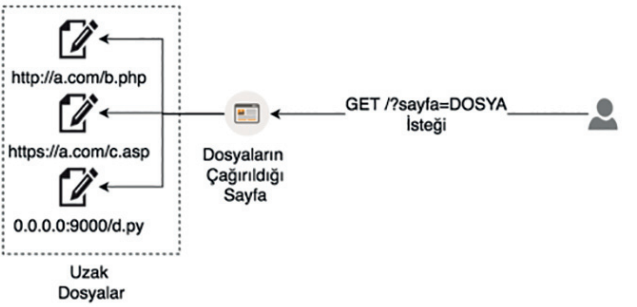


Şekil 6.17. Dosya çağırma işlemi

Yerel dosya çağırma zafiyetlerine sayfanın bir bölümün HTTP isteklerinden çağırarak kullanan web uygulamaları örnek verilebilir. Sayfanın ilgili bölümünün adını GET parametresinden alan bir web uygulamasına ait parametre değerleri değiştirilerek çağırılması gereken dosya dışında bir dosya çağırılarak ilgili dosya içerisindeki veriler saldırganlar tarafından kullanılabilir. Yerel dosya çağırma zafiyetleri bazı durumlarda uzaktan komut çalıştırma ile sonuçlanan ciddi zafiyetlere sebebiyet vermektedir. Şekil 6.18'de yere dosya çağırma zafiyeti tetikleyen örnek bir sömürü kodu gösterilmektedir.

Şekil 6.18. Yerel dosya çağırma zafiyetinin tetiklenmesi

Uygulamalar bazı durumlarda uzaktaki bir dosya içerisindeki kodları kullanabilirler. Uzak bir sistemdeki dosyalar ilgili web uygulamasında gösterilmesi için çağırılabilir (Bkz. Şekil 6.19).



Şekil 6.19. Uzak dosya çağırma işlemi

Uzaktan dosya çağırma zafiyetleri ise uzaktaki saldırganın istediği dosyanın hedef sistem tarafından çağırılarak kullanması sonucu oluşmaktadır. Bu zafiyet ile saldırgan hedef sisteme zararlı kodları kendisinin yönettiği uzak bir sistemdeki zararlı dosyayı yükler. Şekil 6.20'de zafiyeti tetikleyen örnek bir sömürü kodu gösterilmektedir. Uzaktan dosya çağırma zafiyetinin gerçekleşmesi için sistemde gerekli yetkiler tanımlı olarak gelmelidir. Varsayılan olarak bazı yazılım dillerinde uzaktan dosya çağırarak çalıştırma işlemlerine izin verilmemektedir.

Şekil 6.20. Uzak dosya çağırma zafiyetinin tetiklenmesi

Dosya çağırma zafiyetlerinin saldırganlar tarafından tetiklenmesi durumunda tüm sistemi ve bağlı sistemlerde saldırganların yüksek yetkiler ile komut çalıştırabileceği sonuçlar oluşabilmektedir. Yerel dosya çağırma zafiyetleri sunucuda dosya okunmasına olanak vermektedir. Bu türdeki zafiyetler web sunucusunun yerel sistemde erişebileceği tüm dosyaların okunması ile sonuçlanabilmektedir. Okunan dosyalara, saldırganların yazma yetkisinin de olması durumunda saldırganlar web sunucularının yetkisinde komut çalıştırabilirler. Uzaktan dosya çağırma zafiyetlerinde ise saldırgan istediği

dosyayı hedef uygulama içerisinde çalıştırabilmektedir. Genellikle web sunucu tarafından desteklenen yazılım dillerine ait zararlı kodların bulunduğu sayfaların çağırılması web sunucu yetkileri ile uzaktan komut çalıştırmaya olanak tanımaktadır.

Her iki zafiyette de dinamik olarak çağırılan sayfalara beyaz liste uygulanması zafiyeti gidermek için etkili bir yöntemdir. Web sunucu ayarlarının doğru yapılandırılarak web sunucunu sadece ihtiyacı olan dosyalara erişmesini sağlamak, gerekli olmadığı durumlarda uzaktan çalıştırılabilir dosyaları web uygulamalarına eklenmesini kapatmak alınması gereken diğer önlemler arasındadır.

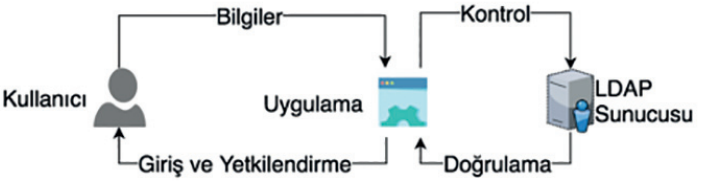
6.4.7. Diğer Enjeksiyon Zafiyetleri

Günümüzde birbirleri ile etkileşimli sistemler arttığından dolayı ihtiyacı karşılamak için web servis olarak sunulan hizmetler de artırmıştır. Web servisi tabanlı hizmetlerde, hizmeti sağlayan servisi kullanan için kendi sistemlerine erişip yapıp işlem yapan bir arayüz sunmaktadır [77]. Hizmeti kullanan gerekli işlemleri web servisin kurallarına göre istekler göndererek gerçekleştirir ve işlenen cevabı geri almaktadır. XML tabanlı diller doküman yayımlamak, elektronik marketlerde ürün kataloglarını kayıt etmek ve işler arasında veri alışverişini sağlamak için idealdirler [78]. Web servislerinde de XML kullanılmaktadır. Örnek bir XML dokuman şablonu aşağıda verilmiştir.


```
<urun>
<isim>Ürün adı</fiyat>
<fiyat>Fiyat</fiyat>
<kategori>Ürün Kategori</kategori>
<aciklama>Ürün açıklaması</aciklama>
</urun>
```

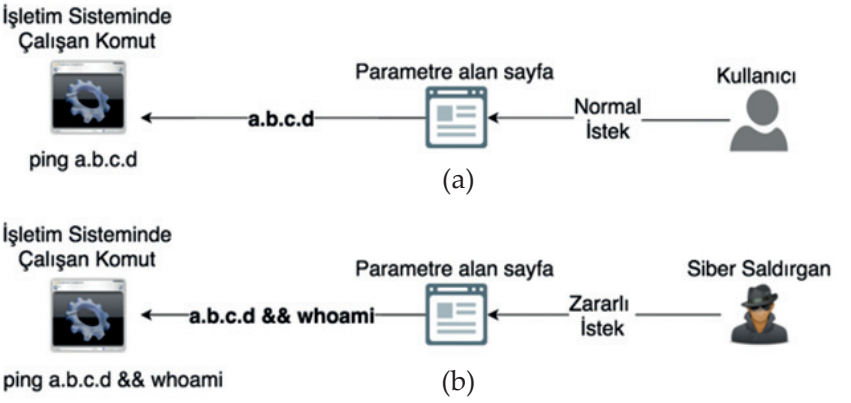
XML tabanlı web servislerine XML şablonunda istekler gider ve dönen cevaplar yine genellikle XML tabanlı olur. Saldırganlar web servisine giden XML isteklerini bozarak farklı istekleri hedef web servisine gönderebilirler. XML enjeksiyonu saldırısı XML yapısını değiştirerek gönderilen mesaja XML etiketlerini içeren içeriklerin eklenmesi ile oluşur [79]. XML yapısı web servisi sağlayan sistem tarafından işlenirken saldırganın eklediği yeni XML etiketleri sistemin farklı davranmasına sebep olabilmektedir.

Hizmetler, kullanıcılar ve farklı hizmet veya ürünlerin birbirleri ile iletişimi arttıkça kullanıcı yönetiminin önemi de artmaktadır. Kamu kurumlarından, bankalara, üniversitelerden çok sayıda personel çalıştıran özel sektör firmalarına kadar kullanıcı yönetimi bilişim sistemlerinin doğru çalışması için önemlidir. Dizin servisleri bir etki alanı içerisindeki verileri düzenli şekilde işlenmesi görevini yürütmektedir. LDAP (Lightweight Directory Access Protocol) bu dizin servisleri ile TCP/IP üzerinden iletişimi tanımlayan bir protokoldür [80]. Özellikle bir etki alanında kullanıcıya ait kimlik doğrulama ve yetkilendirme işlemlerinin gerçekleştirilmesi için web uygulamalarında LDAP kullanılabilir (Bkz. Şekil 6.21).



Şekil 6.21. Web uygulamalarında LDAP

Web uygulamalarında alınan parametreler bası durumda işletim sisteminde çalıştırılabilirler. Kullanıcıdan alınan parametrelerin filtrelenmeden işletim sistemi seviyesinde çalıştırılan komutlarda kullanılması işletim sistemi komut enjeksiyonu zafiyetine sebebiyet vermektedir. Şekil 6.22'de işletim sistemi komut enjeksiyonuna örnek gösterilmektedir.



Şekil 6.22. İşletim sistemi komut enjeksiyonu

XML enjeksiyonu zafiyetleri tetiklenmesi durumunda uzaktan komut çalıştırma, yerel dosya okuma, html kodu enjeksiyonu gibi sonuçlar doğurmaktadır. XML tabanlı web servislerinde alınan tüm istekler doğru şekilde ayrıştırılmalı ve içerisindeki değerler bir beyaz liste kullanılarak yalnızca istenilen değerlerin içerdiğinden emin olunmalıdır. Genel saldırı alanın azaltılması için, aksini yapmak için iyi bir neden olmadığı durumlarda -performans sorunları gibi- gelen XML dokumanı geçerli olan XML şeması ile karşılaştırılmalıdır [81].

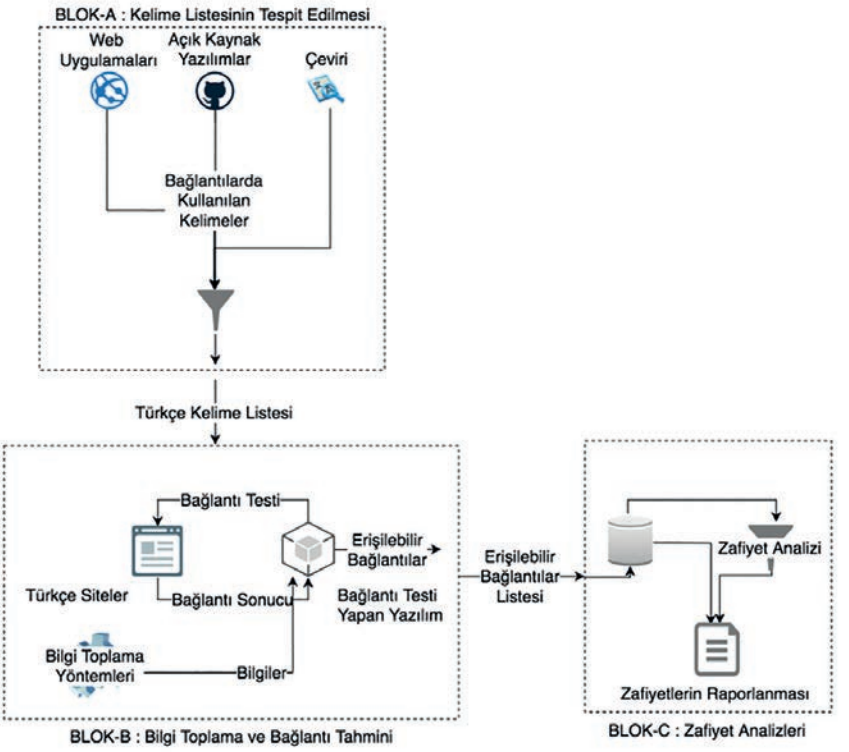
LDAP tüm kullanıcı bilgilerinin tutulduğu, yetkilendirme ve doğrulama işlemlerinin yapıldığı alanları kapsamaktadır. Bu nedenle LDAP enjeksiyonu ile bu sistemlere veri okumadan veri yazmak tehlikeli siber güvenlik ihlalleri doğurabilir. Diğer kod enjeksiyonu zafiyetlerine yönelim çözüm yöntemleri olan girdileri kontrol etme, statik kod analizi, dinamik kontroller LDAP enjeksiyonu zafiyetinde çözüm yöntemleridir. Özellikle uygulama katmanında parantezler, yıldızlar ve mantıksal operatörlerin filtrelenmesi gereklidir [82].

İşletim sistemi komutu enjeksiyonu ise direk olarak komut çalıştırmaya olanak tanıyan bir zafiyettir. Siber saldırganlar tarafından yetki yükseltilmesi durumunda tüm sistem siber saldırganlar tarafından ele geçirilebilir. Web uygulamalarında web sunucu tarafından çalıştırılan işletim sistemi kodlar, web sunucularının yetkisi dahilinde çalışmaktadır. Yüksek yetki ile çalışan sunucularda yetki yükseltmeye gerek kalmadan saldırganlar tüm sistemi ele geçirebilmektedirler. İşletim sistemlerine göre farklılık gösterebilen artarda komut çalıştırmaya yarayan özel karakterler filtrelenmeli ve kullanıcıdan alınan değerler güvenli bir ortamda çalıştırılmalıdır.

6.5. Web Zafiyetlerini Önleme

Gerek güvenlik testleri sırasında gerekse kötü niyetli saldırganlar tarafından yapılan zararlı aktivitelerde web uygulamaları içerisinde tespit edilecek yeni atak vektörleri bütün uygulamanın ve uygulamanın bağlantılı olduğu tüm bilişim sistemlerini tehdit eder. Güvenlik testleri sırasında tespit edilemediğinden dolayı kontrol edilemeyen alanlar, yazılımcılar tarafından eski kalan unutulmuş sayfalar ya da kaynak kodu analizinde ortaya çıkmayan eksiklikler

saldırganlar tarafından tespit edilmesi durumunda güvenlik ihlalleri oluşabilmektedir. Web uygulamalarında arama motorları tarafından tespit edilemeyen, ilgili uygulama içerisindeki herhangi bir bağlantı ile erişimi olmayan gizli kalmış bölümleri tespit etmek için bir kelime listesi ile bağlantı denemesi yapan yazılımlar mevcuttur [10-15]. Bu yazılımlar içerisinde varsayılan olarak İngilizce kelime listesi olduğundan Türkçe yazılmış ve Türkçe kelimeleri bağlantılar içerisinde kullanan web uygulamaları için yazılımlar yetersiz kalmaktadır. Bu çalışma, web uygulamalarında kullanılabilecek Türkçe kelime listesinin belirlenmesi ve Türkçe web uygulamalarında gizli kalmış, gözden kaçan yeni alanların tespit edilip güvenlik ihlalleri önlenmesini amaçlayarak üç farklı bloğa ayrılmıştır. Bu bölümler bağlantılarda kullanılan Türkçe kelimelerin belirlenmesi, web uygulamalarından bilgi toplanması ve bağlantı tespiti ve ortaya çıkabilecek zafiyetlerin analizlerinin gerçekleştirilmesidir (Bkz. Şekil 6.23).



Şekil 6.23. Önerilen bilgi toplama ve zafiyet tespit sistemi blok şeması

6.5.1. Bağlantılarda Kullanılan Türkçe Kelime Listesinin Belirlenmesi

Türkçe kelime listenin oluşturulması için çevirilerden, arama motorlarından ve açık kaynak yazılımlardan yararlanılmıştır. Bu kaynakların ilki İngilizce kelime listelerinden yapılan çevirilerdir. Bağlantı tahmini için kullanılan açık kaynak yazılımlar içerisinde kelime listeleri bulunmaktadır. Bu kelime listelerindeki bazı uygulamalara ait özel kelimelerin (phpMyadmin, drupal, wordpress vb) dışında kalan ve Türkçe olarak bağlantılarda kullanılabilecek tüm kelimeler yapılan çeviriler kelime listesine eklenmiştir.

Bağlantı yapılarında kelimelerin yerine rakamlar ve sayılar da bulunmaktadır. İçerisinde tarih bilgisi içeren bağlantılar örnek olarak gösterilebilir. Türkçe kelimeler bu türdeki bağlantıların sonunda (/2017/10/01/ornek.html gibi) yer alabilir. Bu türdeki bağlantıların tespit edilebilmesi için kelime listelerine rakamlar ve gün, ay, yıl belirten sayılar da eklenmiştir.

Github, açık kaynak yazılım projelerinin içerisinde bulunduğu projelere sürüm kontrol sistemi, dokümantasyon, bulgu yönetimi gibi özellik sağlayan bir uygulamadır. Bu uygulama içerisinde açık kaynak birçok web uygulamaları yer almaktadır. Bu web uygulamaları açık kaynak olarak yayınlandığından dolayı içerisindeki bulunan dosya isimlerine veya bağlantılarda kullanılan bağlantı yapısına erişilebilmektedir. Oluşturulan Türkçe kelime listesine açık kaynak yazılımlardan elde edilen bağlantıda kullanılabilir kelimeler de eklenmiştir. Bu sayede yazılım geliştiricilerin gerçek hayatta kullandığı kelimeler listeye eklenmiş, bağlantıların tespit edilebilme ihtimali arttırılmıştır.

Saldırganların zafiyeti belli olan sistemleri toplu halde aramak veya web uygulaması hakkında bilgi toplamak için arama motorlarının kullandığı bilinmektedir. Son olarak arama motorlarında bağlantı yapılarının listelenip listelenmeyeceğine dair izinleri barındıran robots.txt dosyası Türkçe web uygulamalarından çekilmiş içerisindeki Türkçe kelimeler listeye eklenmiştir.

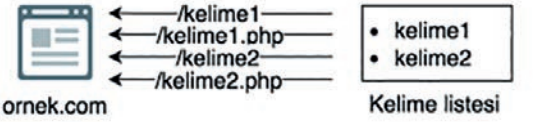
Oluşturulan kelime listesi içerisinde rakamları, sayıları ve küçük harflerle Türkçe kelimeler barındıran tekil bir listeden oluşan bir metin dosyasıdır. Bu dosya içerisindeki bazı Türkçe karakter içeren kelimeler, Türkçe karakterlerin (ü,ı,ö,ş,ç,ğ) İngilizce karşılıkları (u,i,o,s,c,g) ile değiştirilerek yeniden listeye eklenmiştir.

Web sunucu ayarlarında harfe duyarlı bağlantılar tanımlanması durumunda büyük ve küçük harf bağlantılar farklılık göstereceğinden dolayı kelimelerin hem küçük ve ilk harfinin büyük hem de tamamının büyük olduğu ayrı geniş bir listede hazırlanmıştır.

6.5.2. Web Uygulamalarından Bilgi Toplanması ve Bağlantı Tahmini

Web uygulamalarında bağlantı yapısında uygulamada kullanılan programlama teknolojileri, yazılım geliştiricilerin tercihleri ve dil yapısı etkili olmaktadır. Bağlantıda kullanılan dilin yapısı web uygulamaların içerisinde bulunan bağlantılar kullanılarak analiz edilerek kolaylıkla bulunabilmektedir. Yazılım geliştiricisinin bağlantı yapısındaki tercihleri örnek statik kod analizleri ile belirlenir. Web uygulamalarında kullanılan yazılım dili dosyaların uzantılarını etkilediğinden dolayı bağlantı yapısını etkilemektedir.

Bu çalışma Türkçe web uygulamalarındaki gizli kalan bağlantıları dışarıdan tespit etmeye yönelik olduğundan dolayı yazılım dillerinin tespit edilmesi önem taşımaktadır. Yazılım dillerinin dosya uzantılarına etkisinden dolayı bağlantı yapısını değiştirebileceği değerlendirilmektedir. Şekil 6.24'de bağlantı yapısında bir kelimenin hem dizin hem de dosya olarak denenmesi örnek olarak gösterilmektedir.



Şekil 6.24. Dosya ve dizin denenmesi

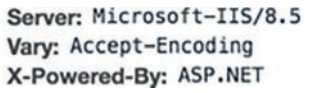
Kullanılan yazılım dili ya da web sunucularında yapılan ayarlar dolayısıyla değişen dosya uzantıları bağlantı tahmininde edinilmesi gereken bilgilerdir. Bağlantılarda kullanılan dosya uzantısını tespit etmek için gerekli bilgileri toplama yöntemi bu çalışmada dörde ayrılmıştır.

1. Gezinilebilen web sayfalarının kaynak kodunun incelenmesi
2. Web sunucu başlık bilgilerinin incelenmesi
3. Deneme yoluyla
4. Arama motorları kullanımı ile

Web uygulamalarında gezinilen sayfaların kaynak kodlarında bulunan bağlantlılar kullanılan uzantı hakkında bilgi vermektedir. HTML kodları içerisinde kullanılan "a href" etiketi ile oluşturulan

bağlantılar dosya uzantısı içermesi durumunda yapılan incelemeler ile kullanılan uzantı tespit edilebilir. Bazı web uygulama teknolojileri kaynak kodlara kendilerine özel imzalar ekleyebilirler. Bu imzalar ile de kullanılabilecek dosya uzantılı tahmin edilebilir.

Web sunucuları varsayılan olarak web uygulamalarında kullanılan yazılarım dillerini, cevap mesajlarının HTTP başlıklarında gönderebilirler. Cevap mesajı içerisinde X-Powered-By başlığında kullanılan teknoloji belirtilmektedir. Şekil 6.25'de X-Powered-By başlığı içerisinde gönderilen değer incelendiğinde ilgili web uygulamasının PHP ile geliştirildiği görülmektedir. Fakat bu başlık sunucu tarafındaki ayarlar ile kapatılabilir veya değiştirilebilir.



Şekil 6.25 . X-Powered-By başlığı

Diğer bir yöntem olan deneme yöntemi ile web uygulamalarında kullanılan uzantıların, varsayılan olarak gelen dizin ana sayfa isimleri ile birlikte denenmesidir. Dizin anasayfa isimleri bir dizine yapılan istek sonrası o dizin içerisinde varsayılan olarak web sunucusu tarafından bakılacak dosya isimleridir. En çok kullanılan isimlerden biri index.html dosya adıdır, web sunucular tarafından sunucu tarafındaki programlama dillerinin uzantılarını da içeren bir liste olarak tanımlanabilir (default,index,index.php,default.asp vb).

Web uygulamalarında kullanılan bazı dosya uzantıları Çizelge 6.3'de sunulmaktadır.

Çizelge 6.3. Web uygulamalarında kullanılan bazı dosya uzantıları

spx	axd	asx	asmx	asp	cfm	yaws
swf	html	xhtml	jsp	jspx	wss	do
action	pl	php4	php3	phtml	rb	rhtml
xhtml	cgi	dll	do	action		

Bu uzantıların bilinen varsayılan olarak gelen dizin ana sayfa isimlerinden index ve default kelimelerinin sonuna eklenerek bağlantıda denemesi ve cevabın kontrol edilmesi durumunda kullanılan dosya uzantıları tespit edebilir.

Arama motorları üzerinden dosya uzantısına ait tüm sayfaların aratılması (filetype:cgi, filetype:asp, vb) ve sonuçlarda yapılan incelemelerde de kullanılan teknoloji tespit edilebilir. Bu yöntemin otomatik hale getirilmesi zor olabileceğinden dolayı diğer yöntemleri le daha hızlı sonuç alınabileceği değerlendirilmektedir.

Bağlantı yapısında bir dosya uzantısı olmaması durumunda ya da dosya uzantısının tespit edilemediği durumlarda kelime listesi dosya uzantısız olarak denenmelidir. Uzantı tespit edildiği durumlarda ise bağlantı yapısındaki dizinlerden dolayı kelime listesi dizinlerin altına hem uzantılı hem de uzantısız olarak denenmelidir.

Web uygulamalarında kullanılan dosya uzantısının bulunmasının ardından kelime listesinin bağlantı listesinde denenerek gizli kalmış bağlantıların tespit edilme işlemi gelmektedir. Bu işlem kelime listesinin öz yinelemeli olarak denenmesi ile tespit edilebilir.

Öz yinelemeli olarak denenmesi işlemi, bağlantısı yapısında bir dizinin tespit edilebilmesi durumunda tüm kelime listesinin ilgili dizin yapısı altında tekrar denenmesi gerekmektedir. Sunucudan dönen mesaj içerisinde 20 veya 30 ile başlayan bir cevap kodu olması, ilgili bağlantıya istemci tarafından doğru şekilde erişildiği ve sunucu tarafında bir karşılığı olduğu anlamını taşımaktadır. Çizelge 6.4'de ornek.com uygulamasına bağlantı tahmini için Türkçe kelime listesi kullanılarak yapılan isteklerden başarılı olan örnekler gösterilmektedir. Örnek isteklerde hedef web uygulamasında PHP kullanıldığı varsayılmakta bu nedenle .php uzantılı dosyalar tespit edilmeye çalışılmaktadır. Yapılan bağlantı denemelerinde dosya uzantılarının denenmesinden önce dizinlerin tespit edilmesi kaynak kullanımı açısından daha etkili bir yöntem olarak değerlendirilmektedir.

Çizelge 6.4. Örnek bağlantı tespit etme istekleri ve cevap kodları

Bağlantı Denemesi	Cevap kodu
ornek.com/deneme/1/deneme	200
ornek.com/yonetim	200
ornek.com/yonetim/deneme/	200
ornek.com/yonetim/kullanici.php	302
ornek.com/deneme.php	200
ornek.com/2017/	200
ornek.com/2017/10/deneme.php	200

Bağlantı denemeleri açık kaynak bağlantı tespit eden ve dosya ismini parametre olarak alan herhangi bir yazılım ile yapılabilmekte birlikte bağlantı denemesi yapan sözde (pseudo) yazılımın kodu aşağıda paylaşılmaktadır.

```
fqdn = 'sonunda / karakteri olmadan alan adı'
wordListFile ='Türkçe kelime listesi'
extension = 'kullanılan dosya uzantısı'
output = 'dizin tespitlerinin çıktılarının yazılacağı dosya'
extOutput = 'dosya tespitlerinin çıktılarının yazılacağı dosya'
Function url_test_without_ext(fqdn,wordList,output):
        Foreach Word in wordList:
                url = fqdn + '/' + Word
                request = 'url'e http isteği'
                statusCode = 'Request'a ait cevap kodu'
                if statusCode > 200 and statusCode < 400:
                        Write url to output
                        return url_test(url,wordList, output)
Function url_test_with_ext(urlList,wordList,ext,output):
        Foreach Url in urlList:
                Foreach Word in wordList:
                        url = Url + '/' + Word+'/'+ext
                        request = 'url'e http isteği'
                        statusCode = 'Request'a ait cevap kodu'
                        if statusCode > 200 and statusCode < 400:
                                Write url to output
Open "kelime listesi" as wordList
url_test_without_ext (fqdn,wordList,extenstion,output)
Open output as urlListWithoutExt
url_test_with_ext (urlListWithoutExt,wordList,extenstion, extOutput )
```

Bilgi toplaması ve Türkçe kelime listesinin denenmesi ile yapılan bağlantı tespiti sonrası zafiyet analizlerinin gerçekleştirilmesi ve

yeni tespit edilen bağlantıların herhangi bir güvenlik ihlali oluşturup oluşturulmadığı kontrol edilmelidir.

6.6. Değerlendirmeler

Bu bölümde, ülkemizde Türkçe web sitelerine yönelik olarak gerçekleştirilen güvenlik testleri ve zafiyet analizlerinde tüm kapsamın doğru şekilde test edilmesi için bağlantılarda kullanılabilecek Türkçe kelime listesiyle, ortaya çıkabilecek zafiyetler, kapatma yöntemleri, etkileri ele alınmış farklı senaryolar ile örnekler üzerinde çözümler üretilmiş ve gösterilmiştir.

Bu bölümde sunulan Türkçe kelime listesinin oluşturulması ve web uygulamalarında bilgi toplama aşamasında bağlantı tespitinde denenmesi ile güvenlik testlerinde kullanılan bilgi toplama yöntemleri ve araçları kullanılarak Türkçe web uygulamalarında bağlantı tespitinin yetersiz yapılması, zafiyetlerin giderilememesi, kapsamın doğru tespit edilememesi problemlerine çözümler üretilmiştir.

Gerçekleştirilen çalışmada bağlantı yapısının ve bağlantı tahmini sonrası oluşabilecek zafiyetlerin daha iyi anlaşılması adına web uygulamaları ile ilgili sistemler ve teknolojiler ile alakalı bilgiler verilmiştir. Sonrasında web uygulamalarındaki zafiyetler ele alınmış, önleme yöntemleri gözden geçirilmiştir. Web uygulamalarındaki bağlantılarda kullanılabilecek Türkçe kelime listesi oluşturulmuş ve kapsamı arttırmak için gerekli bilgi toplama aşaması ele alınmıştır. Türkçe kelime listesinin kullanılması ile web uygulamalarında gizli kalan bağlantıların tespiti sonrası oluşabilecek zafiyetlere senaryo bazlı örnekler gösterilmiştir.

Çalışma öncesinde Türkçe web uygulamalarında gizli kalan bağlantıları tespit etme amaçlı oluşturulan kapsamlı bir Türkçe kelime listesi bulunmadığı görülmüştür. Bu bölümde sunulan çalışma ile;

- bilgi toplama aşamasında yardımcı olabilecek ve daha fazla kapsamı ortaya çıkaracak Türkçe kelime listesi oluşturulmuş,
- Türkçe kelime listesinin İngilizce kelime listesi ile birlikte kullanılmasıyla daha iyi sonuç alınabileceği görülmüş,
- bu çalışmanın ülkemizde özel sektör ve kamu kuruluşlarının web sayfalarının güvenliğini daha yüksek oranda sağlamada katkı sağladığı belirlenmiş,

- oluşturulan kelime listesinin açık olarak yayınlanması güvenlik problemlerine yol açabileceğinden dolayı kelime listesi öncelikle Ulusal Siber Olaylara Müdahale Merkezi (USOM) ile paylaşılmış, ve
- son olarak geliştirilen çözümün ülkemizde kamu kurumları ve sektörün web uygulamalarının güvenliğinin arttırılmasına katkılar sağlanmıştır.

Kaynaklar

[1] Internet: Amazon Is Planning to Hire 100,000 Full-Time Employees. URL: http://fortune.com/2017/01/12/amazon-full-time-employees/. Son Erişim Tarihi: 07.05.2017.

[2] Internet: 2015 Web Application Attack Report(WAAR). URL: https://www.imperva.com/docs/HII_Web_Application_Attack_Report_Ed6.pdf. Son Erişim Tarihi: 03.01.2017.

[3] Doupé, A., Cavedon, L., Kruegel, C., & Vigna, G. (2012). Enemy of the State: A State-Aware Black-Box Web Vulnerability Scanner. USENIX Security Symposium, 523–538.

[4] Jai Narayan Goela,b, BM Mehtreb, Vulnerability Assessment & Penetration Testing as aCyber Defence Technology, 3rd International Conference on Recent Trends in Computing 2015 (ICRTC-2015)

[5] Xiang F., Xin L., Boris P., Shijun Chen, Kai Q., Lixin T., AStatic Analysis Framework For Detecting SQL Injection Vulnerabilities, 20 Ağustos 2007.

[6] Prithvi B., Venkatakrishnan V. N., XSS-GUARD: Precise Dynamic Prevention of Cross-Site Scripting Attacks, 2008.

[7] Abdul R., Khalid L., Farooq Ahmad H., Ali H., Zahid A., Peter Charles B., Semantic security against web application attacks, 6 Ağustos 2013.

[8] Víctor H. G., Raúl M., Maricela Q., Web Attack Detection Using ID3, 2006.

[9] YongJoon P., JaeChul P., Web Application Intrusion Detection System for Input Validation Attack, Kasım 2008.

[10] Internet: Dirsearch. URL: https://github.com/maurosoria/dirsearch. Son Erişim Tarihi: 12.04.2017.

[11] Internet: Wfuzz - The Web fuzzer. URL: https://github.com/xmendez/wfuzz. Son Erişim Tarihi: 12.04.2017.

[12] Internet: AngryFuzz3r. URL: https://github.com/ihebski/angryFuzzer. Son Erişim Tarihi: 12.04.2017.

[13] Internet: Cansina. URL: https://github.com/deibit/cansina/. Son Erişim Tarihi: 12.04.2017.

[14] Internet: Burp Dirbuster. URL: https://github.com/vulnersCom/burp-Dirbuster. Son Erişim Tarihi: 12.04.2017.

[15] Internet: DirBuster. URL: https://sourceforge.net/projects/dirbuster/files/. Son Erişim Tarihi: 13.04.2017.

[16] Yılmaz V., Kurumsal Bilgi Güvenliği ve Sızma (Penetrasyon) Testleri, Gazi Universitesi, Mayıs 2007

[17] Razzaq, A., Latif, K., Farooq Ahmad, H., Hur, A., Anwar, Z., & Bloodsworth, P. C. (2014). Semantic security against web application attacks. Information Sciences, 254, 19–38. https://doi.org/10.1016/j.ins.2013.08.007

[18] Lee, J. K., & Sohn, M. M. (2003). The eXtensible Rule Markup Language. Communications of the ACM, 46(5), 59–64.

[19] Internet: Usage of server-side programming languages for websites. URL: https://w3techs.com/technologies/overview/programming_language/all. Son Erişim Tarihi: 25.06.2017.

[20] Internet: CodeIgniter Framework. URL: https://codeigniter.com/ Son Erişim Tarihi: 17.05.2017.

[21] İnternet: How does internet work ? URL: http://www.theshulers.com/whitepapers/ internet_whitepaper /index.html#ip. Son Erişim Tarihi : 08.08.2017.

[22] Internet: Internet Engineering Task Force. URL: https://en.wikipedia.org/wiki/Internet_Engineering_Task_Force. Son Erişim Tarihi: 15.05.2017.

[23] Internet: World Wide Web Consortium. URL: https://en.wikipedia.org/wiki/World_Wide_Web_Consortium. Son Erişim Tarihi: 22.06.2017.

[24] Pham, K., Santos, A., & Freire, J. (2016). Understanding Website Behavior based on User Agent. Proceedings of the 39th International ACM SIGIR Conference on Research and Development in Information Retrieval - SIGIR '16, 403, 1053–1056.

[25] Prokhorenko, V., Choo, K. K. R., & Ashman, H. (2016). Web application protection techniques: A taxonomy. Journal of Network and Computer Applications, 60, 95–112.

[26] Akyazı, U. (2011). Gezgin Etmenler ve Doğadan Esinlenen Sezgiseller Kullanılarak Dağıtık Bilgisayar Güvenliğinin Sağlanması

[27] Şahinaslan, E., Kandemir, R., & Kantürk, A. (2010). Bilgi Güvenliği Risk Yönetim Metodolojileri ve Uygulamaları Üzerine İnceleme. ABGS 2010–Ağ ve Bilgi Güvenliği Sempozyumu.

[28] Internet : UEKAE BGYS-0004 BGYS Risk Yönetim Süreci Kılavuzu. URL: https://www.bilgiguvenligi.gov.tr/bilgi-guvenligi-yonetimi-dokumanlari/uekae-bgys-0004-bgys-risk-yonetim-sureci-kilavuzu.html. Son Erişim Tarihi: 07.05.2017.

[29] Feng, N., & Li, M. (2011). An information systems security risk assessment model under uncertain environment. Applied Soft Computing, 11(7), 4332–4340.

[30] Küçükşahin, A. (2006). Güvenlik Bağlamında, Rïsk Ve Tehdït Kavramları Arasındakï Farklar Nelerdïr Ve Nasıl Belïrlenmelïdïr ?, Güvenlik S(4), 7–41.

[31] Nelson, A. (2007). Penetration Testing and Vulnerability Assessments. Network Communications and Emerging Technologies (JNCET), (8), 1–2.

[32] Knowles, W., Baron, A., & McGarr, T. (2016). The simulated security assessment ecosystem: Does penetration testing need standardisation? Computers and Security, 62, 296–316.

[33] Internet: Penetration Testing. URL: https://www.fireeye.com/services/penetration-testing.html. Son Erişim Tarihi: 05.04.2017.

[34] Engebretson, P. (2013), The Basics of Hacking and Penetration Testing, Second Edition: Ethical Hacking and Penetration Testing Made Easy, S53.

[35] Rahalkar, S. A. (2016). Certified Ethical Hacker (CEH) Foundation Guide, 97–107.

[36] Internet: Harvester. URL: https://github.com/laramies/theHarvester. Son Erişim Tarihi: 02.05.2017.

[37] Bau, J., Bursztein, E., Gupta, D., & Mitchell, J. (2010). State of the art: Automated black-box web application vulnerability testing. Proceedings - IEEE Symposium on ecurity and Privacy, 332–345.

[38] Gupta, S., & Gupta, B. B. (2017). Cross-Site Scripting (XSS) attacks and defense mechanisms: classification and state-of-the-art. International Journal of Systems Assurance Engineering and Management, 8(s1), 512–530.

[39] Internet : Protection, Usability and Improvements in Reflected XSS Filters. URL: http://www3.cs.stonybrook.edu/~rpelizzi/xss.pdf. Son Erişim Tarihi: 22.04.2017.

[40] Rao, K. S., Jain, N., Limaje, N., Gupta, A., Jain, M., & Menezes, B. (2016). Two for the price of one: A combined browser defense against XSS and clickjacking. 2016 International Conference on Computing, Networking and Communications, ICNC 2016.

[41] Baranwal, A. K. (2012). Approaches to detect SQL injection and XSS in web applications. Eece 571B, Term Survey Paper, April 2012, (April).

[42] Hydara, I., Sultan, A. B. M., Zulzalil, H., & Admodisastro, N. (2015). Current state of research on cross-site scripting (XSS) - A systematic literature review. Information and Software Technology, 58, 170–186.

[43] S.Shalini, & S.Usha. (2011). Prevention Of Cross-Site Scripting Attacks XSS On WeApplications In The Client Side. International Journal of Computer Science Issues, 8(4), 650–654.

[44] Pan, J., & Mao, X. (2017). DomXssMicro: A micro Benchmark for evaluating DOM-based cross-site scripting detection. Proceedings - 15th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, 10th IEEE International Conference on Big Data Science and Engineering and 14th IEEE International Symposium on Parallel and Distributed Proce, 208–215.

[45] Shar, L. K., & Tan, H. B. K. (2012). Defending against cross-site scripting attacks. Computer, 45(3), 55–62.

[46] Internet: 2011 CWE/SANS Top 25 Most Dangerous Software Errors. URL: http://cwe.mitre.org/top25/ . Son Erişim Tarihi: 08.04.2017.

[47] Gupta, B. B., Gupta, S., Gangwar, S., Kumar, M., & Meena, P. K. (2015). Cross-Site Scripting (XSS) Abuse and Defense: Exploitation on Several Testing Bed Environments and Its Defense. Journal of Information Privacy and Security, 11(2), 118–136.

[48] Gupta, S., & Gupta, B. B. (2016). Automated Discovery of JavaScript Code Injection Attacks in PHP Web Applications. Physics Procedia, 78(December 2015), 82–87.

[49] Internet: Beef Project. URL: https://github.com/beefproject/beef/wiki/. Son Erişim Tarihi: 24.04.2017.

[50] S. Fogie et al., XSS Attacks: Cross Site Scripting Exploits and Defense, Syngress, 2007

[51] Shar, L. K., & Tan, H. B. K. (2012). Defending against cross-site scripting attacks. Computer, 45(3), 55–62.

[52] Shanmugam, J., & Ponnavaikko, M. (2007). Behavior-based anomaly detection on the server side to reduce the effectiveness of Cross Site Scripting vulnerabilities. 3rd International Conference on Semantics, Knowledge, and Grid, SKG 2007, 350–353.

[53] Vogt, P., Nentwich, F., Jovanovic, N., Kirda, E., Kruegel, C., & Vigna, G. (2007). Cross-Site Scripting Prevention with Dynamic Data Tainting and Static Analysis. Work, 42(13), 4188–4190.

[54] Wassermann, G., & Su, Z. (2008). Static detection of cross-site scripting vulnerabilities. ICSE '08 Proceedings of the 30th International Conference on Software Engineering, 171–180.

[55] Elshazly, K., Fouad, Y., Saleh, M., & Sewisy, A. (2014). A Survey of SQL Injection Attack Detection and Prevention. Journal of Computer and Communications, 2(8), 1–9.

[56] Mavromoustakos, S. (2016). Causes and Prevention of SQL Injection Attacks in Web Applications, 1–5.

[57] Bhor, R. V. (n.d.). Analysis of web application security mechanism and attack detection using vulnerability injection technique.

[58] Kim, M. Y., & Lee, D. H. (2014). Data-mining based SQL injection attack detection using internal query trees. Expert Systems with Applications, 41(11), 5416–5430.

[59] Internet: Bernardo Damele, A., & Stampar, M. (2013). SQLMAP – automatic SQL injection and database takeover tool. URL: http://sqlmap.org. Son Erişim Tarihi: 17.03.2017.

[60] Internet: SqlMap. URL: https://github.com/sqlmapproject/sqlmap/wiki/Techniques. Son Erişim Tarihi: 13.03.2017.

[61] Sadeghian, A., Zamani, M., & Abdullah, S. M. (2013). A Taxonomy of SQL Injection Attacks. 2013 International Conference on Informatics and Creative Multimedia, 269–273.

[62] Pramod, A., Ghosh, A., Mohan, A., Shrivastava, M., & Shettar, R. (2015). SQLI detection system for a safer web application. Souvenir of the 2015 IEEE International Advance Computing Conference, IACC 2015, 237–240.

[63] Tandel, N., & Patel, K. (2014). Mitigation of CSRF Attack, 3(6), 1416–1420.

[64] Internet: 2013 Top 10 List. URL: https://www.owasp.org/index.php/Top_10_2013-Top_10. Son Erişim Tarihi: 13.06.2017.

[65] Dukes, L., Yuan, X., & Akowuah, F. (2013). A case study on web application security testing with tools and manual testing. 2013 Proceedings of IEEE Southeastcon, 1–6.

[66] Ding, C. (2013). Cross-Site Request Forgery Attack and Defence: Literature Search, 2–3.

[67] Chaudhari, K., & Tijare, M. (2016). Prevention of CSRF attack using STG pattern and JSED. International Journal of Applied Engineering Research, 11(7), 4934–4938.

[68] Gaw, S., & Felten, E. W. (2006). Password management strategies for online accounts. Proceedings of the Second Symposium on Usable Privacy and Security - SOUPS '06, 44.

[69] Das, A., Bonneau, J., Caesar, M., Borisov, N., & Wang, X. (2014). The Tangled Web of Password Reuse. Proceedings 2014 Network and Distributed System Security Symposium, (February), 23–26.

[70] Najafabadi, M. M., Khoshgoftaar, T. M., Kemp, C., Seliya, N., & Zuech, R. (2014). Machine learning for detecting brute force attacks at the network level. Proceedings - IEEE 14th International Conference on Bioinformatics and Bioengineering, BIBE 2014, 379–385.

[71] Khan, A. A. (2013). Preventing Phishing Attacks using One Time Password and User Machine Identification, 68(3), 7–11.

[72] Bocić, I., & Bultan, T. (2016). Finding access control bugs in web applications with CanCheck. Proceedings of the 31st IEEE/ACM International Conference on Automated Software Engineering - ASE 2016, 155–166.

[73] Gonz, H. F., Polit, U., San, D., & Potos, L. (2008). Types of hosts on a Remote File Inclusion (RFI) botnet, 105–109.

[74] Begum, A., Hassan, M., Bhuiyan, Y., & Sharif, H. (2016). RFI and SQLi Based Local File Inclusion Vulnerabilities in Web Applications of Bangladesh, 1(December), 12–13.

[75] Internet: OWASP Testing Guide v4 Table of Contents. URL: https://www.owasp.org/index.php/OWASP_Testing_Guide_v4_Table_of_Contents. Son Erişim Tarihi: 16.04.2017.

[76] Tajbakhsh, M. S., & Bagherzadeh, J. (2015). A sound framework for dynamic prevention of Local File Inclusion. In 2015 7th Conference on Information and Knowledge Technology, IKT 2015.

[77] Asmawi, A., Affendey, L. S., Udzir, N. I., & Mahmod, R. (2012). Model-based system architecture for preventing XPath injection in database-centric web services environment, 5(10), 621–625.

[78] Florescu, D., Grünhagen, A., & Kossmann, D. (2003). XL: An XML programming language for Web service specification and composition. Computer Networks, 42(5 SPEC.), 641–660.

[79] Jensen, M., Gruschka, N., Herkenhoner, R., & Luttenberger, N. (2007). SOA and Web Services: New Technologies, New Standards - New

Attacks. In Fifth European Conference on Web Services (ECOWS'07) (pp. 35–44).

[80] Internet: Lightweight Directory Access Protocol (LDAP): The Protocol. URL: https://tools.ietf.org/html/rfc4511. Son Erişim Tarihi: 22.04.2017.

[81] Knap, T., & Mlýnkovà, I. (2009). Towards more secure web services: Pitfalls of various approaches to XML signature verification process. 2009 IEEE International Conference on Web Services, ICWS 2009, 543–550.

[82] Alonso, C., Bordón, R., Guzmán, A., & Beltrán, M. (2008). LDAP Injection & Blind LDAP Injection In Web Applications.

[83] O. Aktaş, Web Uygulamalarında Zafiyet Oluşturabilecek Türkçe Dosya ve Dizin İsimleri Analizi, Yüksek Lisans Tezi, Gazi Üniversitesi, Fen Bilimleri Enstitüsü, Bilgi Güvenliği Mühendisliği ABD, 2018, Ankara.

Kablosuz Algılayıcı Ağlarında Güven

BÖLÜM 7

Gülüstan DOĞAN

KABLOSUZ ALGILAYICI AĞLARINDA GÜVEN

Bu bölümde; güvenin tanımlanması, değişik alanlarda kullanımı ve özellikleri kısaca incelenmiş, siber güvenlikte yeri anlatılmış, güvenlik uygulama yöntemlerinden birisi olan güven kavramının kablosuz algılayıcı ağlar içerisindeki yeri ve bu konuda gelişmeler gözden geçirilmiş, yapılan bazı çalışmalar ile uygulamalar özetlenmiş, son olarak da konularla ilgili görüş ve önerilerde bulunulmuştur.

7.1. Tanımlar: Güven, Güvenilirlik ve İtibar

Türkçe bir kelime olan "Güven", Türk Dil Kurumu (TDK) Sözlüğünde "Korku, çekinme ve kuşku duymadan inanma ve bağlanma duygusu, itimat" [1] şeklinde tanımlanmaktadır. Diğer sözlüklerde de benzer ifadelerle tanımlanan ve insanlık tarihiyle yaşıt olduğu düşünülen güven kavramı, son yıllarda bilişim terimi olarak da kullanılmaya başlamıştır.

Güven konusu uzun bir süre için araştırılmıştır [34]. Bu konu sosyal bilimler [35], ekonomi [36] gibi birçok disiplinler tarafından incelenmiştir. İnsanlar her gün evde, işte, sosyal yaşamlarında güveni kullanmaktadırlar. Bilişim ve siber güvenlikte de güven çok önemli bir yere sahiptir. Ancak güvenin tek bir tanımının olduğunu söyleyemeyiz. Kullanıldığı alana göre farklı tanımları yapılmıştır.

Josang vd. [5], güveni tanımlarken Gambetta'nın tanımlamalarını temel alırlar [6]. Gambetta güveni şu şekilde tanımlamıştır [6]. **Güven** (veya simetrik olarak güvensizlik), bir ajanın, başka bir ajanın veya bir ajan grubunun, bu tür bir eylemi izleyebilmesinden önce (veya her zaman kendi kapasitesinden bağımsız olarak), belirli bir eylemi gerçekleştireceğine dair belirlediği öznel bir olasılık seviye-

sidir. Josang güveni şöyle tanımlamıştır; bir tarafın, herhangi bir durumda, göreceli güvenlik hissi veren belirli bir durumda, olumsuz sonuçların ortaya çıkmasına rağmen, birine veya bir şeye bağlı kalma isteğinin kapsamıdır. Güven 0 (tam güvensizlik) ve 1 (tam güven) arasında değişen nesnel bir olasılıktır [5]. Siber güvenlik söz konusu olduğunda güvenin net bir değerinin olması gerekmektedir. Sosyal bilimlerdeki gibi belirsiz ifadeler kullanılamamaktadır. O yüzden çoğu çalışmada ya 1-0 ya da 1 ile 0 arasında değişen bir rasyonel değer olarak kullanılmıştır.

Güvenilirlik

Solhaug vd. güvenilirliği güvenilen belirli bir eylemi güvenilen kişinin çıkarlarına bağlı objektif bir olasılık olarak tanımlarlar [7]. Güven ve güvenilirlik birbirleriyle ilişikli kavramlardır ve bazen birbirlerinin yerine kullanılabilir [38]. Ancak güvenilirlik güvenden farklıdır. Güvenilirlik, güvenden daha kapsamlı bir kavramdır ve güvenilirlikteki yük, güvenden daha fazladır. Güven ve güvenilirlik arasındaki temel fark ise şudur. Güven düşünülen olasılık değeri, güvenirlik ise gerçek olasılık değeridir. Bu fark ortaya risk faktörünü çıkarır [4]. Güvenin yanlış konumlandırılması risk faktörünü artırır.

İtibar

Güvenle ilişkili olduğundan dolayı itibar (reputation) da önemli bir kavramdır. Bazen itibar ve güven aynı bağlamda kullanılabiliyor olsa da ikisi farklı anlamlara sahiptir. İtibar bir birimin diğer bir birimin hakkındaki görüşünü temsil eder. Ancak güven ise bir birimin itibarının türevidir.

7.2. Farklı Alanlarda Güven

Momani ve Challa'nın çalışmasında güvenin sosyal bilimler, e-ticaret, dağıtık sistemler ve ad-hoc ağlarındaki tanımları verilmiştir [54], [25], [29]-[34].

7.2.1. Sosyal Bilimler ve E-Ticarette Güven

Güven insan yaşamının bir parçası olduğundan, sosyal bilimlerle ilişkisi oldukça fazladır [10], [11]. Güven arkadaşlık etme, sırlarını

paylaşma, satış ve satın alma işlemlerinde ve birlikte çalışma gibi insan ilişkilerinde büyük bir etkiye sahiptir. Güven karar alma işlemlerinde, delegasyon, belgelendirme ve kaynak erişimindeki yardımlarıyla günlük yaşantımızı kolaylaştırır [12].

Güven araştırmalarındaki motivasyon alanlarından biri de e-ticarettir. İnternette alıcılar ve satıcılar arasında bir güven ilişkisi vardır. Alıcılar güvendikleri satıcılardan ürün alırlar. Güven, satıcılarının itibarı üzerine kuruludur. Satıcı geçmişte yaptığı davranışlarıyla itibar kazanır. Bay [41], Yahoo [13] ve Keynote [14], [15] gibi bazı e-ticaret sistemleri, itibar ve güven değerlerini sürdürmek için bir merkezi güven yetkisi sağlarlar.

Abdul-Rahman ve Hailes güvenin özelliklerine dayalı sosyolojik bir güven modeli tasarlamışlardır [16]. Modellerinde, kuruluşlara kendi itibarlarına ve doğrudan deneyimlerine bağlı olarak bir güven değeri verilir.

Josang ve Ismail elektronik marketler için bir itibar sistemi geliştirmiştir [17]. Çoğu itibar sistemi sezgisel ve geçicidir fakat onlar itibar sistemlerini istatistikteki beta yoğunluk fonksiyonu üzerine inşa etmişlerdir. Bu beta dağılımı durumların gerçekliği noktasında bir fikir sunar.

7.2.2. Dağıtık ve Akran Sistemlerde Güven

Dağıtık sistemlerde, varlıkların güveni değerlendirmek için merkezi bir sistemleri yoktur [9]. Bu nedenle varlıklar kendi eşleriyle ile bilgi alışverişinde bulunarak kendi güven görüşlerini oluştururlar. Genellikle oyun teorisi [18] ve Bayes ağ [19] metotları, dağıtık sistemlerin güvenini hesaplamak için kullanılır.

Aberer ve Despotovis, P2P sistemleri için bir itibar yönetimi sistemi öneren ilk araştırmacılardır [20]. Bu sistemde, bir merkezi yetkiden bilgi gerektirmeyen algoritmalar ve veri yapıları kullanılmıştır. Güven modelleri, düğümler arasındaki geçmiş etkileşimlere dayanmaktadır. Tasarladıkları sistemlerinin dezavantajı ise sadece olumsuz geri bildirimlerin kabul edilmesi ve sistemin sadece akran (peer) aksaklıklarına duyarlı olmasıdır.

Akran (Peer-to-peer) sistemleri için başka güven modelleri de vardır. Bu çalışmada algılama ağlarındaki güven modelleriyle ilgile-

nildiğinden ayrıntıya girilmemiştir. Momani ve Challa tarafından incelenen diğer güven mekanizmaları Bayesian Network Model [19], SECURE [21], UniTec [22], BambooTrust [23], B-trust model [24] modelleridir.

7.2.3. Ad-Hoc Ağlarda Güven

Geçici ağlarda düğümler çok sık yer değiştiren ağlara katılırlar. Ağın işlevselliğini destekleyen hiçbir düğüm yoktur. Düğümler arasındaki ilişki, ağda sürekli meydana gelen değişim gibi dinamiktir [37], [25], [57].

Geçici ağlarda güven mekanizmaların çoğunluğu oyun teorisi ve Bayes ağ yaklaşımlarını kullanır. CONFIDANT [26] ve CORE [27] bu sistemlere örnek verilebilir.

7.3. Siber Güvenlikte Güven Kavramı

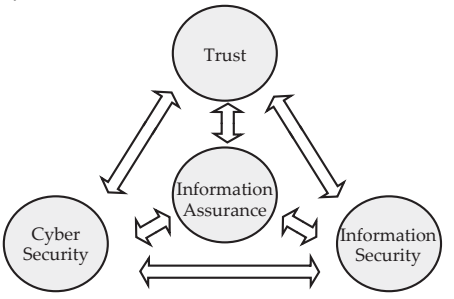
Çevrimiçi sistemlerin yaygınlaşması ve Endüstri 4.0 ile birlikte birçok ortamda robotlar gibi otonom akıllı sistemlerin kullanılması ile bu sistemlere duyulan güven ile ilgili bazı sorunlar ortaya çıkmıştır. Bunun üzerine literatürde güven (trust) isimli kavram tanımlanmıştır [61]. İnsanların çevrim içi ve makine etkileşimi içeren ortamlarda birbirleriyle ve makineyle tüm etkileşimleri bir siber güven temeli üzerine oturmaktadır. Örneğin e-ticaret gibi çevrimiçi bir ortamda insanların birbirleriyle iletişimlerini güven etkilemektedir. Özellikle internetteki birçok uygulamada güven temel oluşturmaktadır. İnsan kullandığınız her uygulamaya, internette iletişime geçtiğiniz her kişiye karşı bir güven geliştirmektedir. Aynı zamanda makine ve uygulamalarda bize karşı bir güven geliştirmektedir. Özellikler geriye dönük bilgilerin tutulabilmesi ve yapay zekâ çalışmaları sayesinde makinelerin de insan için geliştirdiği matematiksel bir güven olabilmektedir. Şekil 7.1. de de görüldüğü üzere güven, siber güvenlik ve bilgi güvenliği konuları çok ilgilidir [62]. Teknolojiyi kullanarak kaliteli ve güvenilir bilgi üretmek için tüm bu kavramlar birlikte önem kazanmaktadır.

Siber güvenin önem kazandığı bir diğer alan da, etkileşim kurdukları insanlar tarafından robot gibi otonom sistemlere nasıl güvenilebileceği konusudur. Bu çok önemlidir çünkü otonom sistemler

güven olmadan yaygın olarak kabul edilmeyecektir. Güven oluşturmanın etkili bir yolu, insanlara otonom sistemlerin onlarla iletişim kurabileceklerini göstermektir. Ancak bu konu güven analizinin zor hesaplanabilir olması ve hesaplamanın çok soyut bir düzeyde gerçekleştirilebilir olması dezavantajına sahiptir. Çoğu çalışma otonom sistemlerin belirli kurallara göre çalıştığını ispatlayarak insanların bu sistemlere güvenini artırmak şeklinde olmuştur.

Cho vd. yaptıkları çalışmada güveninin özelliklerini şu şekilde sıralamışlardır [8]. Tablo 7.1'de listelenilen maddeler de güvenin özelliğidir [62].

- **Dinamiklik:** Bir sistemdeki ajanlardaki hata ve hareketlilik dolayısıyla siber güvenlik sistemleri yüksek bir dinamikliğe sahiptir, bu nedenle güven de dinamik olmalıdır.
- **Öznellik:** Ağ dinamik olduğu için düğümler aynı düğümdeki güven seviyelerini farklı düzey seviyesine yerleştirmeye karar verebilirler [5].
- **Geçişlilik:** Güvenin kesin olarak geçişli olduğu söylenemez. Geçişlilik için iki tip güvene ihtiyaç duyarız. Birincisi güvenilen (trustee) içerisinde güven, ikincisi güvenilenin (trustee) önerilerindeki güven.
- **Asimetri:** Bir ajan diğer bir ajana güvenebilir ama güvenilen (trustee) güvenene (trustor) güvenmeyebilir.
- **İçerik-bağımlılık:** Güven, içerik-bağımlıdır [6]. Örneğin bir ağda bir düğüm diğer bir düğümden gelen görüntü verilerine güvenebilir ama bir düğüm aynı düğümden gelen ses verilerine güvenmiyor olabilir.



Şekil **7.1.** Siber Güvenlik ve Güven İlişkisi [62]

Veri toplama işlemi, güven yönetim modeli tasarımı sürecinde oldukça önemlidir. Güven modellerini girdi olarak kullanabilecek birçok veri vardır. Örneğin bir ajanın uzun süre hayatta olmaması veya bir ajanın rastgele görünmesi ve kaybolması güvenli olamayabilir. İletişim katmanında eksik bilgi veren bir ajan güvenilir olmayacaktır. Örnek olarak bir yangın alarm algılayıcısının düşük güven değerinde aktif duruma geçmesi verilebilir [4]. Bu yangın alarm sistemine güvenilirliğin düşmesi gerektiğini gösterir. Bu bağlamda daha önceki sistem geçmişi bilinmeli ve geçmiş davranışları göz önüne alınmalıdır [4]. Bizim çalışmalarımızda geliştirdiğimiz sistemimiz de geçmişteki davranışları hesaplama ve analiz etme noktası düşünülerek tasarlanmıştır. Ayrıca güven yönetim sistemindeki her ajan (agent) geçmiş zaman aralıklarında oluşturulan verilerin hata payını göz önüne alarak, bu hata paylarıyla ilgili istatistiki bilgi tutabilme yeteneğine sahiptir. Yalnız, bu istatistiki bilgilerin güven modeline büyük bir yük getirmesi en büyük kısıtlayıcı etkenlerden birisidir. Bu yüzden güven modellerinin sisteme büyük bir yük getirmemesi önemlidir [4].

Tablo 7.1. Güvenin özellikleri

Özellik	Örnek
Güven ölçülebilir.	A varlığının B varlığına güveni, C varlığına güveninden daha çoktur.
Güven içerikle bağlantılıdır.	Varlık A, URL filtreleme yapmak için B'ye güvenebilir, ancak kimlik doğrulama görevi yapmak için B'ye güvenmez.
Güven zamanla değişir.	A'nın B'ye olan güveni etkileşimler gerçekleştikçe artabilir veya azalabilir.
Güven yönlü olabilir.	A varlığı B'ye güvenebilir fakat B varlığı A'ya güvenmeyebilir.
Güvenin sosyal farkındalığı vardır.	A varlığı C varlığına güvenebilir, çünkü C, B tarafından A'ya tanıtılmıştır ve A zaten B'ye güvenir.

7.4. Kablosuz Algılama Ağlarında Güven

Güven, kablosuz algılama ağları gibi kendi kendini yönetebilen ve yapılandırabilen sistemler için oldukça önemli bir kavramdır.

Güven kavramı, kablosuz algılama ağlarında elde edilen verilerin inandırıcılığı noktasında önemli bir yer teşkil etmektedir. Kablosuz algılama ağları, sınırlı hesaplama yeteneğine ve enerji noktasında kısıtlı imkânlara sahip olmaları ve ağ saldırılarına maruz kalabilme ihtimalleri dolayısıyla çok hassas bir yapıya sahiptirler. Buna ek olarak bir kablosuz algılama ağının dışarıdaki fiziksel saldırılara da açık olması ayrı bir sorun teşkil etmektedir. Bir kablosuz algılama ağında güven yönetim modeli, bir düğüm arızası veya aksaklığı meydana geldiği zaman, bu hataları ve aksaklıkları göz ardı edebilir bir noktaya çekmek için karar verme sürecinde etkili bir rol alır. Örneğin, bir düğüm başka bir düğümle bu güven modelini temel alarak iş birliği yapmaya karar verebilir. Güven konusunda yapılan çalışma sayısının az olduğu göz önüne alındığında bu araştırma konusunun yeni olduğu çıkarımı yapılabilir [2], [3]. Daha çok P2P ağlar ve Ad-hoc ile ilgili çalışmalarda güven kullanılmıştır. Bu ağ tiplerinin birbirine çok benzer olmasına rağmen kablosuz algılama ağlarının sınırlı işlem yapabilme kapasitesine sahip olmaları ve enerji noktasındaki kısıtlarının olması nedeniyle hala yeni güven yönetim modelleri geliştirilmeye çalışılmaktadır.

Güven kavramının sosyal güven, zihinsel güven ve haberleşme güveni gibi birçok farklı türü vardır. Kablosuz algılama ağlarında veri elemanları ve algılama düğümleri arasındaki bilgi güveni değerlendirilmiştir. Bilgi güveni veya veri güveni nesneler veya işlemler ile üretilen verilerin güven bölgesini ifade eder. Bir ağdaki bilgi güveni, ağda biriken hatalı verileri önleyebildiği için önemlidir. Bir ağdaki bir düğüm veri oluşturabilir, veriyi bir füzyon gibi işleyebilir ve veriyi aktarabilir.

Kablosuz algılama ağları gizlice dinlenme, uydurma, sızma, paketlerin değiştirilmesi gibi farklı saldırı senaryolarıyla karşılaşabilirler. Bu tarz saldırılar gizlilik, hesap verebilirlik, veri bütünlüğü, veri kimlik doğrulaması ve veri tazeliği gibi konuları gündeme getirmektedir. Kablosuz algılama ağlarında güvenle ilgili daha önce yapılan çeşitli çalışmalar vardır [2], [28]. Momani ve Challa tarafından kablosuz algılama ağların güvenliğiyle alakalı bazı çalışmalar yapılmıştır [54], [25], [29]-[34]. Şifreleme mekanizmaları bu sorunları tamamen çözememiştir. Kötü niyetli düğümler tarafından meydana gelebilecek sistem hataları, hatalı veri ve kötü yönlendirme ağın

arızalanmasına sebep olabilir. Şifreleme yaklaşımları istatistik, e-ticaret, sosyal bilimler gibi alanlarda araçları ile birlikte entegre edilmelidir. Bazı düğümler kötü niyetli davranabilir. Bu yüzden güven mimarilerinin, kötü düğümleri keşfetmesi ve bu düğümleri saf dışı bırakması gerekir. Bu bağlamda araştırmacılar tarafından benimsenen farklı yaklaşımlar mevcuttur [25]. Bunlar:

- Bir alt ağdaki tüm düğümler için bir güven ve itibar tablosu sağlamak
- Düğümlerin davranışlarını izlemek için bir izleme mekanizması kullanmak
- Hatalı düğümleri keşfedip onları ağdan uzaklaştırmak
- Protokol kurallarına uyacak olan düğümleri ödüllendirmek
- Verilerin bütünlüğünü korumak için düşük maliyetli şifreleme kullanmak

Düğümler arasında güven kurulması kablosuz algılama ağlarında etkili bir güvenlik yaklaşımıdır. Düğümlerin iş birliği içerisinde çalışmasıyla, düğümler arasındaki güven ilişkisi kablosuz algılama ağlarının güvenliğini artırır.

Kablosuz algılama ağlarında güven ve itibar aynı kavramlar olarak düşünülmemelidir. İtibar zamanla oluşan bir kavramdır. Doğru bir karar vermek için güven, itibara dayalı olarak hesaplanmalıdır. İtibar olmadan güven, anlık davranışlara dayalı bir değere sahip olacaktır. Örneğin belli bir zaman aralığında kötü amaçlı davranmış bir düğüm, o anda iyi davranabilir ve bu da bizim aldanmamıza neden olabilir. Ancak kötü davranış geçmişini tutan bir itibar değeri olduğu zaman son eylemden aldanılma gibi bir durum meydana gelemeyecektir.

Kablosuz algılama ağları için geliştirilecek olan güven yönetim sisteminde aşağıda sıralanan noktalara dikkat etmek gerekir.

(1) İlk Elden Bilgi Toplama

Bir algılama ağında güveni hesaplamak için kullanılan donanım hataları, enerji sorunları, düğüm yer değişimleri ve algılama okuma sapmaları gibi birçok etmen mevcuttur. Bunlar ilk elden bilgi olarak

kabul edilir ve bu etmenler ihtiyaç duyulduğu zaman dikkate alınır. Bir güven yönetim sistemi, bilginin birçok kaynaktan sağlanması sayesinde daha güçlü olacaktır.

(2) İkinci Elden Bilgi Toplama

Algılama ağları, iş birliği içerisinde çalıştığı düğümlerden meydana gelmektedir. İkinci el bilgi, güven yönetimi için düşünülmelidir. Bir düğüm yerel zekâya sahip olabilir. Bu düğümlerin kendisi, bir dereceye kadar anormal faaliyetleri tespit edebilir ve bunu komşu düğümlerine rapor edebilir. Aynı zamanda bir düğüm bir komşusunun kötü davranışını, bir diğer komşusuna rapor edebilir. Ancak ikinci elden bilgi alındığı zaman ikinci ağız (mouthing) saldırılarına uğrama ihtimali göz ardı edilmemelidir. Kablosuz algılama ağlarında kötü ağız (bad mouthing) saldırıları olduğu zaman, bir düğüm iyi bir düğüm hakkında kötü rapor verebilir veya bir düğüm kötü bir düğüm hakkında iyi rapor verebilir. Bu da güven hesaplama noktasında yanılmamıza sebep olacaktır.

(3) İlk Değerler

Ağdaki düğümlere dağıtım sırasında ilk güven değerleri verilmelidir. İlgili çalışmada, bir ağ yöneticisinin düğümleri yapılandırdığı, test ettiği varsayılmıştır. Bununla birlikte başlangıçta her düğüme eşit güven değeri verilmiştir. Ancak sistem, ağa eklenen düğümlerin dağıtımı sonrasında şüpheli olmalıdır. Burada bir düğüm yeni bir kimlik oluşturarak kötü itibara sahip olabilir ve beyaz temizleme (white-washer) saldırısının bir parçası olabilir.

(4) Tanesellik

Bir kablosuz algılama ağındaki düğümlerin algılama, yönlendirme gibi farklı eylemleri olabilir. Farklı güven değerleri için, bir algılama düğümüne farklı görevler verilmelidir.

(5) Güven Değeri Güncellemesi

Güven yapılandırılması uzun zaman almaktadır. Bir düğümün güven değeri güncellendiği zaman, geçmiş güven değerleri üzerine yazılmamalıdır. Ağın önceki güven değeri unutulmamalıdır ve kaydı tutulmalıdır. Eğer geçmişteki kötü davranışlar unutulursa, ağ açık-kapalı (on-off) saldırılarına karşı savunmasız olacaktır [61].

7.5. Kablosuz Algılama Ağları İçin Geliştirilen Bazı Güven Uygulamaları

Lopez vd. kendi [39] ve diğer çalışmalara dayanarak kablosuz algılama ağlarındaki güven yönetiminin en iyi uygulamalarını tanımlamışlardır [4], [40], [50].

İlk olarak Ganeriwal ve Srivastava algılayıcı ağlar için RFSN (Reputation-based Framework for High Integrity Sensor Networks) güven modelini geliştirmişlerdir [2]. Güven ve itibar değerlerini güncellemek ve belirlemek için istatistiki bir yöntem olan beta dağılımını kullanmışlardır. Güven kavramlarını ise iş birliği olan ve iş birliği olmayan eylemler olarak iki temel sınıfa ayırmışlardır. Düğümler güvenirliği hesaplamada ikinci el bilgileri dolaylı olarak kullanmışlardır. Güvenilir düğümden elden edilen ikinci el bilgilere daha fazla ağırlık verilir. Beklenen itibar değeri düğümlerin güven değerini temsil eder. Eğer güven değeri eşik değerin altından çıkarsa bu düğüm iş birliği yapmayan düğüm olarak belirlenir. Yazarlar çalışmalarında sadece pozitif bildirim aldıkları düğümleri kullanarak gelebilecek saldırıları bertaraf etmeye çalışmışlardır.

Bir algılayıcının yerini belirlemek hayati bir önem taşıdığından bu görevi yapacak DRBTS (Distributed Reputation-based Beacon Trust System) adında bir sistem modellenmiştir [41]. Bu sistem yer bilgisini eksik bildiren düğümler için işaret düğümü kullanır. Her işaret düğümü beklenmeyen bir durum sergileyen düğümler için 1-hop komşu izleme ekranı dağıtılmış ve komşu itibar tablosunda eksik raporlama yapan düğümlerin itibar değerleri tutulup ve güncellenmiştir. Algılayıcı düğümler bilgi aldığı bir düğümün güvenirliğini tartmak için komşu itibar tablosunu kullanır.

Bundan önce yapılan başka bir çalışmada ise hem verilerin hem de veri benzerliği, yol benzerliği, veri çatışması ve veri kesilmesi gibi değişik faktörlere dayalı veri kaynaklarının güven düzeyini tahmin etme fikrine dayalı bir anlayış benimsenmiştir [42]. Dai dört faktöre dayalı güven puanları hesaplamıştır [42] :

- Yol benzerliği
- Veri benzerliği
- Veri çatışması
- Veri kesintisi

Veri benzerliği için iki sayısal değer arasındaki mesafeyi hesaplanmıştır. Bunlar iki kategorik değer arasındaki mesafe ve iki dize (string) arasındaki mesafe değerleridir. Fakat bu teknik, rapor edilen duruma farklı ve birden fazla düğüm tarafından rapor edilmesi durumunda yüksek güvenilirlik atfeder ve gizli saldırıyı fark edemez.

Lim vd. akış verilerinin güven puanlarını kaynağına (provenance) dayalı olarak değerlendirmişlerdir [43],[44]**.** Akış ortamlarının güven hesaplanmasında bilgi kökeninden (provenans) faydalanmaları bizim yaklaşımımızla paralellik göstermektedir. Lim vd. güven değerlerini hesaplamak için fiziksel kökeni kullanmışlardır. Bilgi kökeni verilerini bir veri tabanında saklamış ve merkezi bir şekilde güven değerlendirmesi yapmışlardır. Buna karşın bizim önerdiğimiz modelde ise güven hesaplamaları dağıtık bir şekilde yapılacaktır.

IBM T.J. Watson merkezinde çevrimiçi sağlık analizi için biyomedikal veri akışı sistemine dayalı bir çalışma mevcuttur. Century adı verilen sistemlerinde bir olaya veri ve işlem noktasında destek sağlamak için tanımlanan ve köken (provenans) bilgileri depolayan tıbbi algılayıcılar mevcuttur [45], [46]**.**

Öte yandan TIBFIT tarafından güven endeks tabanlı, hataya dayanıklı bir sistem inşa edilmiştir. Güven endeks değerinin, önceki olay raporlarının aslına uygunluğunu nicel bir ölçü olarak tutmuşlardır [47]. Onların bu yaklaşımı, düğümlerin geçmiş doğruluğunu tutmak anlamında bizim mimarimizle benzerlik göstermektedir. Ancak bizim çalışmamızda, güvenin sadece bir hata oranından ibaret olmadığı fikri üzerine durulmuştur. Ve bizim hata oranımız, itibar ve kaynak vektörlerinde saklanan birçok değer kullanılarak hesaplanan geniş bir metriktir.

Bayes ağı [19], [48] ve oyun teorisi [18] teknikleri de, ağlarda güven oluşturmak için kullanılabilir. Bizim sistemimizde ise güven değerlendirmesi için köken bilgisinden destek alan, dizin tabanlı güven modeli kullanılmıştır. Bu bağlamda bizim modelimizin yukarıdaki modellerden farklıdır.

Algılayıcı ağların en önemli güvenlik açığı, küme başlarının kötü olma ihtimalidir. Crosby vd. [49] güvenilir küme başlarının seçimi

için dağıtık güven tabanlı bir araç önermişlerdir. Bu yaklaşımda, güvenilir düğümlerden gelen doğrudan ve dolaylı bilgileri kullanmışlardır. Güven, paket düşürme oranı, veri paketleri ve kontrol paketlerinin ağırlıklı hesaplanmasına göre ölçülür. Bununla beraber her bir düğüm, kendi etrafındaki düğümlerin güven tablosunu tutup bunu istek üzerine küme başına raporlar.

Hur vd. algılayıcı verilerinin güvenilirliğini ölçmek ve kötü düğümlerden gelen bilgiyi silmek için bir güven modeli önermişlerdir [50]. Geliştirilen bu model bizim çalışmamızla benzerlik göstermektedir**.** Fakat onların önerdikleri model geçmiş verileri kullanmaz. Her bir düğüm komşusunun güvenirliğini, komşusunun gereksiz bilgi verilerini kendi sonuçlarıyla karşılaştırarak değerlendirir. Kötü düğümlerden gelen bilgi göz ardı edilerek daha kesin sonuçlar elde edilir.

Chen vd. [21] olasılık, istatistik ve matematik analizden araçlar kullanan itibar tabanlı bir güven modeli önerirler. Kablosuz algılayıcı ağlarında bir güven alanı ve itibar alanı oluştururlar ve itibar alanından güven alanına bir dönüşüm tanımlarlar. Son olarak kablosuz algılayıcı ağlarındaki önemli özellikleri ele alırlar ve kablosuz algılayıcı ağlarındaki itibar sistemleriyle alakalı açık problemlere dikkat çekerler.

Xiao vd. SensorRank adı verilen sistemlerinde güven oylaması (Trust Voting) algoritmasını kullanırlar. Algılayıcı düğümler, okudukları verilerin doğru olup olmadığını doğrulamak için komşularına danışırlar [51]. Hatalı düğümler Voting algoritmasına dâhil olmazlar.

Tanachaiwiwat vd. algılayıcı ağları için bir güven yönlendirme modeli (TRANS) geliştirmişlerdir [52]. Modellerinde, düğümler komşularına inceleme mesajları gönderir ve ACK mesajları beklerler. Mesajı istenmeyen yere yönlendiren veya mesajın ulaşmasını engelleyen düğümler baş düğüm tarafından kara listeye alınırlar. Mesaj akışı baş düğüm aracılığıyla yapılır.

Beta itibar sistemini kullanan modellerden birisi de Srinivasan vd. [53] tasarladığı CDS tabanlı itibar izleme sistemidir. Düğümler diğer düğümlerden direk olarak bilgi elde eder ve beta dağıtım parametrelerinin değişken gruplarını depolar.

Momani vd. [54] kablosuz algılayıcı ağları için Gauss itibar sistemini geliştirmişlerdir. Her düğümün rapor edilen verisi komşu düğümler tarafından değerlendirilir. Momani vd. direk olarak gözlenen bilgiyle, komşu düğümlerden elde edilen bilgileri füzyon etmek için Bayes' in olasılıksal yaklaşımını kullanmışlardır.

GTMS [55], Shaikh vd. tarafından geliştirilen grup tabanlı güven yönetim modelidir. Shaikh vd. bu çalışmada merkezi ve dağıtık yaklaşımları bir araya getirmişlerdir. Bu çalışmanın bizim yaklaşımımızla birçok benzerlik gösterdiği gözlemlenmiştir. Fakat bu model kötü düğümler tarafından bildirilen hatalı bilgiyi dikkate almaz. Her grubun, baz istasyonundaki küçük bir veri tabanında tutulan bir güven değeri vardır.

ATRM'de [56] düğümler güven ve itibar bilgilerini yerel olarak depolarlar [41]. Ağ modeli kümelenmiş kablosuz algılama ağına dayanmaktadır.

Güven ihmal düğümleri, kümeleri birleştirme ve düğümleri ekleme gibi kablosuz algılama ağlarının yeniden inşa edilmesinde kullanılır. Kablosuz algılama ağları, düğümlerin güveni ve işbirliği yapısı özelliğini temel aldığı için güvenin kurulması bir zorunluluktur. Kablosuz algılama ağlarının sınırlı kaynaklara sahip olması nedeniyle, bu ağlarda geleneksel şifreleme yaklaşımlarını kullanmak mümkün değildir [59],[60]. Bu yüzden kablosuz algılama ağları için farklı güven mekanizmaları gereklidir. Kablosuz algılama ağlarında güven hala açık ve zorlu bir alandır.

Kablosuz algılama ağlarında geliştirilen diğer güven uygulamaları için bu çalışmaya da bakılabilir [58].

7.5. Değerlendirmeler

Sonuç olarak siber güvenlikte güven kavramı önem verilmesi gereken yeni gelişmekte olan bir konudur. Geliştirilen sistemler güven değerleri oluşturup onları güncelleyecek bir yapıda olurlarsa kullanıcılarla daha etkili bir iletişim olacaktır. Bilim-kurgu filmlerinde olan insanların da puanlandığı, bir numerik güven değeri verildiği sistemler aslında yakın gelecekte gerçekleşebilecek senaryolardır. Sistemler geçmiş bilgileri ve davranışları kaydederek sürekli güncellenen bir güven sistemi ile oluşturulursa insanların o sistemleri

kullanmaları daha uzun süreli ve etkili olacaktır. Her alanın güven hesaplama ve güncelleme sistemi o alanın özelliklerine göre farklı olacaktır. Fakat yukarıdaki bölümlerde bahsedildiği gibi sayısal olarak ifade edilen ve güncellenen bir güven değeri olacaktır.

Endüstri 4.0 ve Nesnelerin interneti ile birçok yeni uygulama alanı bulan kablosuz algılayıcı ağlarının güvenli olması çok önemlidir. Aksi takdirde kablosuz algılayıcı ağdan gelen verilerle yapılacak yanlış kararlar ve yönlendirmeler önemli sorunlar teşkil edebilir. Kablosuz algılayıcı ağlar düşman gözetleme sistemleri, yangın kontrol sistemleri gibi çok hayati alanlarda kullanılmaktadır. Diğer güvenlik konularına ek olarak güven (trust) konusunda da ülkemizde çalışmalar yapılması, konunun farklı boyutlarıyla ele alınması, bu konuda tezler üretilmesi, ulusal özgün ürün ve teknolojilerin geliştirilmesi, bu konu gerekli yatırımların yapılmasının ülke siber savunması ve güvenliğine büyük katkı sağlayacağı değerlendirilmektedir.

Kaynaklar

[1] TDK Sözlüğü, Güven, http://www.tdk.gov.tr/index.php?option=com_gts&kelime=GÜVEN (Erişim: 11 Şubat 2019).

[2] Ganeriwal, S. Balzano, L.K. ve Srivastava, M.B., (2008). "Reputation-based framework for high integrity sensor networks", ACM Transactions on Sensor Networks (TOSN), 4: 15.

[3] Yao, Z., Kim, D., Lee, I., Kim, K., & Jang, J. (2005). A security framework with trust management for sensor networks. In *Security and Privacy for Emerging Areas in Communication Networks, 2005. Workshop of the 1st International Conference on* (pp. 190-198). IEEE.

[4] Fernández-Gago, M. C., Román, R., & Lopez, J. (2007). A survey on the applicability of trust management systems for wireless sensor networks. In *Third International Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing (SecPerU 2007)* (pp. 25-30). IEEE.

[5] Josang, A., & Presti, S. L. (2004, March). Analysing the relationship between risk and trust. In *International Conference on Trust Management* (pp. 135-145). Springer, Berlin, Heidelberg.

[6] Gambetta, Diego (2000) 'Can We Trust Trust?', in Gambetta, Diego (ed.) *Trust: Making and Breaking Cooperative Relations*, electronic edition, Department of Sociology, University of Oxford, chapter 13, pp.

213-237, <http://www.sociology.ox.ac.uk/papers/ gambetta213-237.pdf>.

[7] Solhaug, B., Elgesem, D., & Stolen, K. (2007). Why trust is not proportional to risk. In *Availability, Reliability and Security, 2007. ARES 2007. The Second International Conference on* (pp. 11-18). IEEE.

[8] Cho, J.-H. Swami, A. ve Chen, R., (2011). "A survey on trust management for mobile ad hoc networks", Communications Surveys & Tutorials, IEEE, 13: 562-583.

[9] Abdul-Rahman, A., & Hailes, S. (1997). S.: Using Recommendations for Managing Trust in Distributed Systems. In *Proceedings of the IEEE Malaysia International Conference on Communication.*

[10] Bhargava, B. Lilien, L. Rosenthal, A. Winslett, M. Sloman, M. Dillon, T. Chang, E. Hussain, F. Nejdl, W. ve Olmedilla, D., (2004). "The pudding of trust [intelligent systems]", Intelligent Systems, IEEE, 19: 74-88.

[11] Scott, J., (2012). Social network analysis: Sage.

[12] Ries, S., Kangasharju, J., & Mühlhäuser, M. (2006). A classification of trust systems. In *OTM Confederated International Conferences" On the Move to Meaningful Internet Systems"* (pp. 894-903). Springer, Berlin, Heidelberg.

[13] Resnick, P. ve Zeckhauser, R., (2002). "Trust among strangers in internet transactions: Empirical analysis of ebay's reputation system", The Economics of the Internet and E-commerce, 11: 23-25.

[14] Blaze, M., Feigenbaum, J., & Keromytis, A. D. (1998). KeyNote: Trust management for public-key infrastructures. In *International Workshop on Security Protocols* (pp. 59-63). Springer, Berlin, Heidelberg.

[15] Blaze, M., Feigenbaum, J., & Lacy, J. (1996). Decentralized trust management. *IEEE Symposium on Security and Privacy* (pp. 164-173).

[16] Abdul-Rahman, A., & Hailes, S. (2000). Supporting trust in virtual communities. *Proceedings of the 33rd IEEE Annual Hawaii International Conference on System Sciences* (pp. 9-pp).

[17] Josang, A., & Ismail, R. (2002, June). The beta reputation system. In *Proceedings of the 15th bled electronic commerce conference* (Vol. 5, pp. 2502-2511).

[18] Xiong, L., & Liu, L. (2003). A reputation-based trust model for peer-to-peer ecommerce communities. In *Proceedings of the 4th ACM conference on Electronic commerce* (pp. 228-229).

[19] Wang, Y., & Vassileva, J. (2003). Bayesian network-based trust model. *IEEE/WIC International Conference on Web Intelligence* (pp. 372-378).

[20] Aberer, K., & Despotovic, Z. (2001). Managing trust in a peer-2-peer information system. In *Proceedings of the tenth ACM international conference on Information and knowledge management* (pp. 310-317).

[21] Cahill, V., Gray, E., Seigneur, J. M., Jensen, C. D., Chen, Y., Shand, B., ... & Wagealla, W. (2003). Using trust for secure collaboration in uncertain environments. *IEEE pervasive computing*, *2*(3), 52-61.

[22] Kinateder, M. Baschny, E. ve Rothermel, K., (2005). Towards a generic trust model–comparison of various trust update algorithms, ed. Trust Management. Springer, 177-192.

[23] Kotsovinos, E., & Williams, A. (2006). BambooTrust: Practical scalable trust management for global public computing. In *Proceedings of the 2006 ACM symposium on Applied computing* (pp. 1893-1897). ACM.

[24] Quercia, D. Hailes, S. ve Capra, L., (2006). B-trust: Bayesian trust framework for pervasive computing, ed. Trust Management. Springer, 298-312.

[25] Zhou, D., (2003). "Security issues in ad hoc networks": CRC Press, Inc.

[26] Buchegger, S., & Le Boudec, J. Y. (2002). Performance analysis of the CONFIDANT protocol. In *Proceedings of the 3rd ACM international symposium on Mobile ad hoc networking & computing* (pp. 226-236). ACM.

[27] Michiardi, P. ve Molva, R., (2002). Core: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks, ed. Advanced Communications and Multimedia Security. Springer, 107-121.

[28] Aivaloglou, E. Gritzalis, S. ve Skianis, C., (2008). "Trust establishment in sensor networks: behaviour-based, certificate-based and a combinational approach", International Journal of System of Systems Engineering, 1: 128-148.

[29] Wang, Y. Attebury, G. ve Ramamurthy, B., (2006). "A survey of security issues in wireless sensor networks".

[30] Papadimitratos, P. ve Haas, Z.J., (2002). "Securing mobile ad hoc networks", Handbook of Ad Hoc Wireless Networks: 665-671.

[31] Walters, J.P. Liang, Z. Shi, W. ve Chaudhary, V., (2007). "Wireless sensor network security: A survey", Security in distributed, grid, mobile, and pervasive computing, 1: 367.

[32] Newsome, J., Shi, E., Song, D., & Perrig, A. (2004). The sybil attack in sensor networks: analysis & defenses. In *Proceedings of the 3rd international symposium on Information processing in sensor networks* (pp. 259-268). ACM.

[33] Perrig, A., Stankovic, J., & Wagner, D. (2004). Security in wireless sensor networks. *Communications of the ACM*, *47*(6), 53-57.

[34] McKnight, D.H. ve Chervany, N.L., (1996). "The meanings of trust".

[35] Rothstein, B., (2000). "Trust, social dilemmas and collective memories", Journal of Theoretical Politics, 12(4): 477-501.

[36] Deelmann, T. ve Loos, P., (2002). "Trust economy: aspects of reputation and trust building for SMEs in e-business", AMCIS 2002 Proceedings: 302.

[37] Pirzada, A. A., & McDonald, C. (2004, January). Establishing trust in pure ad-hoc networks. In *Proceedings of the 27th Australasian conference on Computer science-Volume 26* (pp. 47-54). Australian Computer Society

[38] Lopez, J. Roman, R. Agudo, I. ve Fernandez-Gago, C., (2010). "Trust management systems for wireless sensor networks: Best practices", Computer Communications, 33: 1086-1093.

[39] Josang, A. Gray, E. ve Kinateder, M., (2006). "Simplification and analysis of transitive trust networks", Web Intelligence and Agent Systems, 4: 139-161.

[40] Josang, A. Ismail, R. ve Boyd, C., (2007). "A survey of trust and reputation systems for online service provision", Decision support systems, 43: 618-644.

[41] Srinivasan, A., Teitelbaum, J., & Wu, J. (2006, September). DRBTS: distributed reputation-based beacon trust system. *2nd IEEE International Symposium on Dependable, Autonomic and Secure Computing* (pp. 277-283).

[42] Dai, C., Lin, D., Bertino, E., & Kantarcioglu, M. (2008). Trust evaluation of data provenance. *Center for Education and Research Information Assurance and Security*.

[43] Lim, H. S., Moon, Y. S., & Bertino, E. (2009). Research issues in data provenance for streaming environments. In *Proceedings of the 2nd SIGSPATIAL ACM GIS 2009 International Workshop on Security and Privacy in GIS and LBS* (pp. 58-62). ACM.

[44] Lim, H.-S. Moon, Y.-S. ve Bertino, E., (2010). Assessing the trustworthiness of streaming data, Technical Report TR 2010-09, CERIAS.

[45] Misra, A. Blount, M. Kementsietsidis, A. Sow, D. ve Wang, M., (2008). Advances and challenges for scalable provenance in stream processing systems, ed. Provenance and Annotation of Data and Processes. Springer, 253-265.

[46] Blount, M., Davis, J., Ebling, M., Kim, J. H., Kim, K. H., Lee, K., ... & Wang, M. (2007). Century: Automated aspects of patient care. In *13th IEEE International Conference on Embedded and Real-Time Computing Systems and Applications, 2007. RTCSA 2007.* (pp. 504-509). IEEE.

[47] Krasniewski, M., Varadharajan, P., Rabeler, B., Bagchi, S., & Hu, Y. C. (2005). Tibfit: Trust index based fault tolerance for arbitrary data faults in sensor networks. In *Dependable Systems and Networks, 2005. DSN 2005. Proceedings. International Conference on* (pp. 672-681). IEEE.

[48] Wang, Y., & Vassileva, J. (2003). Trust and reputation model in peer-to-peer networks. In IEEE International Conference on Peer-to-Peer Computing (p. 150).

[49] N. Pissinou, G. V. Crosby and J. Gadze, "A Framework for Trust-based Cluster Head Election in Wireless Sensor Networks," *DSSNS 2006. Second IEEE Workshop on Dependability and Security in Sensor Networks and Systems(DSSNS)*, Columbia, MD, 2006, pp. 13-22.

[50] Hur, J., Lee, Y., Youn, H., Choi, D., & Jin, S. (2005). Trust evaluation model for wireless sensor networks. The 7th IEEE International Conference on Advanced Communication Technology (Vol. 1, pp. 491-496).

[51] Xiao, X. Y., Peng, W. C., Hung, C. C., & Lee, W. C. (2007). Using sensorranks for in-network detection of faulty readings in wireless sensor networks. In *Proceedings of the 6th ACM international workshop on Data engineering for wireless and mobile access* (pp. 1-8). ACM.

[52] Tanachaiwiwat, S., Dave, P., Bhindwale, R., & Helmy, A. (2004). Location-centric isolation of misbehavior and trust routing in energy-constrained sensor networks. In *Performance, Computing, and Communications, 2004 IEEE International Conference on* (pp. 463-469). IEEE.

[53] Srinivasan, A., Li, F., & Wu, J. (2008). A novel CDS-based reputation monitoring system for wireless sensor networks. In *28th IEEE International Conference on Distributed Computing Systems Workshops* (pp. 364-369).

[54] Momani, M., Aboura, K., & Challa, S. (2007). RBATMWSN: recursive Bayesian approach to trust management in wireless sensor networks. *ISSNIP 3rd* IEEE *International Conference on Intelligent Sensors, Sensor*

Networks and Information (pp. 347-352). YANLI;LIKLA 56 DA OLACAK

[55] Shaikh, R. A., Jameel, H., Lee, S., Rajput, S., & Song, Y. J. (2006). Trust management problem in distributed wireless sensor networks. In *Embedded and Real-Time Computing Systems and Applications, 2006. Proceedings. 12th IEEE International Conference on* (pp. 411-414). IEEE.

[56] Boukerch, A. Xu, L. ve El-Khatib, K., (2007). "Trust-based security for wireless ad hoc and sensor networks", Computer Communications, 30: 2413-2427.

[57] Eschenauer, L., Gligor, V. D., & Baras, J. (2002). On trust establishment in mobile ad-hoc networks. In *International Workshop on Security Protocols* (pp. 47-66). Springer, Berlin, Heidelberg.

[58] Han, G. Jiang, J. Shu, L. Niu, J. ve Chao, H.-C., (2014). "Management and applications of trust in Wireless Sensor Networks: A survey", Journal of Computer and System Sciences, 80: 602-617.

[59] Ozdemir, S., (2008). "Functional reputation based reliable data aggregation and transmission for wireless sensor networks", Computer Communications, 31: 3941-3953.

[60] Dogan, G. (2016a). Protru: a provenance-based trust architecture for wireless sensor networks. Wiley International Journal of Network Management, 26 (2), 131–151. doi: 10.1002/nem.1925

[61] Etzioni, A. (2017). Cyber trust. Journal of Business Ethics, 1-13.

[62] de Oliveira Albuquerque, R., Villalba, L. J. G., Orozco, A. L. S., de Sousa Júnior, R. T., & Kim, T. H. (2016). Leveraging information security and computational trust for cybersecurity. The Journal of Supercomputing, 72(10), 3729-3763.

Fidye Yazılımlar

BÖLÜM 8

A. Nurdan SARAN

FİDYE YAZILIMLAR

8.1. Giriş

Kötü amaçlı yazılımlar, bilgisayarlara, mobil aygıtlara, bilgisayar ağlarına, çalıştırdıkları yazılımlara veya kullanıcıların verilerine zarar vermek için özel olarak tasarlanmış yazılımlar olarak tanımlanabilir. Zararlı davranışlar sergileyen kötü amaçlı yazılımlar siber suçlar içinde en yaygın saldırı yöntemlerinin başında gelmektedir ve çeşitli türleri vardır. Bunlardan birkaçı virüsler, solucanlar, trojanlar, casus yazılımlar ve fidye yazılımlardır. Tüm kullanıcıların farklı biçimlerdeki kötü amaçlı yazılımları nasıl tanıyacaklarını ve kendilerini nasıl koruyacaklarını bilmeleri önemlidir. Bu bölümde bir kötü amaçlı yazılım türü olan fidye yazılım (İng: Ransomware) konusu incelenecektir. Fidye yazılımlar aracılığıyla genellikle mağdurların özel bilgilerini veya kritik verilerini kaybetme veya geri dönüşü olmayan donanım hasarları ile karşılaşma tehdidi ile saldırılar gerçekleştirilmektedir. Fidye yazılımlar, son yılların en yaygın ve en zararlı kötü amaçlı yazılım türlerinden biridir. Kriptografik fidye yazılımlar, en yaygın türü olmakla beraber kriptografik olmayan fidye yazılımlarda vardır. Aslında fidye yazılım saldırıları, kötü amaçlı yazılım olmaktan çok bir tür suç iş modelidir. Scareware (İng.) de denilen bu modelde korkutma taktikleri kullanarak kötü amaçlı yazılım veya benzeri bir davranış biçimi ile kazanç elde edilmesi hedeflenmektedir. Genel olarak, mağdurun bilgisayarı veya mobil cihazını kilitleyen veya elektronik dosyalarını şifreleyen bir kötü amaçlı yazılım (Truva veya başka bir virüs türü) bulaştırılıp, verilere erişiminin yeniden sağlanması içinse mağdurdan fidye ödenmesi talep edilir. Burada kötü amaçlı yazılım, fidye için değerli bir varlık yaratmak için kullanılır ve bu nedenle fidye yazılım olarak adlandırılır. Fidye saldırıları genellik-

le e-posta (örn. eklenti dosyalarla veya e-posta içerisinde bulunan linkler), kaynağı belirsiz programlar, taşınabilir aygıtlar, korsan DVD/CD ler, forum siteleri ve korsan oyunlar aracılığıyla gerçekleştirilmektedir. Bir fidye yazılımı ile bir sistem enfekte olduktan sonra, kullanıcının verilerini geri alması veya bilgisayarını yeniden etkinleştirmesi için gerekli şifre çözme anahtarını sağlamak için fidye ödenmesini isteyen açılır pencereler gönderilmektedir. Veriyi şifre çözme anahtarı olmadan kurtarmak çok zordur. Genellikle 300-600 Amerikan Doları civarında olan bu fidyenin BitCoin olarak, 72 saat içerisinde ödenmesi talep edilmektedir. Ödenmediği takdirde şifreleme anahtarının silineceği ve verinin geri dönüşünün mümkün olmadığı tehdidiyle fidye talebi yapılmaktadır. Ödeme, iTunes, Amazon hediye kartları ya da TOR gibi gizlilik sağlayan hizmetler ile BitCoin olarak talep edilebilmektedir. Bahsedilen bu yöntemlerin talep edilmesinin nedeni ise gönderdiğiniz kişinin kimliğinin tespit edilememesini ve ödemenin anonim kalmasını sağlamaktır. Kullanıcı verilerinin şifrelendiği bu tür yazılımlar bu işlemi birkaç dakika içinde (70 MB veriyi 18 saniye ile 16 dakika arasında [1] yapabilmekte ve dosyaları orjinaline geri dönülmesi imkânsız şekilde kullanıcı bilgisayarından temizleyebilmektedir. Son zamanlarda, kötü amaçlı yazılımları tarayan anti virüs yazılımları tarafından fark edilmeden hareket edebilmek amacıyla, dosya içermeyen (İng: fileless) fidye yazılımlar, veri yükünü belleğe veya çekirdeğe (İng: Powershell) saklayarak tespit edilmekten kurtulabilmektedir.

Bilinen ilk kötü amaçlı fidye yazılım saldırısı, 1989 yılında yazılan "AIDS Truva atı" adlı yazılım ile gerçekleştirilmiştir. Sabit sürücüdeki dosyaları gizleyerek yalnızca dosya isimlerinin şifrelendiği bu yazılım ile "PC Cyborg Corporation"a 189 Amerikan Doları ödeme yapılması istenmiştir [2]. Fidye yazılım saldırılarının sayısı, 2013 yılında büyük bir artış göstermiştir. 2018 yılında da bir önceki yıla göre fidye yazılım saldırısı sayısı %500 artmıştır [3]. Örneğin, 2013 itibarıyla tüm dünyada birçok bilgisayarı etkisi altına almayı başaran Cryptolocker fidye yazılımının 200.000 ile 250.000 bilgisayarı etkisi altına aldığı tahmin edilmektedir [4]. Bu zararlı yazılım Türkiye'de genellikle e-fatura bilgisi gibi gelen bir sahte e-posta ile yayılmaktadır ve bu tür saldırılar oltalama (İng: phishing) yöntemi olarakta adlandırılmaktadır. Fatura tutarını oldukça yüksek gös-

tererek kullanıcının dikkatini çekmekte ve kullanıcıyı gönderdiği e-postadaki linke (örneğin "http://efatura.ttnet-fatura.com/") tıklamaya yönlendirilmekte, linkten e-faturanın "zip" uzantılı bir dosya halinde indirilmesi sağlanmaktadır. Kullanıcı, "zip" uzantılı dosyayı açıp içindeki e-fatura dosyasına ("exe" uzantılı) tıkladığında ise kullanıcının tüm dokümanları güçlü şifreleme algoritmaları ile şifrelenmektedir. 2015 yılı Telefonica Trend Raporuna [5] göre Türkçe TOR platformunda üçüncü en çok kullanılan dildir. TOR kullanıcıların anonim olarak İnternet'te gezinmelirini sağlayan, açık kaynak kodlu bir ağ ve yazılım projesidir. TOR platformundaki Türkçe'nin bu denli yaygın olması Türkiye'nin zararlı yazılım konusunda çok sayıda anonim kullanıcılardan gelebilecek tehlikelere karşı dikkatli olması gerektiğini göstermektedir.

Bugüne kadar birçok kuruluş istenen fidyeleri ödemek zorunda kalmıştır, çünkü talep edilen fidyeyi ödemenin diğer birçok çözümden daha ucuz bir çözüm olduğu görülmüştür. Saldırganlar fidye ödemesinin gecikmesi durumunda fidye miktarını arttırmakla da tehdit edebilmektedirler. 2016 yılının ilk çeyreğinde, fidye yazılım kullanan siber suçlara ödenen miktarın 209 milyon dolar olduğu tahmin edilmektedir [6].

2017 yılında, bir hizmet olarak fidye yazılımı (ing: Ransomware as a Service (RaaS)) kavramı ile tanıştık. Karanlık Web'de (Dark Web) satılan fidye yazılım dağıtım kitleri ile çok az teknik beceriye sahip kişilerin göreceli kolaylıkla fidye saldırısı düzenlemesine olanak sağlayan bu model, ciddi bir siber güvenlik problemi olarak karşımıza çıkmıştır. Bu kitlerin bir kısmı Bitcoin ile satılırken bir kısmı da mağdurdan alınacak paranın belirli bir yüzdesi şeklinde fiyatlandırılmaktadır (örneğin kazanılacak paranın %30'u). Ülkelerin siber güvenlik ile ilgili birimlerinin özellikle bu tür servislere karşı gerekli önlemleri alması çok önemlidir.

8.2. Fidye Yazılım Saldırısının İşleyiş Aşamaları

Fidye yazılım saldırıları genellikle mağdurun dikkatsizliği ile indirdiği veya açtığı meşru bir dosya olarak gizlenmiş bir Truva atı kullanılarak gerçekleştirilir. Ancak, bu yöntemin istisnaları da vardır. Örneğin, "WannaCry" veya "WannaCryptor" olarak bilinen solu-

can, Windows işletim sistemindeki smb servisindeki açıktan faydalanarak kullanıcı etkileşimi olmadan bilgisayarlar arasında hızla yayılmayı başarmıştır. 10 Mayıs 2017 tarihinden itibaren 75.000'den fazla kuruma saldırıda bulunulmuştur[1].

Bir fidye yazılımı saldırısının 5 farklı aşaması vardır [7].

1. Sömürü ve Enfeksiyon (0. zaman): Saldırının başarılı olması için, kötü amaçlı fidye yazılımı dosyasının bir bilgisayarda çalışması gerekir. Bu genellikle bir oltalama e-postası veya istismar (exploit) kiti ile yapılır.
2. Yerleştirme ve Yürütme (0-5 dakika): Bu aşamada, gerçek fidye yazılımı çalıştırılır. Kurbanın sistemine exe uzantılı dosya yerleştirilir ve çalıştırılır.
3. Yedeklemeyi Engelleme (5-10 dakika arası): Fidye yazılımı, kurbanın sistemindeki yedek dosyalarını (ing:backup) ve klasörlerini hedefler ve geri yüklemeyi önlemek için bunları siler.
4. Dosya Şifreleme (~2 Saat): Sistemde kullanılacak şifreleme anahtarları oluşturulur ve dosyalar şifrelenir.
5. Kullanıcı Bildirimi ve Temizleme (~15 saat): Orjinal dosyalar geri dönüşümü mümkün olmayacak şekilde şifrelenip temizlendikten sonra kullanıcıya ödeme talebi içiren bir bilgilendirme penceresi gösterilir. Sıklıkla, kurbana ödeme için birkaç gün verilir, gecikme durumunda talep edilen ücretin artırılacağı bilgisi verilir.

8.3. Fidye Yazılımlarının Evrimi

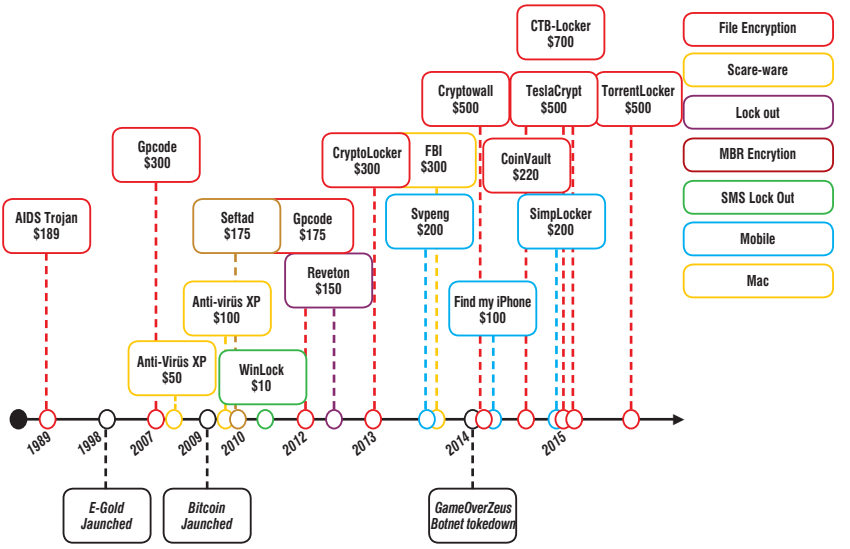
Bilinen ilk fidye yazılımı 1989 yılında ortaya çıkan AIDS olarak adlandırılan zararlı yazılımdır. Şekil 8.1'de, bilinen bu ilk fidye yazılımdan başlamak üzere tarihsel sıra düzeninde zararlı etkileri öne çıkan belli başlı fidye yazılımları.

8.3.1. AIDS (1989)

Bilinen ilk fidye yazılımı, Dr. Joseph Popp adında AIDS araştırmalarına aktif olarak katılan bir biyolog tarafından AIDS Truva'sını

[1] https://www.rt.com/news/388153-thousands-ransomeware-attacks-worldwide/

içeren 20.000 disket ile 90'dan fazla ülkeye hayali bir firma olan "PC Cyborg Corporation" tarafından dağıtılmıştır. Bu yazılım DOS işletim sistemine sahip bilgisayarları etkilemiştir. Bugüne kadar, Popp'in motivasyonu açıklanamamıştır. Autoexec.bat komut dosyasını kötü niyetli komutlarla kullanan trojan, 90. önyükleme de mağdurun fidye ekranı ile karşılaştığı ilk yazılımdır. Havale ile Panama da bir hesaba 189 Doları gönderilmesi talebi ile şifre çözme anahtarını göndereceğini vadeder. Ancak bu ilk yazılımda dosya sisteminin kendisi şifrelenmemiştir. Sadece dosya isimleri ve dizin isimleri simetrik şifreleme ile şifrelenmiş ve bu simetrik anahtar mağdurun bilgisayarında da saklanmıştır [8].



Şekil 8.1. Fidye Yazılımların Evrimi [5].

8.3.2. GPCode

GPCode, Windows işletim sistemi üzerindeki dosyalara erişimi engellemek için PGP şifreleme yöntemini kullandığını iddia eden ve 100 ile 200 Amerikan Doları karşılığı E-Gold veya Liberty Reserve dijital para birimleri talep eden kötü amaçlı bir yazılımdır. Ancak, yapılan analizlerde yazılımın tek bir saldırgan tarafından geliştirildiği ve inanılmaz derecede zayıf olduğu ortaya çıkarılmıştır. Bununla birlikte, takip eden beş yıl boyunca GPCode geliştirilmeye devam edildi, şifrelenmiş dosyaları yeni bir konuma yazıp orijinalleri silindi, algoritma olarak 3DES, RSA ve AES kullanıldı ve veri kur-

tarmayı engellemek için şifrelenmiş dosyalar fiziksel olarak varolan dosyaların üzerine yazıldı. Bu zararlı yazılımda her enfeksiyon için yeni bir simetrik anahtar oluşturulmakta ve bu anahtarların gömülmesi içinde ancak saldırganın özel anahtarı ile şifresini çözebildiği, gömülü bir RSA ortak anahtarı kullanılmaktadır. GPCode örneği, zararlı yazılım geliştiricilerinin de kendilerini sürekli geliştirdiklerini ve yazılımlarını zamanla oldukça karmaşık hale getirdiklerini göstermektedir.

8.3.3. Reveton (2012)

Reveton ailesi ile başlayan kilitleme (ing:locker) fidye yazılım çeşidi, mağdurun işletim sistemine erişimini engelleyen ve kilitleyen bir yapı ile karşımıza çıkmıştır. Windows işletim sistemine sahip bilgisayarları etkileyen bu fidye yazılımı, mağdurun cihazının yasadışı bir faaliyet (korsan müzik, film veya yazılım gibi) için kullanıldığının iddia edilmesi ile başlar ve mağdurdan bu durumun düzeltilmesi için fidye istenir. Kilitli cihazlar genellikle yalnızca kullanıcının bilgisayar arayüzü ile sınırlı yeteneklerle etkileşimde bulunmasına izin verir (örneğin ödemeyi yapabilmek için rakamlar yazmasına izin verilmesi, fareye erişimin devre dışı bırakılması gibi). Büyük ölçüde temel sistem özelliklerine ve verilere zarar vermez. Tabi bu tipteki fidye yazılımlar üzerinde çalıştıkları işletim sisteminin özelliklerini ve API'lerini kullanırlar.

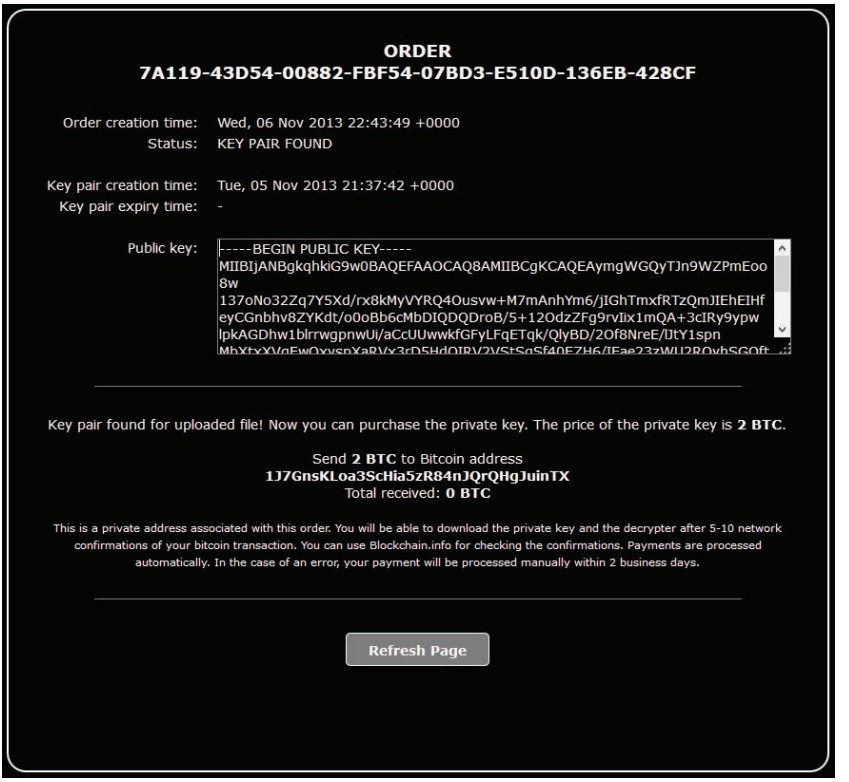
8.3.4. Cryptolocker (2013)

CryptoLocker'ın ilk sürümleri, ev İnternet kullanıcılarını değil, iş profesyonellerini hedef alan spam e-postaları aracılığıyla dağıtılmıştır. Yem olarak, genellikle kuruluşlara karşı "tüketici şikayeti" şeklinde bir spam e-posta kullanılmıştır. 13 ile 17 karakter içeren rastgele bir alfabetik dosya adı bulunan bir ZIP arşivi bu e-postalara eklenmiş olarak gelmektedir. ZIP arşiviyle aynı dosya adında ancak bir EXE uzantısı ile tek bir yürütülebilir dosya içermektedir. Açık anahtarını (public key) komut ve kontrol sunucusundan (ing: command and control server, C&C) indirdiğinden sunucuya başarıyla ulaşıp dosyaları şifreleyene kadar varlığını kurbanlardan gizleyen bir Truva atıdır. Bu nedenle, virüs bulaşmış sistemlerde komut ve kontrol sunucusuna http protokolü ile bağlanana kadar sistemin çalışmasını ve yeniden başlatmalara devam etmesine olanak sağlar.

Ağ iletişimi için ilk versiyonları statik IP adresi kullanırken sonraki versiyonları günde 1000 potansiyel komut ve kontrol sunucusu alan adı adresi üreten bir dahili etki alanı oluşturma algoritması (ing: domain generation algorithm, DGA) kullanmaktadır [4]. (Alan adları 12 ila 15 alfabetik karakter içerir ve olası en üst düzey alanlardan birini içerir: com, net, org, info, biz, ru veya co.uk). CryptoLocker içine gömülü bir RSA açık anahtarıyla şifrelenmiş bir mesajı bu sunucuya gönderir, yalnızca ilgili RSA özel anahtarına sahip sunucular bu mesajı çözebilir ve virüslü bir sistemle başarılı bir şekilde iletişim kurabilir. CryptoLocker, Microsoftun tarafından sunulan, CryptoAPI üçüncü taraf sertifikalı güçlü bir şifreleme kullanır. GetLogicalDrives() komutu ile sistemdeki diskler tespit edildikten sonra GetDriveType() komutu ile yerel mi yoksa ağ diskleri mi olduğuna bakılır, taşınabilir diskler dahil tüm disklerde tüm dosyalar farklı AES anahtarları ile şifrelenir. Buna ek olarak, AES anahtarları da komut ve kontrol sunucusundan gelen açık anahtar ile şifrelenir. Şifrelenmiş dosyalar orjinallerinin üzerine yazılır. Mağdura Şekil 8.2'deki gibi bir fidye talebi isteği gönderilir.

Şekil 8.2. Cryptolocker Uyarı Ekranı

Dosyaları geri almak için ise mağdura Şekil 8.3'deki gibi bir ödeme bilgisi ekranı gösterilmektedir.



Şekil 8.3. Ödeme Bilgisi Ekran Görüntüsü (Kaynak: Dell SecureWorks).

8.3.5. Kovter (2013)

Windows işletim sistemi kullanan bilgisayarlara yönelik olarak geliştirilmiş olan bu fidye saldırısı yazılımı dosyasız enjeksiyon yöntemini kullanır. Diğer bir ifadeyle, etkilenen cihazın yerel disklerinde indirilmiş dosyaları yürütmeyi gerektirmez. Bunun yerine, sistemin belleğinde yürütülür veya kalıcılık için sistemin kayıt defterinde tutulur. Varolan bir uygulama/yazılımın belleğine veya PowerShell gibi bir uygulama içinde komutlar çalıştırarak veri yükleri enjekte edilebilir. Windows PowerShell -komut satırı kabuğu- kullanıcıların işletim sistemi hizmetlerine erişmesini sağlayan bir arabirim ve komut dosyaları oluşturmak için çerçevesine dayanan bir programlama dili içeren yerleşik bir araçtır. Sistemdeki tüm USB aygıtlarını,

sürücüleri ve hizmetleri görüntüleme, bir dizi komut zamanlama ve arka planda ayarlama veya işlemleri sonlandırma gibi sistem yönetimi görevlerini otomatikleştirmek için tasarlanmıştır. PowerShell ayrıca, yöneticilerin sistem ve sunucu konfigürasyonlarını, aynı zamanda üzerinde çalıştıkları yazılım veya hizmetleri ve ortamları sorunsuz bir şekilde yönetmelerini sağlamak için tasarlanmıştır. Kovter fidye saldırısında, genellikle makro tabanlı bir Microsoft uygulamasında bulunan kötü amaçlı bir program parçacığı (script) spam e-posta eklentisi halinde iletilir. 2016 sonrasındaki versiyonlarında ise, yetişkin pornografisi web sitesi Pornhub ile yayılmaya başlamıştır. Açılan bir mesaj, acil bir güncellemeyi (sahte tarayıcı güncellemeleri veya sahte Adobe Flash güncellemeleri) tıklamaya zorlamak için uyarır. Sonuç olarak, sahte trafik ve tıklamalarla para kazanmak için tıklama başına ödeme reklamlarını içeren tipik tıklama sahtekarlığı etkinlikleri ile sonuçlanır. Mağdur burada istemeden tıkladığı reklamlar aracılığıyla saldırgana para kazandırmış olur.

8.3.6. SimpLocker (2014)

SimpLocker, Symantec tarafından Android mobil işletim sistemlerine yönelik olarak ilk ortaya çıkan fidye yazılımı olduğu onaylanmış dosya şifrelemesi yapan bir zararlı yazılımdır.

8.3.7. CTBLocker (2014)

Windows işletim sistemine sahip bilgisayarlara yönelik olarak geliştirilen CTBLocker, CryptoLocker gibi AES ve RSA birlikte kullanılmasına rağmen CrytoLocker dan farklı olarak komut ve kontrol sunucusuna bağlanmasını beklememek için gömülü RSA açık anahtarı bulundurur. Bu zararlı yazılımda ağ bağlantısı beklememek bir avantaj iken, saldırganın her enfeksiyon için ayrı açık anahtar üretmesi gerekmektedir.

8.3.8. Locky (2016)

Windows işletim sistemine sahip bilgisayarlarda e-posta ekinde gelen Word belgesinde bulunan zararlı bir makro üzerinden sisteme sızar.

8.3.9. Cerber Version 6.0 (2016)

Dosyasız fidye yazılımı olmakla birlikte çok kullanımlı (İng:multithreading) şifreleme yöntemi kullanmaktadır.

8.3.10. SamSam-Samas, Samsa (2016)

Yamalanmamış savunmasız Linux tabanlı sunucuları (Red Hat JBoss gibi) hedeflemektedir. Bu sunuculardaki bilinen güvenlik açıklarından (uzak masaüstü protokolü - RDP gibi) yararlanarak sunuculara sızdıktan sonra kaba kuvvet saldırıları veya bazı mevcut araçlar yardımıyla kimlik bilgileri ve/veya ağa bağlı bilgisayarlarla ilgili bilgi toplarlar. Daha sonra bir fidye talep etmeden önce bu sistemlerde dosyaları şifrelemek için fidye yazılımlarını dağıtırlar [9].

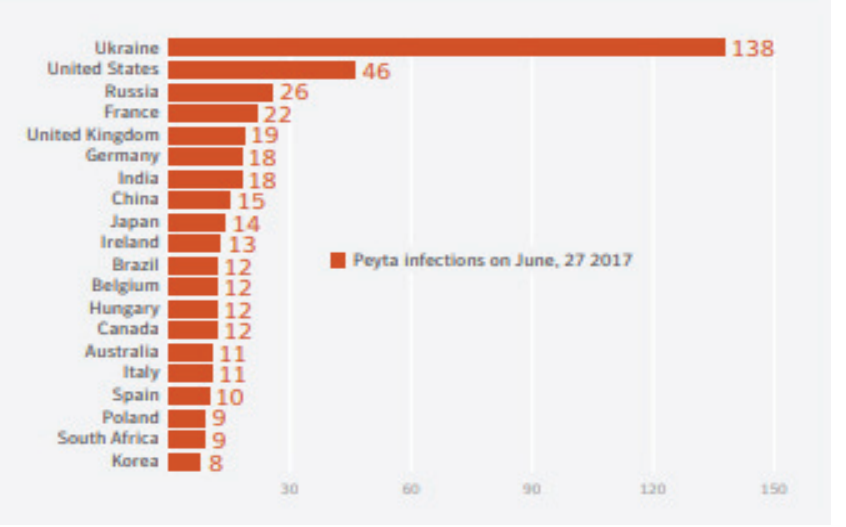
8.3.11. WannaCry (2017)

WannaCry ya da WannaCryptor'un en önemli özelliği, Windows'da EternalBlue istismarı olarak bilinen iki güvenlik açığını (CVE-2017-0144 ve CVE-2017-0145) kullanılarak geliştirilen bir solucan aracılığıyla bilgisayar ağındaki herhangi bir enfekte olmamış bilgisayara yayılmayı başarabilmesiydi. Bu özelliği ile, saldırıya başladığı ilk saatler içinde İnternette binlerce makineye yayılmaya başarabildi. Her makine için ayrı bir Bitcoin cüzdan adresi üretmesinin hedeflenmesine rağmen, yazılımın bir açığı olarak ödeme için sadece 3 Bitcoin adresinde çalıştığından saldırganlar hangi mağdurun ödeme yaptığını anlayamadılar. Bununla birlikte, saldırganlar varolmayan bir alan adresi canlı değilse saldırıyı durdurmak üzere bir tasarım yapmışlardı; ancak bu alan adresi bir güvenlik araştırmacısı tarafından farkedilip satın alınınca saldırı saldırganın isteği dışında hızlıca durdurulabildi. Eğer yazılımın bu açığı olmasaydı, WannaCry yaratıcılarına on milyonlarca dolar kazandırabilirdi [10].

8.3.12. Petya/NotPetya (AxPetr) (2017)

WannaCry gibi, Petya/NotPetya da EternalBlue istismarını yayılmak için kullandı, fakat aynı zamanda diğer Sunucu Mesaj Bloğu (ing: Server Message Block, SMB) ağ yayma tekniklerini de içeriyordu. Bu da EternalBlue'ya karşı yamalanmış bilgisayarlara dahi yayılabileceği anlamına geliyordu. WannaCry'dan farklı olarak, disk şifresi çözülemediğinden, Petya/NotPetya gerçekten fidye ya-

zılımı değildi, disk wiper denilen bir disk siliciydi ve özellikle Şekil 8.4'te görüleceği üzere özel olarak Ukrayna'yı hedef almıştı. Petya/NotPetya tarafından şifrelenen diskler hiçbir zaman kurtarılamayacaktı. Ancak EternalBlue ve SMB yayma teknikleri kullanıldığından saldırganların istemi dışında Ukrayna dışındaki bazı cihazlara da bulaşmıştır.



Şekil 8.4. Petya 2017'den etkilenen ülkeler (Kaynak: Symantec [10])

8.3.13. BadRabbit (2017)

En çok Rusya'da etkili olan BadRabbit, Petya/NotPetya'ya benzemekle birlikte ondan farklı olarak bir fidye yazılımdır, disk silici değildir. Bununla birlikte, EternalBlue istismarı yerine yerel ağda yatay olarak hareket etmek için EternalRomance istismarını kullanır. Rusya'ya Petya'ya karşı bir misilleme olduğu görüşü hakimdir. Bu saldırılar politik çekişmelerin karşılıklı siber saldırılarla bir siber savaşa dönüşmesine örnek teşkil etmektedirler.

8.4. Fidye Yazılımlarına Karşı Alınabilecek Önlemler

Ransomware ya da fidye yazılım saldırısına karşı savunma diğer kötü amaçlı yazılımlara karşı yapılacak savunmadan çok farklı değildir. Bu bölümde bu saldırılara karşı alınabilecek bazı basit önlemler anlatılacaktır. Özellikle kişisel bilgisayarlarında Windows işletim sistemi kullananların sayısı diğer işletim sistemlerini kulla-

nanlardan daha fazla olduğu için fidye yazılım saldırıları daha çok Windows işletim sistemine yönelik yapılmaktadır. Bu nedenle, bazı önerilerde özellikle Windows işletim sistemine yönelik örnekler verilmiştir.

1. Yedekleme yapmak (İng: Back Up) : Düzenli olarak yedek almak, güncel yedekleri farklı bir lokasyonda saklamak.
2. Spam bağlantılarından kaçınmak: Kaynağı bilinmeyen tüm bağlantılardan kaçınmak. Güvenilir kaynaklardan geldiği belli değilse, herhangi bir bağlantıya veya reklama tıklanılmamalıdır. Şüpheli durumlarda çevrimiçi web sitesi derecelendirme hizmetleri kullanarak bir sitenin ziyaret edilmesinin güvenli olup olmadığı kontrol edilebilir (Örn. https://safeweb.norton.com/, https://transparencyreport.google.com/safe-browsing/search, https://global.sitesafety.trendmicro.com/ gibi).
3. Bilinmeyen kaynaklardan (kaynak isimlerindeki aldatmacalara dikkat edilmelidir) gelen e-posta eklerini açmamak: Siber suçlular genellikle bir çevrimiçi mağazadan, bir bankadan, güvenlik birimlerinden, bir mahkeme veya vergi tahsilat kurumundan gelen e-posta bildirimlerine çok benzeyen, kötü niyetli bir bağlantıyı tıklayıp zararlı yazılımları sistemlerine bırakan sahte e-posta mesajlarını dağıtır.
4. Yamaları takip etmek (ing:patch): Tüm işletim sistemini, tarayıcıları, güvenlik sistemini, Flash ve Java gibi üçüncü taraf eklentileri her zaman güncel tutmak ve yayınlanan yamaları takip etmek. İşletim sisteminin ve/veya tüm uygulamaların yeni bir sürümü yayınladığında yüklemek ve eğer yazılım otomatik güncelleme seçeneği sunuyorsa, bu özelliği açık tutmak.
5. Yayılmayı önlemek: Enfeksiyona uğramış cihaz sayısını en aza indirmek için enfeksiyona uğramış cihazı ağdan çıkartmak.
6. Dosya uzantılarını göstermek: Bilgisayarınızdaki dosya listeleme ayarlarında dosya uzantılarını göster seçeneğini etkinleştirmek. Bu etkinleştirme, potansiyel olarak zararlı dosyaları ('.exe', '.vbs' ve '.scr' gibi) tespit etmeyi çok daha kolaylaştıracaktır. Saldırganlar, kötü amaçlı çalıştırılabilir bir dosyayı video, fotoğraf veya

belge olarak gizlemek için çeşitli uzantıları kullanabilir (Örn. hotchics.avi.exe veya doc.scr gibi) [11].

7. Yazılım Kısıtlama İlkelerini yapılandırmak: Beyaz listeleme (İng: whitelisting) de denilen Yazılım Kısıtlama İlkelerini sıkı bir şekilde uygulamak. Bu yapılandırma tüm uygulamaları varsayılan olarak engelleyerek ve daha sonra yalnızca belirli programların çalışmasına izin vererek kurulum kurallarının ayarlanmasına olanak sağlar. Yazılım Kısıtlama İlkelerini yapılandırmak için iki strateji kullanılabilir:

a. Yürütülebilir dosyaların yalnızca belirli klasörlerden çalıştırılmasına izin verilebilir (Örn. C:/ Program Files (x86) gibi). Örneğin Windows işletim sistemi kullanan bilgisayarlarda - Local Security Policy (secpol.msc) çalıştırarak ayarlamalar yapılabilir.

b. Kullanıcı dizinlerinde çalıştırılabilir dosyaların çalışmasını engellemek. Yönetici ayrıcalıklarına sahip olmayan bir kullanıcının, kendi dışındaki sistem dizinlerine yazma hakkı yoktur. Bu nedenle, bir virüs kendisini kullanıcı profilindeki dizinden başka bir yere yerleştiremez. Windows işletim sistemine sahip bilgisayarlarda Group Policy Editor (gpedit.msc) çalıştırarak ayarlamalar yapılabilir.

Genellikle kötü amaçlı yazılımlar kendilerini /% APPDATA% ve% TEMP% klasöründe kopyalayıp orada * .exe yürütülebilir dosyalarının çalışmasını sağladıklarından bunları engelleyen kurallar oluşturulabilir [12].

WannaCry ve türevleri için alınabilecek ek önlem:

- WannaCry'ın ağınızda yayılmasını önlemek için Sunucu İleti Bloğu (ing:Server Message Blocking) Smb v1 özelliğinin devre dışı bırakmak. Bu protokolü Windows, yerel bir ağda dosya paylaşımı için kullanır. Smb v2 ve v3 sürümleri etkin bırakabilir; bunlar daha güvenlidir.

Locky ve türevleri için alınabilecek ek önlemler:

- Microsoft Office uygulamalarında makroları devre dışı bırakmak. Eğer kullanıcı etkinleştirmemişse varsayılan olarak devre dışı durumdadır.

- ActiveX içeriğini devre dışı bırakmak.

Kurumların Fidye Yazılımlara Karşı Alması Gereken Önlemler:

- Güvenilir bir antivirüs yazılımı kullanmak
- E-posta Filtreleme uygulamak
- URL engelleme yapmak
- Beyaz Listeleme yapmak (Güvenilir Uygulamalar Listesi oluşturmak)

Fidye yazılımları önlemek için birçok akademik çalışma da yapılmıştır. Güvenlik araştırmacıları tarafından kötü amaçlı yazılım tespit etmek için önerilen birçok teknik (anormal davranışları olan sürecin algılanması için işlemci kullanımı, bellek kullanımı ve Girdi/Çıktı oranlarına dayalı istatistiksel yöntemler kullanarak süreçlerin izlenmesi gibi [13]), fidye yazılımların analiz edilmesinde de oldukça yararlıdır. Bununla birlikte, fidye yazılım saldırılarına karşı uygun bir şekilde savunmak, ek bir dizi yeni zorluğun çözümünü gerektirir [14]. Bir NTFS birimindeki her dosya, ana dosya tablosu (ing: master file table, MFT) adı verilen özel bir dosyadaki bir kayıt tarafından temsil edilir. MFT tablosu yakından takip edilerek dosyaların oluşturulması, şifrelenmesi veya silinmesini algılanabilir [15]. Üzerinde çalışılan bir diğer konuda, saldırıların komut kontrol sunucuları ile bağlantıları sırasında yapılan çalışmalardır. DGA tabanlı komut kontrol sunucu kullanan saldırganlar, güvenlik duvarları, IDS / IPS ve hatta tehdit istihbaratı beslemeleri gibi çevre tabanlı güvenlik savunma araçlarından kolayca kaçınabilmektedirler. Fidye yazılım, bu sunuculara bağlanmak için DNS çözümleme sorguları kullanmaktadır. Bu sorgulamalar, sistemin DNS günlüklerinde takip edilebilir. Makine öğreniminde (ML), bu problem iki sınıfın olduğu (iyi niyetli (ing: benign) DNS sunucusu ve kötü niyetli komut kontrol alan sunucusu) bir sınıflandırma problemi olarak ortaya çıkmaktadır [16] [17].

8.5. Değerlendirmeler

Günümüzde fidye yazılımları açık ve istikrarlı bir tehdit olmaya devam etmektedir. Zamanla daha sofistike yapıları ile daha büyük

hedeflere varmak için geliştirilmeye devam edilmektedirler. Dark Web'de farklı fiyatlara satılan (örn. RaasBerry 0.0131 bitcoin, Stampado $39) fidye yazılımı dağıtım kitleri ile çok az teknik beceriye sahip kişilerin bile saldırılarına maruz kalınabilmektedir. Zararlı yazılım geliştiricileri sürekli olarak, karlı stratejiler bulmaya çalışmaktadır.

Son zamanlarda zararlı yazılım geliştiriciler için, fidye yazılımdan kripto para madenciliğe doğru bir trend değişikliği göze çarpmakla beraber, bazı endüstriler fidye yazılımlar aracılığıyla hala hedef olmaya devam etmektedir. Özellikle sağlık sektörü ve özel olarak hastaneler saldırganlar için kazançlı hedefler olmaya devam etmektedirler [18]. Fidye yazılımlara karşı alınabilecek en öncelikli tedbir bilgisayar kullanıcılarının bu yazılımlarla ilgili farkındalığa sahip olmalarını sağlamaktır. Sonrasında ise alınabilecek temel tedbirler konusunda bilgilendirmeler yapılmalıdır.

Kaynaklar

[1] R. Correa, "How Fast Does Ransomware Encrypt Files? Faster than You Think," Barkly, April 2016. [Çevrimiçi]. Available: https://blog.barkly.com/how-fast-does-ransomware-encrypt-files. [Erişildi: 2018].

[2] "AIDS (Trojan Horse)," [Çevrimiçi]. Available: https://en.wikipedia.org/wiki/AIDS_(Trojan_horse). [Erişildi: 9 2018].

[3] S. Corporation, "INTERNET SECURITY THREAT REPORT 2014," 2014. [Çevrimiçi]. Available: http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf. [Erişildi: 2018].

[4] K. Jarvis, "CryptoLocker Ransomware," 18 December 2013. [Çevrimiçi]. Available: https://www.secureworks.com/research/cryptolocker-ransomware. [Erişildi: 2018].

[5] Telefonica, "Trend Report Ransomware," 14 7 2015. [Çevrimiçi]. Available: https://www.elevenpaths.com/wp-content/uploads/2015/07/TDS-Ransomware-Telefonica-2015-07.pdf . [Erişildi: 2018].

[6] D. G. David Fitzpatrick, "Cyber-extortion losses skyrocket, says FBI," 2016. [Çevrimiçi]. [Erişildi: 2018].

[7] LogRhythm, "HOW RANSOMWARE WORKS," [Çevrimiçi]. Available: https://gallery.logrhythm.com/infographics/how-ransomware-works-infographic.pdf. [Erişildi: 2018].

[8] B. Lee, "Unlocking the Lucrative Criminal Business Model," [Çevrimiçi]. Available: https://www.paloaltonetworks.com/resources/research/ransomware-report.html. [Erişildi: 2018].

[9] D. Manky, 31 May 2018. [Çevrimiçi]. [Erişildi: 9 2018].

[10] Symantec, "2018 Internet Security Threat Report," 2018. [Çevrimiçi]. Available: https://www.symantec.com/security-center/threat-report. [Erişildi: 2018].

[11] "No More Ransome," [Çevrimiçi]. Available: https://www.nomoreransom.org/en/prevention-advice.html. [Erişildi: 2018].

[12] W. OSHub, "How to Block Viruses and Ransomware Using Software Restriction Policies," 12 January 2017. [Çevrimiçi]. Available: http://woshub.com/how-to-block-viruses-and-ransomware-using-software-restriction-policies/]. [Erişildi: 2018].

[13] Song, S. Song, B. Kim ve S. Lee, "The effective ransomware prevention technique using process monitoring on android platform," Mobile Information Systems, 2016.

[14] "Protecting against Ransomware: A New Line of Research or Restating Classic Ideas?," IEEE Security & Privacy, cilt 16, no. 3, pp. 103 - 107, 2018.

[15] K. Amin, R. William, B. D. B. Leyla ve K. Engin, "Cutting the Gordian Knot: A Look Under the Hood of Ransomware Attacks," %1 içinde Detection of Intrusions and Malware, and Vulnerability Assessment, Springer, LNCS, 2015.

[16] D. Gujraniya, M. Waseem, B. AR ve S. Singh, "Ransomware Command and Control Detection using Machine Learning," 15 January 2018. [Çevrimiçi]. Available: https://www.acalvio.com/ransomware-command-and-control-detection-using-machine-learning/. [Erişildi: September 2018].

[17] D. Sgandurra, L. Muñoz-González, Rabih Mohsen ve E. C. Lupu, "Automated Dynamic Analysis of Ransomware: Benefits, Limitations and use for Detection," CoRR, 2016.

[18] A. Liska, "5 Ransomware Trends to Watch in 2018," 6 March 2018. [Çevrimiçi]. Available: https://www.recordedfuture.com/ransomware-trends-2018/.

WannaCry ve Petya Fidye Yazılımları

BÖLÜM 9

Burak ÖZÇAKMAK
Prof. Dr. Şeref SAĞIROĞLU

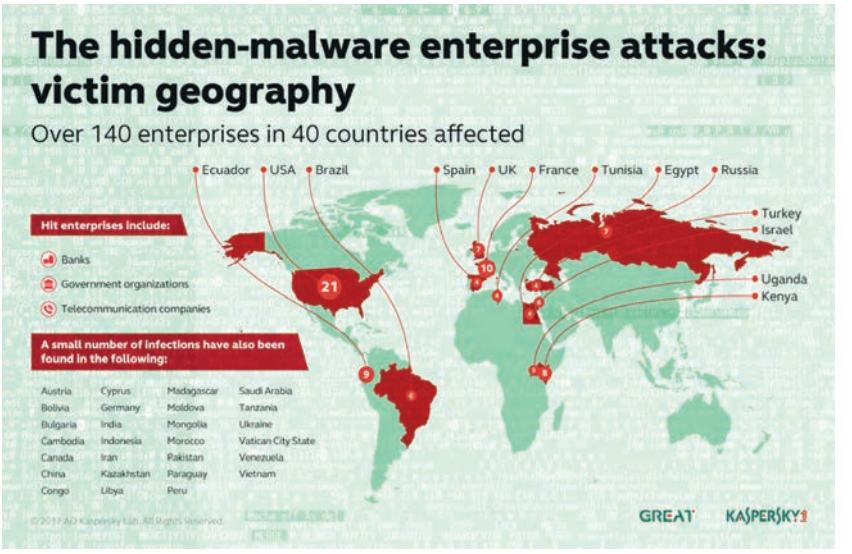
WANNACRY VE PETYA FİDYE YAZILIMLARI

Bir önceki bölümde genel olarak aktarılan, türleri açıklanan, nasıl korunulması gerektiğine dair genel olarak bahsedilen bilgilere ilave olarak kitabın bu bölümünde, fidye yazılımlarından olan WannaCry ile dünya çapında etkisi yüksek olan diğer bir fidye saldırısı olan Petya zararlı yazılımı detaylı olarak incelenmiş, bu iki fidye saldırısına ait kod parçacıkları, verdikleri zararlar ve saldırganların kullandığı sistematik ve kullanılan metodolojiler verilmiştir. Bu kitap bölümünde incelenen konunun detaylarına [45] nolu kaynakta verilen tezden erişebilirsiniz.

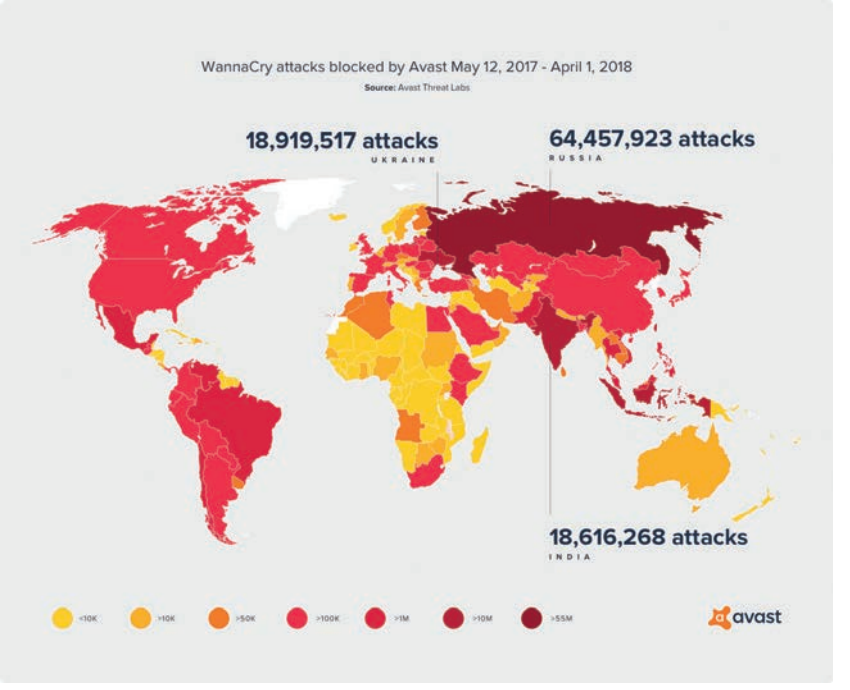
9.1. Giriş

Fidye yazılımı saldırıları (Ransomware attacks) WannaCry ve Petya ile dünya genelinde birçok çevrenin dikkatini çekmiş olsa da 1990'lı yıllardan itibaren etkisini arttırarak devam ettirmiş bir siber saldırı çeşididir. Fidye saldırıları alanında 1990'lı yıllardan günümüze kadar ne çeşit saldırılar olduğu, bu saldırıların nasıl değişim gösterdiği, günümüz siber saldırılarında fidye saldırılarının nasıl bir ağırlığının olduğu, diğer kötücül saldırılar ile fidye saldırıları arasında ne gibi benzerlikler ve farklılıklar olduğu, fidye saldırılarının hangi sistemlere bulaşabildiği, özellikle WannaCry ve Petya ile beraber fidye saldırılarının nasıl bir boyut kazandığı, fidye saldırılarından korunma yöntemleri hakkında akademik dünyada ne gibi çalışmalar yapıldığını bilmek, yapılan saldırıları daha iyi anlamak için çok önemlidir.

WannaCry'ın etkisini daha iyi anlatmak için Şekil 9.1'de bazı güncel istatistikler verilmiştir. Verilen şekilden bu saldırıya maruz kalan ülkeler, saldırı boyutları detaylıca görülebilir[1].



(a) Kaspersky İstatistikleri (2017)



(b) Avast İstatistikleri (2017)

Şekil 9.1. WannaCry'dan etkilenen ülkeler ve yapılar

2014 yılında, CryptoWall [2,4,6] ve CryptoDefence [2,3,5,6] zararlı yazılımları ortaya çıkmış, henüz kırılmamış bir diğer güçlü simetrik şifreleme yaklaşımı olan AES'i kullanarak dosyaları şifrelemişlerdir. 500.000'den fazla sistemin etkilendiği değerlendirilen bu saldırılarda saldırganlar kimliklerinin deşifre olmasını engellemek amacıyla TOR ve benzeri anonim ağları kullanmışlardır [7]. Ayrıca özellikle para akışında iz bırakmamak için de Bitcoin tarzı yeni yaklaşımları kullanmaya başlamışlardır [8].

2015 yılında TelsaCrypt AES kullanan bir başka fidye yazılımı olmasına karşın, 170 farklı dosya formatını şifreleyebilmesi ile diğer fidye yazılımlarına göre çok daha fazla mağdurun bilgisayarlarında etkin olmuştur. 2016 yılında birçok farklı isimli benzer özellikleri taşıyan fidye yazılımları da sistemleri etkilemiştir [8-9]. Aynı dönemde etkin olan diğer zararlı yazılımlar ise; CryptorBit, CTBLocker, SynoLocker, CryptoWall, CryptoBlocker, OphionLocker, Pclock, CryptoWall, TeslaCrypt, Vaultcrypt, LowLevel04 [10] zararlı yazılımlarıdır. Günümüzde halen geliştirilmeye çalışılan fidye yazılımı aileleri ise Cerber, Spore, Serpent, Petya, WannaCry ve NotPetya aileleridir [11]. Fidye yazılımı saldırılarında son yıllarda ciddi artışlar olduğu, Tox fidye yazılımından etklenen makina sayısının bir yılda 4.1 milyon'dan 8.8 milyona ulaştığı raporlanmıştır [12].

Fidye yazılımları ve etkilerini anlatan literatürde çok sayıda akademik çalışma bulunmakta olup aşağıda kısaca açıklanmıştır. Bunlar;

- Fidye yazılım ailelerinin dünyadaki yıkıma neden olan en önemli varyantlarından olarak anılan Scareware ve Locker yazılımları, her saldırı için yeni bir Bitcoin cüzdanı oluşturmakta ve fidye ödemesi için mağdurun kimliğini göndermektedir [13].
- Kriptografik fidye yazılımları ile kullanıcı verilerine erişim, gelişmiş şifreleme algoritmaları ile şifrelenerek engellenmekte ve ödeme gerçekleşmediği takdirde şifrelenmiş verilerin kalıcı olarak silineceğini belirten tehdit edici mesaj içeren not görüntülenmektedir [14].
- Mağdurun sisteminde üretilen simetrik anahtar kullanılarak kullanıcı sistemindeki yer alan değişik formatlı veriler şifrelenmekte, asimetrik yaklaşımlarla komuta kontrol sunucu yapısını andıran sunucular kontrol edilmektedir [15].

- 28 farklı zararlı yazılım ile 22 farklı özellik bazında fidye yazılımları incelenmiştir [1].
- Fidye yazılımlarının belli dosya formatları ile hazırlanarak; exe, zip, rar, 7z, js, wsf, docm, xlsm, pptm, rtf, msi, bat, com, cmd, hta, scr, pif, reg, vbs, cpl, ve jar uzantılı dosyalara bulaştırıldığı raporlanmıştır [16].
- Fidye yazılımlarının yayılım yöntemlerine bakıldığında; trafik-yönlendirme, uzaktan dosya indirtme, e-posta eki ile zararlı yazılım gönderme, sosyal mühendislik yöntemlerinin kullanıldığı görülmüştür. Satın alınan fidye yazılım servisleri [17] ile sosyal mühendislik aracılığıyla kullanıcılar arasında nasıl yayılacaklarını, saldırganların manipülasyon ve ikna için sosyal ağlar, e-posta, mobil cihazlar ve Web 2.0 siteleri gibi yeni araçları kullandıklarını, işletim sistemi, anti-virüs vb. sistemleri ve ağı koruyan güvenlik önlemlerini geçebileceği ve kurumsal ağlara erişimin kazanılabileceğini araştırmalar sonunda görülmüştür[18]. Ayrıca oltalama saldırısı (phishing) ile her kullanıcının kişisel zafiyetinin tespitinde ve bunun sömürülmesinde en kısa zamanda sonuca giden yöntemler [19] vardır.

Saldırıları analiz etme ve önleme içinde yapılan çalışmalar mevcuttur. Bunlar;

- Mağdurun sisteminde zararlı fidye yazılımının çalıştırılmasının sonrasında, mağdurdan para istemek amacıyla gönderilen tehdit edici içerikteki fidye mesajlarının analizi ile saldırgan tarafından bırakılan fidye notunun, mağdur için görüntülendikten sonra saptanması zor olsa da saldırganın komuta kontrol sunucusunun tespitinin yapılabilmesi [20],
- Bytecode gösterimlerini kullanarak Android fidye yazılımlarını tespit etme yöntemleri [21],
- Kilitleyici fidye yazılımlarını ve şifreleme yaklaşımlarını tespit etmek için sistemin saldırıdan önce ve sonra verilerini ve ekran görüntülerini alan bir izleme yöntemi önerisi, bulaşma anının tespiti, sistemi nasıl etkilediğinin tespiti, sistemin sürekli yedeği alma [22],
- kriptografik teknikleri kullanarak fidye yazılımlarına karşı proaktif olarak korunma yöntemleri önerme, fidye yazılımı tarafın-

dan yapılan kriptografik API (Uygulama Programlama Arayüzü) çağrılarının dinamik olarak engellenme, özellikle WannaCry ve Petya gibi karmaşık ve çoklu yöntem kullanan fidye yazılımlarına karşı herhangi bir çözüm yazarın yaklaşımında yer almasa da önerilen yöntem uygulandığında genel fidye yazılımı örneklemleri göz önüne alındığında yaklaşık %50 başarım elde etme [23] gibi çalışmalar mevcuttur.

Bunlara ilave olarak son zamanlarda, birçok çalışmada özellikle zararlı yazılımların giderek daha karmaşık hal alması, analiz ve engelleme yöntemlerine karşı kendini geliştirmesi nedeniyle dinamik analizin çok daha güçlü yanlarının olduğu [24]-[27], fidye yazılımını tespit etmek için statik ve dinamik analiz yapılması gerektiği [28] ve fidye yazılımının genel olarak 5 ana adımdan oluştuğu ve bu adımların;

1) fidye yazılım kodunun e-posta ya da web aracılığıyla amaçlanan makineye gönderilmesi,
2) kodun çalışması için iletişimin başlatılması,
3) sistemdeki önemli dosyaların aranması,
4) bulunan dosyaların şifrelenmesi, ve
5) Bitcoin üzerinden fidye talebinde bulunulmasıdır.

Fakat WannaCry ve Petya gibi zararlı yazılımlarda kod bloğunun çok karmaşık olmasından dolayı statik ve dinamik analizin yanında makina öğrenmesi, veri madenciliği, ve karar ağacı tabanlı yaklaşımların kullanılması gerektiği savunulmuş ve fidye yazılımının dinamik analiz ile çok daha rahat anlaşılabileceği belirtilmiştir [27]-[29].

Zararlı yazılımların analizi için ayrıca temel ve ileri seviye analizlerin yapıldığı, temel analizde zararlı yazılım çalıştırılarak sistem üzerinde yaptığı değişiklikler ve işlemlerin ağ trafiği üzerinde analiz edildiği, ileri seviyede yapılan analizde ise işlemler hata ayıklayıcı (debugger) ve paket ayırıcı (disassembler) kullanılarak, çalışan zararlı yazılımın adım adım incelenmesiyle belirlendiği [29]-[32], WannaCry zararlı yazılımının sandbox ortamında analiz edildiği [33], ve dinamik test ortamı ile Cryptowall trafiği analiz edilerek zararlı yazılımın gittiği URL adresleri ve alan adları tespit edildiği

[34], ms17_010 açıklığını kullanarak kullanıcı ile etkileşime girmeden direk olarak hedef sisteme bulaşan, bulaştığı sistemi şifreleyen ve açmak için TOR ağları üzerinden fidye isteyen kötü amaçlı bir yazılım olduğu [35], bu saldırıdan 150 ülkede 230.000 civarında bilgisayarın etkilendiği, fidye yazılımları için alınan önlemlerin mevcut kötü amaçlı yazılıma karşı alınan önlemler ile benzerlikler gösterdiği [36]; saldırıya maruz kalan kişiler üzerinden alınan log kayıtları ve saldırı yaklaşımlarına dair kanıtları kullanarak bir sonraki saldırıdan korunma yöntemleri belirlendiği [37]-[38]; bir önceki kitap bölümünde de belirtildiği gibi fidye yazılımlarından korunmak için antivirüslerin güncellenmiş olması gerektiği, spam mesajlarının başkalarına iletilmemesi, anti-spam cihazlarının düzgün yapılandırılması gerektiği, indirilen dosya tiplerininde beyaz liste kullanılması gibi tavsiyeler verildiği [39] görülmüştür.

Yukarıdaki açıklamalardan ve bir önceki bölüm de de özetlendiği gibi siber saldırılarda en büyük etkinin son dönemde fidye yazılımları ile gerçekleştirildiği verilen raporlarda yer almaktadır. Fidye yazılımlarının özellikle WannaCry ve Petya ile beraber sıfırıncı gün zafiyetlerini kullanarak çok daha hızlı yayıldığı ve etkin olduğu görülmüştür.

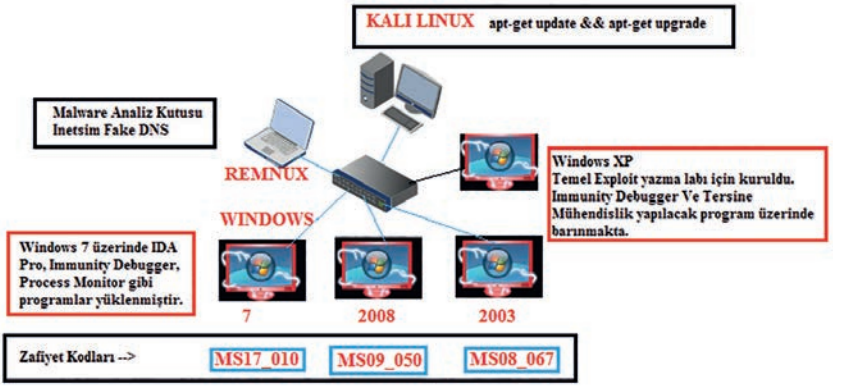
9.2. Petya ve WannaCry Fidye Yazılımları

Şekil 9.1'den de görülebileceği gibi 140 ülkede milyonlarca bilgisayara bulaşarak çok farklı dillere sahip bir fidye yazılımı olan WannaCry, fidye talep eden geniş çaplı bir siber saldırı aracı olarak kabul edilmiştir. Etkileri Rusya Federasyonu, Ukrayna, Hindistan, Tayvan, Tacikistan, Kazakistan, Lüksemburg, Çin, Romanya, Vietnam, İtalya, Brezilya, Hong Kong, İran, İspanya ve ABD'nin de dahil olduğu 140'ın üzerinde ülkede görülmüştür. Global alanda etkilenen bazı kurumlar aşağıdaki gibi sıralanabilir.

- İngiltere: NHS
- İspanya: Telefonica
- Amerika Birleşik Devletleri: FedEx, Waterloo Üniversitesi
- Rusya: Rusya İçişleri Bakanlığı, Cбepa Bank, Rusya Demiryolları
- Hindistan: Shaheen Airlines
- Almanya: Frankfurt Tren İstasyonu, Neustadt İstasyonu

WannaCry ve Petya zararlı yazılımlarının incelenebilmesi ve bahsedilen zararlı yazılımlar üzerinde gerçekleştirilen teknik işlemlerin anlaşılabilmesi için exploit, 0. gün (zero day), fidye yazılımı, zararlı yazılım ve tersine mühendislik konuları hakkında bilgi sahibi olunması gerekmektedir.

Petya ve WannaCry zararlı yazılımları sunucu taraflı ms17_010 açıklığını kullanarak bilgisayarları ele geçirirler. WannaCry ele geçirdiği PC'leri şifrelerken Petya dosyaları şifrelemenin yanında MBR ve MFT dizinlerini de şifrelemektedir. Ayrıca, Petya saldırısının 2017'de kullanılan sürümünde dosyaların tamamını (wipe ederek) silmektedir. WannaCry ve Petya'nın farkını anlamak için öncelikle Samba açıklıklarının kullanımı ve derin paket (deep package) incelemelerinin yapılması, sonrasında ise fidye saldırısı analizi yapılması için Şekil 9.2'de verilen bir yapı kurularak bunun testlerinin yapılması gerekmektedir.



Şekil 9.2. Test kapsamında oluşturulan yapının blok şeması

Test çalışmalarında;

- işletim sistemlerinin çalıştırıldığı sanallaştırma ortamlarının ağ ayarları host-only olarak ayarlanması
- paylaşılan ağ içerisindeki bilgisayarların birbirleri ile konuşabilirken internete çıkmaları engellenmesi
- dinamik analiz sırasında zararlı alan adlarının bulunabilmesi için sadece Remnux üzerine iki adet ağ kartı takılması ve biri internete biri host only ağa göre yapılandırılması

- gereken durumlarda diğer işletim sistemlerine gateway olarak ayarlanacak şekilde bırakılması
- zararlı yazılımın sanal ortamdan fiziksel ortama geçerek tüm sistemi etkileme olasılığından dolayı, sistem izole ortamda çalışılması,
- test ortamı kurulumlarında Kali Linux üzerinde apt-get update ve apt-get upgrade komutları ile işletim sisteminin güncellenmesi,
- Windows 7 üzerinde Process Monitor, IDA Pro gibi programlar kullanılması,
- Windows XP üzerinde ise exploit lab için Immunity Debugger programı kullanılması

gibi işlemler gerçekleştirilmelidir.

İncelenen WannaCry ve Petya zararlı fidye yazılımlarının, sistemi etkilemesinin en büyük nedeni olan 0. Gün açıklıklarının kullanılması olduğu bilinmektedir. Yaması çıkmamış, daha üreticisi tarafından bile bilinmeyen bir açıklığa 0. Gün açıklığı (Zero Day) adı verilmektedir. WannaCry'ın dünya genelinde etkisinin bu kadar çok olması ve o zamana kadar alınan önlemlerin etkisiz kalmasının en önemli sebebi ise, 0. Gün açıklığı ile beraber, ek bir yöntem gerektirmeden, hedefin bir şey yüklemesi veya izin vermesine gerek kalmadan sisteme bulaşabilmesi ve kullanıcı farkına varmadan kullanılan sistemi ele geçirebilmesidir. Sunucu taraflı bir exploit kod ile yayılan WannaCry diğer fidye yazılımlarından bu özelliğiyle çok daha tehlikeli bir duruma gelmektedir. Bir başka deyişle, sunucu taraflı yayıldığı zaman kullanıcı etkileşimine dahi girmeden güvenlik açıklığından yararlanmaktadır. WannaCry ile fidye yazılımlarında yeni bir devir açıldığı ve bu devrin Petya fidye yazılımı ile devam ettiği düşünülmektedir.

Deep web, herkesin kolaylıkla erişemediği, internetin en alt katmanı olarak nitelendirilen ortamdır. Fidye saldırıları da diğer siber saldırılarda olduğu gibi Deep web de pazar bulmaktadır. TOR ağı üzerinden bedava, paralı ya da servis hizmeti veren fidye saldırıları siteleri araştırılmıştır. İlk olarak hiddenwiki web sitesi incelenmiştir. Satan adlı fidye saldırısı servisi incelendiğinde ilgili web sitesi üzerinden fidye saldırılarının paylaşıldığı görülmektedir [24].

Ranion isimli web sitesinde, paralı ve parasız versiyonlara sahip bir fidye yazılımı satıcısı tespit edilmiştir. Paralı modelde, kullanıcı paneli ve fidye saldırılarında kullanılmak üzere komuta kontrol sunucusunda ve iz kaybettirmeye yarayan ara sunucularında verilen hizmette yer aldığı görülmektedir. Kolaylıkla komuta kontrol sunucusu hedef kullanıcı için kurulmakta ve saldırılarınız için uygun ortam oluşturulmaktadır. 1 yıllık 900 dolar olan ve her istenilen özellik için ücrete karşılık ilgili ayarlama yapılmaktadır [40]. Deep Web'de zararlı yazılımların bulunması için kullanılan arama motorlarından biri de Torch'tur [41]. Torch arama motoru kullanılarak WannaCry ve fidye yazılımları aratılmıştır. İlgili arama sonucunda farklı özelliklerde hizmet sunan birçok site olduğu görülmüştür. Aynı arama NotEvil arama motoru ile tekrarlanmış ve farklı özelliklerde sunulan fidye yazılımı hizmetleri hakkında bilgiler elde edilmiştir [42]. İki arama motoru sonuçları karşılaştırıldığında Raasberry adındaki fidye yazılım servisinin etkin bir şekilde kullanıldığı görülmüştür. Bu servis komuta kontrol sistemi panel gibi kolaylıklar sağlamaktadır. Ayrıca; İspanya, Hindistan, Arap ülkeleri, Rusya gibi ülkelerden yoğun talep olduğu [43] ve Deep Web arama özelliklerinden olan "Hidden Answers" başlığı altında fidye yazılımlarına ilişkin aramalar yapıldığında elde edilen sonuçların örtüştüğü görülmüştür [44]. Sonuç olarak; saldırganların çoğunlukla kullandığı Deep Web üzerinden gerçekleştirilen araştırmalar neticesinde fidye yazılımlarının kolaylıkla satın alınabildiği ve istenildiği gibi konfigüre edilerek kullanılabildiği görülmüştür. Bu durumda artık siber saldırıların teknik altyapısı olmayan birçok insan tarafından da kolaylıkla elde edilebildiği görülmüştür.

9.3. WannaCry ve Pedya Fidye Yazılımlarının Çalışma Mekanizmaları

9.3.1. WannaCry

İnternet tarihinde geniş çapta yapılan en büyük fidye saldırısı olarak kabul edilen WannaCry saldırısı, Microsoft Windows işletim sisteminin SMB servisinin zafiyetinden (MS17_010) yararlanarak bulaştığı sistemdeki önemli dosyaları şifrelemekte ve 300 dolar (bitcoin) fidye talep etmektedir. Diğer fidye yazılımlarından fark-

lı olan saldırı şekli, SMB zafiyetini kullanarak EternalBlue sömürücüsü ile hedef sistemde dosya şifrelemektedir. Çalışma şeklini komuta&kontrol (C&C) sunucusuna canlı bağlantı ile gerçekleştirmektedir. C&C sunucusu ile iletişim kurmak için kullanılan "TOR. onion" adreslerinin bir listesini ve resmi bir TOR tarayıcı paketinin linkini WannaCry zararlı yazılımı kod içerisinde bulundurur. Diğer fidye yazılımları gibi offline olarak çalıştırılabilmektedir.

WannaCry zararlı yazılımın imza ve biçim bilgileri, mekanizması, saldırının dağılma ve yayılma süreci, tespit edilebilir imza davranışları ve şifreleme aksiyonları, RansomWare saldırı modelleri ile WannaCry saldırı yaklaşımı arasındaki farkları ve benzerlikleri, şifrelenen dosyanın çözümü ile anlaşılabilmektedir.

WannaCry saldırılarında kullanılan zararlı dosyaların teknik incelemeleri sonucunda elde edilen veriler aşağıda verilmiştir. İncelenen zararlı yazılımın Hash değerleri dosyanın orjinalliğini göstermek adına verilmiştir. Ayrıca kullanılan zafiyete ilişkin bilgiler, etkilenen sistemler de detaylı olarak tez çalışmasında yer almaktadır.

SHA256 değeri: ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e-5babe8e080e41aa

MD5 Hash değeri: 84c82835a5d21bbcf75a61706d8ab549

Dosya Tipi: Win32.exe

Kullandığı exploit: EternalBlue

Dosya boyutu: 3,5 MB (3,514,368 bytes)

Yayılmaya başlama tarihi: 11 Mayıs 2017

Hedef alınan sistem: SMB V1.0 kullanılan Microsoft işletim sistemleri

- Windows XP
- Microsoft Windows Vista SP2
- Windows 7
- Windows 8.1
- Windows RT 8.1
- Windows 10
- Windows Server 2008 SP2 ve R2 SP1

- Windows Server 2012 ve R2
- Windows Server 2016

Bitcoin adresleri üzerinden saldırganların fidyeleri topladığı ve bu sayede izlerinin bulunmasını zorlaştığı, Bitcoin adresleri üzerinden aldıkları ücretleri izlenemez hale getirip para tahsil ettikleri, Chain yapısının kullanılmasıyla paranın farklı hesaplara parçalanarak gönderildiği sonra tamamen alakasız bir hesapta tekrar toplandığı ve böylelikle iz sürülmesinin daha da zorlaştırıldığı görülmüştür.

WannaCry saldırısında kullanılan zararlı fidye yazılımlarının birçok farklı dosya formatında etkin hale geldiği, ve farklı uzantılardaki dosyalarda zararlı yazılımın çalışıp şifreleme yaptığı bilinmektedir. Ayrıca, bu saldırıda kullanılan zararlı kod içeren yazılımların sisteme yüklenirken kullanılan dosya isimleri gerçekleştirilen analiz çalışmaları neticesinde elde edilmiş olup aşağıda bazıları yer almaktadır.

- Busywin 17.XX Universal Patch.EXE
- WannaCry02
- wcry.exe
- WannaCry.exe
- Pentagon-RAT.EXE
- tasksche.exe
- Win32Filecoder.WannaCryptor.D
- WannaCrypt0r.exe1
- wanna2.0.exe
- WannaCry-2.0.exe
- wcry2.exe
- Ransom Wcry.exe
- svchost.exe

Mevcut ağ üzerinde sıçrama ve yayılma şekli SMB servisi (445. ve 139. Portlar) ile gerçekleşmektedir. Zararlı fidye yazılımı çalıştırıldığında ilk olarak WinMain executable'ı yürüterek komuta kontrol sunucusu önündeki ara sunucuya bağlanmaya çalışmaktadır. Bura-

dan herhangi bir dosya çekmemekte, sadece bağlantı kontrolü sağlamaktadır. Bu zararlı yazılımın çalışmasını engelleyecek bir "kill switch" tekniğidir. Bağlantı sağlandığı takdirde zararlı yazılım çalışmayı durdurmaktadır. Bağlantı sağlanmadığı takdirde çalışmaya devam etmektedir.

Zararlı fidye yazılımının yayılım işlevleri "mssecsvc2.0" (Microsoft Security Center Service) servis derleyicisinin kontrolündedir. Bu servisin işlevi, WSA fonksiyonunu başlatma ve şifreleme fonksiyonunu başlatma olarak ikiye ayrılır. WSA fonksiyonu, özellikle SMB kullanımı için iki iş parçacığı üretir; biri iç hedefleri enfekte etmek için, diğeri dış hedefleri etkilemek içindir. WSAStartup() fonksiyonunu zararlı yazılımın iki iş parçacığının çağırıldığı fonksiyondur. WSAStartup çalıştıktan sonra CryptAcquireContext() fonksiyonunu çalıştırıp crypto API'sini başlatmaktadır ki bu sayede sözde-rastlantısal numara üretici fonksiyon devreye girebilmektedir. Bundan sonra çağırdığı fonksiyon ise fidye yazılımının payload dll dosyalarını saklamak için tampon bellek oluşturmaktadır, bu dll'lerin birisi x64 sistemler için, diğeri ise x86 sistemler için kullanılmaktadır. Bu fonksiyon payload dll'lerini, zararlı yazılımların içinde bulunan ".data" içerisindeki alandan çekip kopyaladıktan sonra tüm zararlı binary'sini de kopyalamaktadır.

Kopyalanan her dll dosyasının boyutu oldukça küçüktür, zararlı fidye yazılımının binary kodu mevcut sabit diske C:\WINDOWS\mssecsvc.exe olarak kendini kopyalayıp çalışmaktadır. Zararlı fidye yazılımı kendini tamamıyla kopyaladıktan sonra mevcut iki fonksiyonu çalıştırmaktadır. Bunlardan ilki yerel ağ üzerindeki sistemleri taramaktadır, diğeri ise internet üzerinden tarama yapmaktadır. Lokal ağ üzerinde tarama yapmak için GetAdaptersInfo() fonksiyonu kullanılmaktadır. Bu fonksiyon ile lokal ağ üzerindeki IP aralıklarının listesi kopyalanır, her bir IP adresi için yeni bir dizi yaratılır. Taramayı gerçekleştiren fonksiyon taradığı sistemler üzerinde 445'inci port'u kontrol etmektedir. Eğer port açık ise ikinci bir fonksiyon devreye girip MS17-010/EternalBlue zafiyetini tetiklemeye çalışmaktadır. Bahsi geçen fonksiyon eğer zafiyet tetikleme aşaması 10 dakika içerisinde bitmez ise zararlı fidye yazılımı saldırıyı durdurmaktadır.

WannaCry fidye yazılımında kullanılan "MS17_010" güvenlik açığının teknik detaylarına bakıldığında; MS17_010, Microsoft'un SMB versiyon 1.0 servisinin zafiyetine karşılık yayınlanan güvenlik bültenidir. "MS" ibaresi Microsoft'u "17" ibaresi 2017 yılını ve "010" ibaresi ise yayınlanan güvenlik açığının numarasını tanımlamaktadır. Başarılı olarak tetiklenmesi sonucunda "uzaktan komut çalıştırma" gerçekleşir. Tetikleyen, hedef sistem üzerinde istediği kodu çalıştırabilme yetkisine sahip olur. Yapılan bir ileti isteği SMB/MaxBufferSize'dan büyük ise iletiler ikincil "Trans2" ileti olarak gönderilir. Bu durumda "buffer" taşırılarak zafiyetin gerçekleştirileceği alan olan trans2 iletim alanına zararlı istek yazılır ve iletim sağlanır. Oturum_setup_andx_request ile "Max buffer" boyutu taşırılarak iletime trans2_request ile devam edilir.

Zararlı yazılımın bulaştığı her sistem kendi RSA 2048 bit anahtarını CryptGenKey ile üretmektedir. Genel anahtar CryptExportKey() kullanarak 00000000.pky dosyasında tutulmaktadır. Özel anahtar ise 00000000.eky dosyasında tutulmaktadır. CryptExportKey() fonksiyonu ile şifrelenen ama aynı zamanda CryptEncrypt ile daha önceden şifrelenen dosya, disk şifrelemeden sorumlu dll dosyasında tutulmaktadır. AES anahtarı ise kullanıcıların genel anahtarı ile şifrelenir ve "AES ciphertext" alanında tutulur. AES anahtarını çözmenin tek yolu, özel anahtarı bulmaktır.

WannaCry fidye zararlısı önemli dosyaları şifreledikten sonra şifreleme anahtarlarını silmektedir. Bu anahtarlar olmadan, şifrelenmiş dosyaların şifresi çözülemez. Ancak bu süreçte erken davranılırsa kurtarma gerçekleşebilmektedir. Rastgele olarak üretilen anahtarlar silinmiş olsa da, bu şifreleme anahtarlarını yeniden oluşturmak için kullanılan asal sayılar, sisteminiz yeniden başlatıncaya kadar sistem belleğinden yani RAM'den silinmez. Ancak, zararlı yazılım bulaştıktan sonra sisteminizi yeniden başlatırsanız bu şans ortadan kalkmaktadır. Zararlı yazılım bulaştıktan sonra ekrana gelen mesajda, fidyenin ödenmesi ile anahtarın verileceği söylense de, yapılan uyarılara göre fidye ödenmemelidir. Bunun sebebi saldırıyı düzenleyenlerin iletişim yollarının kapatılması veya engellenmesidir.

9.3.2. Petya

27 Haziran 2017 günü Avrupa'da yayılmaya başlayan fidye yazılımı, Ukrayna kaynaklı başlayarak, ağırlıklı olarak Belçika, Brezilya, Almanya, Rusya ve A.B.D.'nin de dahil olduğu 64 farklı ülkede görülmüştür. Petya/Mischa/Petwrap/GoldenEye familyasına ait olduğu bilinen en güncel Petya fidye yazılımı solucan (worm) kapasitesine sahip olduğundan sıçranan ağlar arasında dolaşabilmektedir. "Ransom:Win32/Petya" imzalı zararlı program ile benzer kodlara sahip olduğu anlaşıldıktan sonra Petya'nın yeni bir varyasyonu olduğu tespit edilmiştir. Ancak bu yeni varyasyon daha sofistike bir fidye yazılımıdır. Petya zararlı fidye yazılımının dosya bilgileri aşağıda verilmiştir.

SHA256 Hash değeri:

027cc450ef5f8c5f653329641ec1fed91f694e0d229928963b30f-6b0d7d3a745

MD5 Hash değeri: da2b0b17905e8afae0eaca35e831be9e

Dosya boyutu: 353.9 KB

Yayılmaya başlama tarihi: 27.06.2017

Bazı anti-virüs firmalarının isimlendirmeleri:

- Trojan.Ransom.Goldeneye.B
- Trojan.Ransom.Petya
- Win32/Diskcoder.C
- Win32/Petya

Hedef alınan sistem: Intel 386 ve sonraki işlemcileri kullanan Windows işletim sistemleri.

Dosya uzantısı: DLL (Win32 DLL)

İncelenin dosyanın derlenme tarihi: 18.06.2017

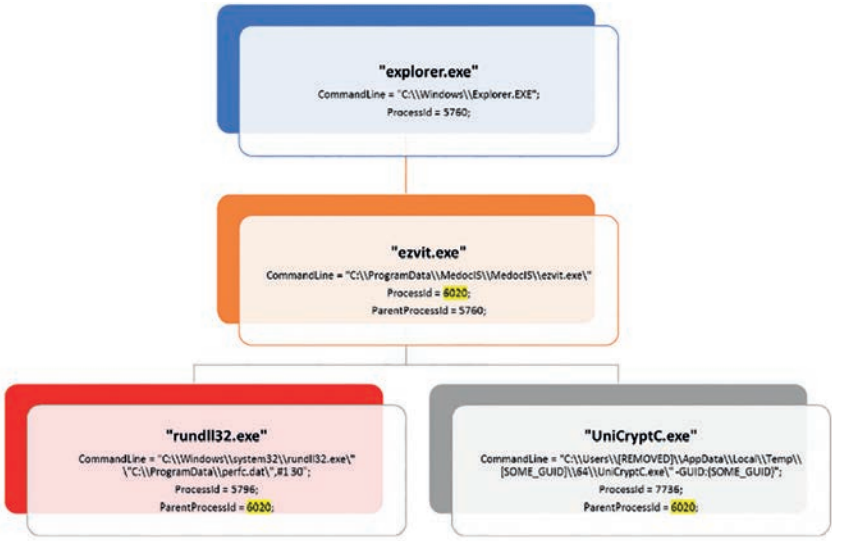
Kullandığı (Import) DLL dosyaları:

- ADVAPl32.dll
- CRYPT32.dll
- DHCPSAPI.dll
- IPHLPAPI.dll
- KERNEL32.dll
- MPR.dll

- NETAPl32.dll
- SHELL32.dll
- SHLWAPI.dll
- USER32.dll
- WS2_32.dll
- msvcrt.dll
- OLE32.dll

İlk etapta bilinen bir Microsoft Office zafiyetini kullanarak sistemi ele geçiren zararlı makro virüsüne sahip bir Excel dosyası ile bulaşmış olduğu düşünülen en yeni Petya sürümü, yapılan en son incelemeleri takiben Ukrayna kaynaklı olan sıçrama sürecinin bir yazılım tedarik-zinciri kaynaklı olduğu tespit edilmiştir. Ukrayna merkezli bir firmanın geliştirmiş olduğu vergi muhasebesi programına (MEDoc olarak bilinmektedir) ait bir yazılım güncelleme sürecinde zararlı program (bilindiği hali ile Petya v2) olan fidye yazılımını kullanıcı bilgisayarında yayınlayarak süreci Ukrayna'dan başlatmıştır. MEDoc yazılımının, Ukrayna'da bulunan tüm çalışma sahalarında ve ofislerde zorunlu olarak kurulu olduğu bilinmektedir. Vergi yönetimini kolaylaştırmak adına böyle bir regülasyonun olduğu tahmin edilmektedir. Olayla alakalı MEDoc firması "Sunucularımız bir virüs saldırısında bulunmuştur. Verdiğimiz rahatsızlıktan dolayı özür dileriz." şeklinde bir açıklamada bulunmuş ancak olayın yayılması ardından açıklamayı geri çekmişlerdir. Birbirinden ayrı ağlar bile olsa bu tedarik zinciri talebi ile öncel olarak ağlara yerleşebilen kötücül yazılım, kurtçuk (worm) özelliğini kullanarak bilinen zafiyetle (MS17-010, token taklidi, hesap ele geçirme vb.) ulaşabildiği kadar ağa ulaşmış ve bunun sonucunda dünya üzerinde 64 ülke etkilenmiştir. Bu başarı, ağlarda EternalBlue exploitine karşı hala yama yapılmamış çok sayıda sistemin bulunduğunu göstermektedir. Şekil 9.3'de de verildiği gibi MEDoc yazılımı güncelleme işleminin (*EzVit.exe),* 27 Haziran Salı günü Petya saldırı basamaklarında geçen zararlı bir komut istemi satırı çalıştırdığı tespit edilmiştir.

Fidye yazılımının kurulumu ile sonlanan işlem ağacı, MEDoc'un "*EzVit.exe"* işleminin bu komutu çalıştırmış olduğunu kanıtlar niteliktedir.



Şekil 9.3. MEDoc yazılımının güncelleme (*EzVit.exe)* işlem ağacı

Bilinen fidye yazılımlarından daha sofistike olduğunu kanıtlayan Petya zararlı yazılımının özelliklerinden birisi de daha fazla yayılma kapasitesi kullanmasıdır. Bu teknikler:

- Hesap bilgileri çalma ya da sistem üzerindeki aktif oturumları taklit etme
- Yanlış konfigürasyonlu ve aynı ağda bulunan dosya paylaşımlarına transfer yöntemi ve
- Hali hazırda exploitleri bulunan SMB zafiyetleridir.

Mimikatz benzeri hem 32 hem de 64 bitlik varyasyonlarda gelen bir hesap bilgileri döküm aracı (credential dumping tool) kullanıldığı görülmüştür. Genelde sistemlerde oturumu kullanıcılar tarafından aktif bırakılmış admin yetkili hesaplar bulunmasının kolay olmasından dolayı bu tarz araçlar herhangi bir exploit ile girilen Windows işletim sistemlerindeki hesap bilgilerini kullanarak ağ üzerinde daha fazla makineye sıçramayı hedeflemektedir.

Doğru hesap bilgilerini bulduktan sonra yerel ağları TCP/139 ve TCP/445 portları için taramaktadır. Tespit edilen makinelere ele geçirilen hesap bilgileri ile gerçekleştirilen saldırı başlangıcında bilin-

dik dosya-iletim teknikleri ile kurban makineye bir binary dosyası kopyalamaktadır. Daha sonra psexec ya da wmic gibi yarı doğal (semi-native) ve doğal (native) araçlar kullanılarak uzaktaki sistemde kod çalıştırmayı hedeflemektedir.

Fidye yazılımı uzak paylaşımları bulmak için Windows Management Instrumentation Command-Line'ın (WMIC) NetEnum ya da NetAdd gibi fonksiyonlarını kullanarak kendisini ortak paylaşım alanına kopyalayabilmektedir.

Herkese açık olmayan paylaşımlara erişim sağlayabilmek adına da ele geçirilmiş hesap bilgilerini kullanır ya da ele geçirilmiş sistemde giriş yapmış kullanıcılar, tokenlar ile taklit edilerek dosya paylaşımlarına ulaşabilmektedir.

Bir başka sıçrama opsiyonu da Windows ürünlerinde yakın zamanda ortaya çıkan birden fazla SMB zafiyetini istismar ederek ağ üzerinde yayılmaya çalışmaktır. CVE-2017-0144 ve CVE-2017-0145 kodlu MS17-010 bullet'ine ait olan zafiyetler (sırasıyla EternalBlue ve EternalRomance olarak da bilinmektedir.) Microsoft Vista SP2, Windows Server 2008 SP2 ve R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold ve R2, Windows RT 8.1 ve Windows 10 Gold ürünlerini etkilemektedir.

Shadowbrokers tarafından 14 Nisan 2017 tarihinde NSA tarafından kullanıldığı iddia edilen fuzzbunch isimli bir hack framework'ü yayınlanmış ve bu framework'e dahil istismar kodları arasında MS17-010'u tetikleyebilen EternalBlue ve EternalRomance isimli iki adet istismar kodu da olduğu görülmüştür. Fidye yazılımı bu kodları içermekte ve zafiyetli sistem tespit ettiğinde bunları kullanarak sisteme sıçramaktadır.

Bu SMB zafiyetinin etkilediği tüm sürümleri için istismar kodu bu yayınlanan altyapıda bulunmamakla birlikte EternalBlue ile Windows 7 SP1 ve Windows 2008 R2 SP1, EternalRomance ile de Windows XP, Windows 2003, Windows Vista, Windows 7, Windows 8, Windows 2008, Windows 2008 R2 sistemleri ele geçirilebilmektedir. Microsoft'un bu zafiyetleri düzeltme tarihi 14 Mart 2017'dir. Yamalı sistemler, fidye yazılımın bu yayılma metodundan etkilenmemektedirler.

Şifreleme aksiyonları zararlı yazılımın sistem üzerindeki yetki seviyesine ve sistem üzerinde bulunan çalışan işlemlere göre farklılık göstermektedir. Çalışan işlemleri kullanma şekli ise isimlerini basit bir algoritma ile hashleyerek kod içerisinde karşılaştırmalar yapması ve aksiyona bu şekilde karar vermesidir:

- 0x6403527E ya da 0x651B3005 gibi hashler işlem isimleri hashleri arasında bulunuyorsa, yazılım ağ üzerinde herhangi bir aksiyon gerçekleştirmeyecektir.
- Başka bir örnek olarak eğer 0x2E214B44 hashi işlem hashleri arasında bulunuyorsa, fidye yazılımı sabit diskin ilk 10 sektörünü (MBR de dahil) silmektedir.

Eğer zararlı yazılım sistem üzerinde en yüksek yetki ile çalışıyorsa ve yukarıda bahsedilmiş kontrolleri de olumlu ise MBR kodunu şifrelenmiş MBR ile değiştirecektir. MBR değişiminden sonra sisteme lokal saat + 10 dakikaya yeniden başlatacak bir görev zamanlandırma komutu göndermektedir. MBR değiştirilmişse, sistem yeni başlatılmasından sonra kullanıcı sahte bir sistem mesajı ile karşılaşmaktadır. Windows native CHKDSK aracının disk üzerinde tamir işlemi yaptığını belirten sahte ekran görülmektedir. Eğer zararlı yazılım sistem üzerinde en yüksek yetki ile çalışmıyorsa sistem üzerinde C:\Windows hariç tüm klasörlerin içerisindeki uzantılara sahip dosyaları şifreleyecektir.

Kod üzerinde ReadFile() / WriteFile() kütüphanelerinden ziyade dosyaları haritalayan kütüphaneler bulunmuştur. Birçok fidye yazılımının aksine NotPetya şifreleme işlemi, dosyalara yeni bir dosya uzantısı eklememekte, dosyanın kendisinin üzerine şifrelenmiş halini yeniden yazmaktadır. Makineler üzerinde bulunan her sabit disk için bir AES anahtarı oluşturulmakta ve kod içerisine gömülü 2048 bitlik public anahtar ile şifrelenerek dışa alınmaktadır. Düşük yetki ile çalıştığı takdirde şifreleme işlemi esnasında MBR'ı değiştiremiyor dahi olsa sistem sabit diski üzerinde kritik sektörleri yok etmeye çalışmaktadır. Tüm işlemler bittiğinde fiziksel disk başına oluşturulmuş AES anahtarının da 'kurulum anahtarı' olarak bahsedildiği bir README.TXT oluşturulmaktadır.

Ayrıca program sistem üzerindeki, System, Setup, Security, Application olay günlüklerini temizlemekte ve NTFS günlük bilgilerini de silmektedir.

Ağ güvenliğinden sorumlu kişiler aşağıdaki maddeler halinde verilen göstergelerden yararlanarak zararlı hareket tespitinde bulunabilirler.

1) Dosya ibareleri:
   - 34f917aaba5684fbe56d3c57d48ef2a1aa7cf06d
   - 9717cfdc2d023812dbc84a941674eb23a2a8ef06
   - 38e2855e11e353cedf9a8a4f2f2747f1c5c07fcf
   - 56c03d8e43f50568741704aee482704a4f5005ad
2) Komut istemi ibareleri: Komut istemi loglarının tutulduğu ortamlarda aşağıdaki komut satırları aranabilir:
   - Zamanlanmış Yeniden Başlatma Görevi:

     NotPetya lokal zaman + 10 ila 60 dakika arasında rastgele bir zaman kullanarak yeniden başlatma zamanlamaktadır.

     schtasks /Create /SC once /TN "" /TR "sistem32yolu\shutdown.exe /r /f" /ST <zaman>

     cmd.exe /c schtasks /RU "SYSTEM" /Create /SC once /TN "" /TR "sistem32yolu\shutdown.exe /r /f" /ST <zaman>
   - Yayılma Hareketi:

     "process call create
     \"C:\\Windows\\System32\\rundll32.exe
     \\\"C:\\Windows\\perfc.dat\\\" #1"
3) Ağ ibareleri;
   - Workstationlar kendi subnetleri üzerinde (/24 kapsamında) TCP/139 ve TCP/445 port taramalarında bulunuyorsa,
   - Sunucular (spesifik olarak Etki Alanı Denetleyicileri) birçok subnet üzerinde (/24 kapsamında) TCP/139 ve TCP/445 port taramalarında bulunuyorsa,
4) Engellenmesi gereken şüpheli IP adresleri:
   - 185.165.29.78
   - 84.200.16.242
   - 111.90.139.247
   - 95.141.115.108
   - 169.239.181.127

1990 yılından günümüze kadar gerçekleşmiş olan fidye saldırılarının sınıflandırılması için birçok çalışma yapılmıştır. Gerçekleştirilen çalışmalarda fidye saldırılarının çeşitli yaklaşımları ve başarı ölçüleri göz önüne alınarak değişen metodolojiler kullanılmıştır. Etki bırakmış önemli fidye saldırıları anahtar karakteristiği (key characteristics) yaklaşımıyla sınıflandırılmıştır [21]. Anahtar karakteristiği yaklaşımı;

- Bulaşma yöntemi
- Dosya formatı
- Platform
- Dosya şifreleme metodu
- Oturum anahtarını şifreleme yaklaşımı
- Şifreleme lokasyonu
- Yedeklerin silinip, silinmediği
- Komuta & kontrol sunucuları ile iletişimi
- Çözümleme servisinin lokasyonu
- Fidye ödemesini alma yaklaşımı
- İletişim kurulan dil
- Pasif ve aktif yaklaşımlarla kendini koruma yöntemleri

başlıklarında sınıflandırma yapılan bir yaklaşımdır.

Farklı özellikleri nedeniyle fidye yazılımları denilince akla gelen 13 farklı fidye saldırısı, 12 temel ayırt edici unsur özelinde sınıflandırılmıştır. Gerçekleştirilen sınıflandırmalar, saldırıların birbirinden etkilendiğini ortaya koymaktadır. Fidye saldırılarında iz kaybettirme, minimum risk alma, ödeme yöntemlerini çeşitlendirme, önemli dosyaları şifrelemek için farklı yaklaşımlar geliştirme ve daha fazla mağdura erişebilme her zaman amaçlanan sonuçlardandır. Özellikle dönemsel olarak gerçekleştirilen fidye saldırılarının teknik yaklaşım olarak kendini geliştirdiği söylenebilir.

9.4. Fidye Yazılımlarından Korunma ve Alınması Gereken Önlemler

Fidye saldırıları her geçen yıl etkisini ve önemini arttırarak devam ettiren siber saldırılar arasında yer almaktadır. Fidye saldırıları başlangıçta insanların zafiyetlerinden yararlanarak bulaşma yöntem-

lerini kullanmışlardır. Fidye yazılımları gibi küresel çapta yapılan siber saldırılar karşısında alınması gereken önlemler hem son kullanıcıları hem de kurumları ilgilendirmektedir.

WannaCry saldırısı ile beraber saldırılar sıfırıncı gün (Zero Day exploit) açıkları ile gerçekleştirildiği için bireysel bazda alınacak önlemler ile engellenmesi neredeyse imkânsızdır. Bu saldırılarda bireysel olarak alınacak önlemler değerli olmakla birlikte, kurumlarının birçok farklı alanda önlem alması daha çok önem arz etmektedir. Fakat asıl alınması gereken önlemler geniş kapsamlı, sistematik ve periyodik olmalıdır.

Bu kitabın 8. Bölümünde fidye yazılımlarından korunulması için yapılması gerekenler verildiği için burada bu hususlara değinilmemiştir. Bunun yerine, daha kapsamlı bir bakış açısı ile fidye yazılımlarından korunmak için daha üst seviyede yapılması gereken hususlara yer verilmiştir. Burada verilen hususların 6 Temmuz 2019'da yayımlanan CB Genelgesinde belirtilen pek çok hususu kapsadığı görülebilir. Bunlar;

- Her kurum önemli belgelerini internet bağlantısı olmayan, en az iki katmanlı güvenlik önlemleri içeren kapalı sistemlerde tutmalıdır.
- Her dosya birbiri ile aynı ağda olmayan ve kesinlikle fiziksel bağlantısı bulunmayan ayrı sunucularda yedekli olarak tutulmalıdır.
- Personelin sosyal mühendislik saldırıları başta olmak üzere, gerçekleşebilecek genel siber saldırılara karşı eğitim alması sağlanmalıdır.
- Belirli periyotlarla kurum içerisinde oluşturulacak bir ekip tarafından ve/veya bir firmadan hizmet alımı şeklinde, bütün personele sosyal mühendislik saldırıları gerçekleştirilmeli, oluşacak sorunlara yönelik önlemler alınmalıdır.
- Kurumda kullanılan sistem ve aygıtların tümünün güvenlik testlerinden geçirilmesi ve güncelliğinin kontrol edilmesi gerekmektedir. Bu kontrol en azından yılda bir kaç kez yapılmalı, mümkünse haftada en az bir kez yapılarak sürekli güncel kalma sağlanmalıdır.
- Kurumlarda mümkün oldukça farklı işletim sistemi ve yazılımlar kullanılmalı, birbirini yedekleyecek şekilde farklı donanım ve yazılımlarla sistemler olası saldırılardan korunmalıdır.
- Fidye yazılımları aynı ağı kullanan diğer cihazlara da yayılabildiğinden dolayı, kurumlarda kullanılan iç ağlarda doğru konfügürasyon ayarları girilerek, farklı aygıtlar ve kullanıcılar arasında

dosyalara erişim, değiştirme veya şifreleme gibi işlemlerin kısıtlanması ve onay mekanizmasına sunulması gerekmektedir.

- Siber olayları izleyebilecek, analiz edebilecek ve acil durum planları üretebilecek merkezlerin kurulması gereklidir.
- Hali hazırda USOM tarafından gerçekleştirilen SOME yapılarına ait sistemlerin kısa periyotlar ile etkin bir şekilde denetlenmesi, güvenlik testlerine tabi tutulması ve SOME personelinin teknik kapasitesinin test edilerek ihtiyaç hallerinde eğitim verilmesi çalışmalarının daha aktif yapılmasının faydalı olacağı öngörülmektedir.

9.5. Değerlendirmeler

WannaCry ve Petya fidye yazılımları, metodolojileri ve korunma yöntemlerine ait literatürde yeteri kadar akademik çalışma bulunmamaktadır. Bu saldırılara ait çalışmalara daha çok karanlık (dark) ve derin webte, bloglarda, güvenlik şirketlerinin web sayfalarında rastlanmaktadır. Bu tür çalışmaların günlük hayata kazandırılması, tehlikelerin boyutunun daha iyi anlaşılmasını sağlayacaktır.

Ülkemizde zararlı yazılım analizi alanında yapılan çalışmaların çok kısıtlı olduğu, haber ve duyurulardan öte gitmediği, bu saldırıları analiz edebilecek yeterli bilgi birikimi ve deneyime sahip olunmadığı, akademik camianın konuya ilgisiz olduğu görülmüştür. Ülke bilgi birikimi ve yeteneğinin arttırılmasına yönelik çalışmalar yapılmalıdır.

Fidye yazılımları gibi siber saldırılara karşı ülkemizde alınan önlemlerin artan tehdit vektörleri dikkate alındığında yeterli olmadığı ve buna uygun çözümler geliştirilmediği görülmüştür. Bunlar artırmalı veya geliştirilmelidir.

Ülkemizde fidye yazılımlarına karşı alınması gereken önlemlere yönelik eğitimlerin yeterli düzeyde olmadığı görülmüştür. Fidye yazılım metodolojilerini anlama, dinamik ve statik incelemeleri bilme ve karşı çözümler geliştirme konusunda siber güvenlik uzmanı yetiştirmesine yönelik daha yoğun çalışmalar yapılmalıdır.

Değişimin ve gelişimin çok hızlı olduğu günümüz siber dünyasında, gerçekleşen siber saldırılara karşı önlem almanın yanında, gerçekleşecek çok yönlü saldırıları önlemek ve gelecek yıllarda karşılaşılabilecek yeni tehdit vektörlerine hazırlıklı olabilmek adına Ulusal Siber Stratejilerin doğru tanımlanması ve etkin bir şekilde uygulanması gerekmektedir.

Kaynaklar

[1] Hampton, N. and Baig, Z. A. (2015). Ransomware: Emergence of the cyber-extortion menace. Australian Information Security Management Conference, Australia, 47-56.

[2] Salvi, M. H. U. and Kerkar, M. R. V. (2016). Ransomware: A cyber extortion. UGC Approved List of Journals, 2(2), 12-15.

[3] Richardson, R. and North, M. (2017). Ransomware: Evolution, Mitigation and Prevention, Management International Review, 13(1), 10-14.

[4] Kharraz, A., Robertson, W., Balzarotti, D., Bilge, L. and Kirda, E. (2015). Cutting the gordian knot: A look under the hood of ransomware attacks. In International Conference on Detection of Intrusions and Malware and Vulnerability Assessment, Switzerland, 3–24.

[5] Wyke, J. and Ajjan, A. (2015). The current state of ransomware. SophosLabs Technical Paper, 3-38.

[6] İnternet: Savage, K., Coogan, P. and Lau, H. (2015). The evolution of ransomware. URL: http://www.webcitation.org/query?url=http%3A%2F%2Fwww.symantec.com%2Fcontent%2Fen%2Fus%2Fenterprise%2Fmedia%2Fsecurity_response%2Fwhitepapers%2Fthe-evolution-of-ransomware.pdf+&date=2018-09-04, Son Erişim Tarihi: 18.07.2018

[7] İnternet: (2015). FBI Public Service Announcement, Criminals Continue to Defraud and Extort Funds from Victims Using CryptoWall Ransomware Schemes Alert Number: I-062315-PSA. URL: http://www.webcitation.org/query?url=https%3A%2F%2Fwww.ic3.gov%2Fmedia%2F2015%2F150623.aspx&date=2018-09-06 Son Erişim Tarihi: 18.07.2018

[8] İnternet: Panda Security, Doxware, the Scary New Evolution of Digital Hijacking. URL: http://www.webcitation.org/query?url=http%3A%2F%2Fwww.pandasecurity.com%2Fmediacenter%2Fsecurity%2Fdoxware-evolution-digital-hijacking+&date=2018-09-06 Son Erişim Tarihi: 18.07.2018.

[9] Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. URL: http://www.webcitation.org/query?url=https%3A%2F%2Fbitcoin.org%2Fbitcoin.pdf&date=2018-09-06 Son Erişim Tarihi: 18.07.2018.

[10] İnternet: Abrams, L. (2018). Bleeping Computer, 'Star Trek Themed Kirk Ransomware Brings us Monero and a Spock Decryptor!. URL: http://www.webcitation.org/query?url=https%3A%2F%2Fwww.bleepingcomputer.com%2Fnews%2Fsecurity%2Fstar-trek-themedkirk-ransomware-brings-us-monero-and-a-spock-decryptor%2F&date=2018-07-18, Son Erişim Tarihi: 18.07.2018

[11] Qinyu, L. (2008). Ransomware: a growing threat to SMEs. Housten: Southwest Decision Science Institutes, 360-366

[12] Adamov, A. and Carlsson, A. (2017). The State of Ransomware. Trends and Mitigation Techniques. East-West Design & Test Symposium (EWDTS), Novi Sad, Serbia.

[13] İnternet: Richet, J. L. (2016). Extortion on the internet: the Rise of Crypto-Ransomware. Semanticscholar, URL: http://www.webcitation.org/query?url=https%3A%2F%2Fpdfs.semanticscholar.org%2Fa21a%2Faf1ef6b142556212f4027+9b745cf70db55ca.pdf+++&date=2018-09-06 Son Erişim Tarihi: 18.07.2018

[14] İnternet: WannaCry ransomware used in widespread attacks all over the world. URL: http://www.webcitation.org/query?url=https%3A%2F%2Fsecurelist.com%2FWannaCry-ransomware-used-in-widespread-attacks-all-over-the-world%2F78351&date=2018-07-18 Son Erişim Tarihi: 18.07.2018

[15] İnternet: Sophos. (2015). The current state of ransomware: CTB-Locker. URL: http://www.webcitation.org/query?url=https%3A%2F%2Fnews.sophos.com%2Fen-us%2F2015%2F12%2F31%2F+the-current-state-of-ransomware-ctb-locker+&date=2018-07-18 Son Erişim Tarihi: 18.07.2018

[16] İnternet: Panda Security. (2015). CryptoLocker: What Is and How to Avoid it. URL: http://www.webcitation.org/query?url=http%3A%2F%2Fwww.pandasecurity.com%2Fmediacenter%2F+malware%2Fcryptolocker+&date=2018-07-18 Son Erişim Tarihi: 18.07.2018

[17] Sittig, D. F. and Hardeep, S. (2016). A socio-technical approach to preventing, mitigating, and recovering from ransomware attacks. Applied Clinical Informatics, 7(2), 624.

[18] Internet: Security Threat Report. (2016). URL: http://www.webcitation.org/query?url=https%3A%2F%2Fwww.symantec.com%2Fcontent%2F+dam%2Fsymantec%2Fdocs%2Freports%2Fistr-21-2016-en.pdf&date=2018-07-18 Son Erişim Tarihi: 18.07.2018.

[19] Gallegos-Segovia, P. L., Bravo-torres, J. F., Larios-Rosillo, V. M., Vintimilla-Tapia, P. E., Yuquilima-Albarado, I. F., Jara-Saltos, J. D. (2017). Social Engineering as an Attack Vector for Ransomware, Electrical, electronics engineering, information and communication technologies (Chilecon), Pucon, Chile.

[20] Shaikh, A. N., Shabut, A. M. and Hossain, M. (2016). A literature review on phishing crime, prevention review and investigation of gaps. In Software, Knowledge, Information Management & Applications (SKIMA), 9–15.

[21] Andronio, N., Zanero, S. and Maggi, F. (2015). Heldroid: Dissecting and detecting mobile ransomware. In International Workshop on Recent Advances in Intrusion Detection, Springer, 382–404.

[22] Mercaldo, F., Nardone, V., Santone, A. and Visaggio, C. A. (2016). Ransomware steals your phone. formal methods rescue it. In International Conference on Formal Techniques for Distributed Objects, Components, and Systems. Springer, 212–221.

[23] Kharraz, A., Arshad, S., Mulliner, C., Robertson, W. K. and Kirda, E. (2016). Unveil: A large-scale, automated approach to detecting ransomware. In USENIX Security Symposium, Austin, 757–772.

[24] İnternet: Sophos. (2015). The current state of ransomware: CTB-Locker. URL: http://www.webcitation.org/query?url=https%3A%2F%2Fnews.sophos.com%2Fen-us%2F2015%2F12%2F31%2F+the-current-state-of-ransomware-ctb-locker+&date=2018-07-18 Son Erişim Tarihi: 18.07.2018

[25] İnternet: Barker, E. and Kelsey, J. (2012). Recommendation for random number generation using deterministic random bit generators. URL: http://www.webcitation.org/query?url=https%3A%2F%2Fwww.nist.gov%2Fpublications%2Frecommendation-random-number-generation-using-deterministic-random-bit-generators-2&date=2018-09-06 18 Son Erişim Tarihi: 18.07.2018.

[26] Moser, A., Kruegel, C. and Kirda, E. (2007). Limits of static analysis for malware detection. Paper presented at the Computer Security Applications Conference, Beach, United States.

[27] Klieber, W., Flynn, L., Bhosale, A., Jia, L. and Baner, L. (2014). Android Taint Flow Analysis for App Sets. ACM SIGPLAN conference on Programming Language Design and Implementation, 16.

[28] Zhou, Y., Wang, Z., Zhou, W., and Jiang, X. (2012, February). Hey, you, get off of my market: detecting malicious apps in official and alternative android markets. National Down Syndrome Society, 25(4), 4, 50-52.

[29] Lindorfer, M., Neugschwandtner, M. and Platzer, C. (2015). Marvin: Efficient and comprehensive mobile app classification through static and dynamic analysis. Paper presented at the Computer Software and Applications Conference, Taichung, Taiwan.

[30] Hasan, M. M., and Rahman, M. M. (2017). RansHunt a support vector machines based ransomware analysis framework with integrated feature set. Paper presented at the 20th International Conference of Computer and Information Technology (ICCIT), Dhaka, Bangladesh

[31] Kolter J. Z. and Maloof. M. A. (2006). Learning to detect and classify malicious executables in the wild. The Journal of Machine Learning Research, 7, 2721–2744.

[32] Kharaz, A. (2016). Unveil: A large-scale, automated approach to detecting ransomware. Paper presented at the 25th USENIX Security Symposium (USENIX Security16), (Austin, TX), 757–772, Austin.

[33] Chen, Q. and Bridges, R. A. (2017). Automated behavioral analysis of malware: A case study of wannacry ransomware. machine learning and applications (ICMLA). 2017 Paper presented at the 16th IEEE International Conference, Cancun, Mexico.

[34] Krzysztof, C. (2015). Network activity analysis of CryptoWall ransomware. Przeglad Elektrotechniczny, 91(11), 201-204.

[35] Martin, G., Kinross, J. and Hankin, C. (2017). Effective cybersecurity is fundamental to patient safety. Paper presented at the 2018 The Institute of Electrical and Electronics Engineers Global Engineering Education Conference, Tenerife, Spain.

[36] Ehrenfeld, J. M. (2017). WannaCry, cybersecurity and health information technology: A time to act. Journal of Medical Systems, 41(7), 104.

[37] Kim, D., Choi, G., Lee, J. (2018, Jan). White list-based ransomware real-time detection and prevention for user device protection. Consumer Electronics (ICCE), 2018 IEEE International Conference, Las Vegas.

[38] Mohurle, S. and Manisha, P. (2017). A brief study of wannacry threat: Ransomware attack 2017. International Journal, 8(5), 1938-1940.

[39] İnternet: URL: http://www.webcitation.org/query?url=http%3A%2F%2Fdirectory v6plzm.onion&date=2018-07-18 Son Erişim Tarihi: 18.07.2018.

[40] İnternet: URL: http://www.webcitation.org/query?url=http%3A%2F%2Franionjgot5 cud3p.onion&date=2018-07-18 Son Erişim Tarihi: 18.07.2018.

[41] İnternet:URL:http://www.webcitation.org/query?url=http%3A%2F%2Fxmh57jrz nw6insl.onion&date=2018-07-18 Son Erişim Tarihi: 18.07.2018.

[42] İnternet:URL:http://www.webcitation.org/query?url=http%3A%2F%2Fhss3uro 2hsxfogfq.onion&date=2018-07-18 Son Erişim Tarihi: 18.07.2018.

[43] İnternet:URL:http://www.webcitation.org/query?url=http%3A%2F%2 Fraasbrrypzkuj5cy.onion%2F%3Fref%3Ddarkdir&date=2018-07-18 Son Erişim Tarihi: 18.07.2018.

[44] İnternet:URL:http://www.webcitation.org/query?url=http%3A%2F%2 Fanswertedhctbek.onion&date= 2018-07-18 Son Erişim Tarihi: 18.07.2018

[45] Burak Özçakmak', "WannaCry ve Petya Fidye Yazılımlarının Analizi ve Korunma Yöntemleri", Gazi Üniversitesi Fen Bilimleri Enstitüsü, Bilgi Güvenliği Mühendisliği ABD Yüksek Lisans Tezi, 2018, Ankara.

Siber Para

BÖLÜM 10

Dr. Eyüp Burak CEYHAN
Dr. İsmail Fatih CEYHAN
Dr. Onur ÇAKIRGÖZ

SİBER PARA

Bu bölümde; öncelikle paranın tarih içinde geçirdiği dönüşüm anlatılmış, daha sonra kripto para tanıtılmış, ardından en çok işlem gören ilk üç sanal para hakkında bilgi verilmiştir. Dördüncü başlıkta sanal paranın özellikleri ve normal paraya göre üstünlükleri aktarılarak sanal paranın kullanımı ve ülkelerin konuya yaklaşımları sunulmuştur. Altıncı başlıkta blokzincir tanıtılarak blokzincir sistemindeki potansiyel riskler üzerinde durulmuş, sonraki başlıkta blokzincir sistemlerine yapılmış saldırılara örnekler verilmiştir. Sekizinci başlıkta blokzincirde güvenlik geliştirmeleri örnekleri verilmiş, dokuzuncu başlıkta sanal para ile siber güvenlik arasındaki ilişkiler aktarılmış ve son başlıkta ise değerlendirmeler yapılarak çalışma sonuçlandırılmıştır.

10.1. Paranın Tarihçesi

Paradan önce mal ve hizmetler değiş tokuş işlemi ile edinilmekteyken, daha sonra paranın ortaya çıkmasıyla mal ve hizmetlerin değişim aracı olarak para kullanılmaya başlanmıştır. Paranın değişim aracı olma, değer ölçütü olma ve değer saklama işlevleri bulunmaktadır. Ekonomide yakın geçmişe kadar sadece madeni ve banknot para birimleri varken, daha sonra vadesiz mevduatlar ve kredi kartları da para gibi kullanılmaya başlanmıştır. Son yıllarda ortaya çıkan Bitcoin ise, elektronik ödemeler dahil olmak üzere sanal bir para biriminin kullanımını kolaylaştıran çevrimiçi bir iletişim protokolüdür. İşlemleri herhangi bir tek sunucuda veya bir dizi sunucuda saklamak yerine, Bitcoin'e katılan bilgisayarlardan oluşan bir ağa dağıtılmış işlemler üzerine kuruludur [1]. Tarihsel sıralamayla değerlendirildiğinde para çeşitleri aşağıdaki gibi sınıflandırılabilir [2]:

- **Emtia Para:** Emtia para, değeri yapıldığı üründen kaynaklanan paralara denmektedir. En yaygın kabul gören emtia para çeşidi

altın ve gümüştür. M.Ö. 7. yüzyılda, günümüzdeki anlamına en yakın altın parayı (sikke) Lidyalılar basmış ve kullanmışlardır.

- **Temsili Para:** Değerli metallerin para olarak kullanımında zamanla ortaya çıkan birçok zorluktan dolayı, zaman içerisinde emtia para sistemi altına dayalı temsili para sistemine dönüşmüştür. 10. yüzyılda Çin'de Song Hanedanlığı döneminde basılmış olan "Jiaozi", tarihteki ilk banknottur ve Avrupa'ya geçişi yaklaşık altı yüzyıl sonrasında olmuştur.
- **İtibari Para:** Şekil açısından temsili paralara benzeyen ancak altın veya gümüşe dayalı olmayan itibari paralar 1944'te Bretton Woods anlaşmasıyla ortaya çıkmış, böylece Amerikan Doları başlangıçta altına bağlanmış, diğer ülkelerin paraları ise dolara göre ayarlanmıştır. Daha sonra Amerikan Dolarının altın karşılığı olmadan basılmasına karar verilmiştir.
- **Özel Para:** Kanada'daki Canadian Tire, ABD'nin Massachusetts eyaletinde kullanılan BerkShare ve İngiltere'deki Bristol Pound gibi genellikle yerel yönetimlerde ortaya çıkan alternatif para birimleri, ülke içerisinde merkezi otoritenin bastığı paraya alternatif olarak kullanılan özel para birimleridir.
- **Dijital Para:** Elektronik olarak saklanan ve transfer edilebilen paralardır. Elektronik ödemenin ilk örnekleri arasında, Hollanda'da gece yakıt alan kamyon şoförlerini ve benzin istasyonlarını hırsızlığa karşı korumak için tasarlanan akıllı kartlara para yükleyerek, bu paralarla yakıt alınabilmesi gösterilebilir.
- **Sanal Para:** Herhangi bir merkez bankası, kredi kuruluşu veya e-para kuruluşu tarafından ihraç edilmediği halde, dijital paraya benzeyen ancak kağıt parayı temsil etmeyen sanal paralar ortaya çıkmıştır.
- **Kripto-Para:** Son yıllarda kriptografik/şifreli oldukları için güvenli işlem yapmaya ve ek sanal para arzına olanak sağlayan kripto-paralar hem alternatif para birimi ve dijitaldirler hem de sanal paradırlar.

10.2. Kripto Para

Crypto ve currency kelimelerinin birlikte kullanılmasıyla ortaya çıkan cryptocurrency kelimesi kripto (şifreli) para manasına gelir.

İnternet üzerinde kullanılan, hiçbir merkezi otoriteye ya da aracı kuruma bağlı olmayan kripto para; bir tür sanal para birimini ifade eder. Kripto paralar sadece belirlenen şifrelerin kullanımıyla bulunduğu sanal cüzdanlardan, yine şifreler ile çıkarılıp kullanılabildiği için bu ismi taşırlar. Kripto para birimleriyle gerçek ya da tüzel kişiler, aynen piyasadaki nakit parayla yaptıkları gibi harcama ya da satış yapabilir [3].

Şekil 10.1. Kripto Paranın Aralık 2017 - Ağustos 2018 Tarih Aralığındaki Toplam Piyasa Değeri [11]

Bitcoin gibi kripto para birimlerinin işleyişi, sonuçta katılımcıların bilgileri açık bir şekilde ifşa etme veya gizleme konusundaki anlaşmalarına dayanır. Çeşitli argümanlar, bu anlaşmaların, tüm katılımcıların taraf olduğu geniş bir "çok taraflı sözleşme" anlamına geldiğini ileri sürmektedir. Çok taraflı anlaşma akıllı sözleşme teknolojisi ile otomatik olarak uygulanır.

Akıllı sözleşmeler; önceden belirlenmiş ve dijital olarak kanıtlanmış olaylara bağlı kalarak, yasal olarak ilgili eylemleri başlatan, kontrol eden ve / veya belgeleyen ve koşullara göre yasal olarak bağlayıcı sözleşmelerin sonuçlandırılabileceği yazılım veya donanım olarak tanımlanabilir. Satış makineleri eski tip akıllı sözleşme teknolojisi uygulamasına örnek olarak gösterilebilir [3].

10.3. En Çok İşlem Gören Sanal Para Çeşitleri

Kripto paraların doğası değişim aracı olması bakımından çok uygun olmasına rağmen, paranın değer ifade etme ve hesap birimi

olma özelliklerinin en az birisi açısından aynı rolü tam olarak oynayamadığı görülmektedir.

Bitcoin'in başarısı, farklı niteliklere ve ekonomik özelliklere sahip benzer kripto paralar ortaya çıkmasına neden olmuştur ki, günümüzde 2500'e yakın kripto para çeşidi mevcuttur [7].

Alt başlıklarda kripto paralardan üçüne kısaca değinilecektir.

10.3.1. Bitcoin

2008 yılında, takma ismi Satoshi Nakamoto olan bir programcı, Bitcoin adlı bir dağıtılmış katılımcılar arası dijital nakit tasarımını ortaya çıkarmıştır. Bitcoin Ocak 2009'dan değişim kuru bit başına 0,000764 $'lık bir fiyatla listelenene kadar (Ekim 2009), değersiz paraları çıkartan kriptografi meraklıları arasında zaman zaman belirsiz bir deneysel faaliyet olarak kalmıştır. 22 Mayıs 2010 tarihinde, Bitcoin'in ilk gerçek işleminde, bitcoin başına 0,0025 dolarlık bir değişim işlevi gördüğü kaydedilmiştir. O zamandan itibaren, bitcoin ile 160 milyondan fazla işlem gerçekleşmiş, satın alma gücü 2017'de bitcoin başına yaklaşık 900$ seviyesine yükselmiş ve toplam ticarete konu olan para arzı 150 milyar dolar civarında bir piyasa değerine ulaşmıştır [12].

Bitcoin'in temel tekniği olan blockchain 2009 yılında ilk çıkışından itibaren umut verici bir uygulama beklentisi oluşturmakta ve akademi ve iş dünyasında çok dikkat çekmektedir. İlk kripto para birimi olan Bitcoin, 2015 yılında en yüksek performans gösteren para birimi ve 2016 yılında en iyi performans gösteren emtia olarak değerlendirilmiş olup, Mayıs 2017 itibariyle günlük 300.000'den fazla onaylanmış işleme sahiptir [5].

Bitcoin işleyiş olarak, tüm işlemleri yaklaşık 10 dakikada yeni bir bloğa kaydetmeye programlanmıştır. Ağın bir üyesi bir bloğun işlemlerini doğruladığında ve onunla ilişkili olan çalışma kanıtını çözdüğü zaman, yeni verilen bitcoinler ile ödüllendirilir. Temelde Bitcoin, doğru kayıtlara dönüştürmesi için, doğrulama konusunda elektrik ve işlem gücü kaynaklarını harcadıkları ölçüde üyelerini ödüllendiren bir teknolojidir. Ağ üyeleri çok sayıda işlemci ve elektrik gerektiren son derece karmaşık yineleme işleminde, birbirlerinin onaylarını doğrulamak ve işlemlerin geçerliliği için herhangi

bir üçüncü tarafın güvenilirliğine itimat etmek zorunda kalmadan anlaşmazlıkları bertaraf eden bir mülkiyet ve işlem defteri çıkarmak için işlem gücü harcarlar. Bitcoin %100 doğrulama ve %0 güven üzerine kurulmuştur.

İlk 210.000 blok için, onayladıkları her bir blokla üyelere verilen ödül 50 bitcoin iken. 28 Kasım 2012'den itibaren, 210.000 blok çıkarıldıktan sonra ödül, 25 bitcoin'e ve 9 Temmuz 2016'da, 210.000 blok daha çıkarıldıktan sonra ödül, blok başına 12,5 bitcoin'e indi. Ödül, yaklaşık olarak her dört yılda bir, coin 2140 yılında yok olana kadar art arda yarıya indirilecek şekilde programlanmıştır.

Bitcoin, elektronik ödemeler de dahil olmak üzere sanal para kullanımını kolaylaştıran çevrimiçi bir iletişim protokolüdür. Şubat 2019 itibariyle günlük işlem hacmi yaklaşık 17,5 milyon bitcoin (cari döviz kurlarında yaklaşık 7 milyar dolar) ve dolaşımdaki tüm bitcoinlerin toplam piyasa değeri yaklaşık 67 milyar dolardır [11]. Tablo 10.1, Mart 2015 itibariyle Bitcoin aktivitesini özetleyerek, yukarıdaki verilerle karşılaştırıldığında Bitcoin'in kısa süre içindeki değişimini gözler önüne sermektedir.

Tablo 10.1. Bitcoin Etkinliği [1]

Etkinlik	Miktar
Toplam basılan bitcoin	14 milyon
ABD doları karşılığı piyasa fiyatı	≈ 3,5 milyar
Ulaşılabilir Bitcoin düğümlerinin toplam sayısı	≈ 6.500
Toplam (kümülatif) işlem sayısı	≈ 62,5 milyon
Toplam kullanılan hesap sayısı	≈ 109 milyon
Blok zinciri boyutu	≈ 30,3 GB
Şu ana kadar blok sayısı	≈ 350.000
Tahmini günlük işlem hacmi	≈ 200.000 BTC (≈ 50 milyon $)
Ortalama işlem değeri	≈ 2 BTC (≈ 500$)
Bilişim bulmaca çözümlerine yatırım	≈ 4.254 exaflop
Güç tüketimi	> 173 MW (sürekli)

Bitcoin'in kuralları, avukat ya da herhangi bir düzenleyiciden etkilenmeyen mühendisler tarafından tasarlanmıştır. Bitcoin, işlemleri

tek bir sunucuda veya sunucu kümesinde depolamak yerine, katılımcı bilgisayarlardan oluşan bir ağ üzerinden dağıtılan bir işlem günlüğüne kurulmaktadır.

Herkes, herhangi bir ücret almadan ve herhangi bir merkezi izin prosedürü olmaksızın bir bitcoin hesabı oluşturabilir ancak gerçek isim kullanma zorunluluğu bulunmaktadır. Bu kurallar toplu olarak, daha esnek, daha özel ve düzenleyici gözetim için diğer ödeme şekillerinden daha az uygun olduğu anlaşılan bir sistem ortaya koymaktadır ancak tüm bu faydalar önemli sınırlarla karşı karşıyadır.

Şekil 10.2'de sunulan, 2017-2019 yılları arasındaki tarihi süreçte Bitcoin'in Dolar cinsinden değerinin grafiksel gösteriminde, 2018'deki ani yükseliş ve düşüşü gözler önüne serilmektedir.

Şekil 10.2. 2017-2019 Bitcoin / Dolar paritesi [8]

İktisatçılar mevcut ödeme sistemlerini ve hatta belki de parasal sistemleri bile bozabilecek bir sanal para birimi olarak Bitcoin ile ilgilenmektedir. Şu andaki başlangıç aşamalarında bile, bu sanal para birimleri piyasa tasarımı ve alıcıların ve satıcıların davranışları hakkında çeşitli bilgiler sunmaktadır.

10.3.1.1. Bitcoin Tasarım İlkeleri

Kıtlık, her türlü paraya değer vermek için bir ön şarttır. Mikro düzeyde, kıtlık sahteciliğe karşı korur. Daha geniş anlamda, kıtlık, parasal tabanın büyüme yolunu sınırlar ve fiyat istikrarını kolaylaştırır. Paranın elektronik formlarda tutulduğu modern ekonomilerde,

kıtlık, defter tutma kayıtlarının doğruluğunu garanti eden yasal kurallar ile korunmaktadır. Elektronik para, işlemlerin bir hesap için bir krediyi tetiklediği ve bir başkasına karşılık gelen bir borçlandırmayı içeren bir finansal sistemi içerir. Merkez bankaları dolaşımdaki mutlak para miktarını ayarlama gücüne sahiptir.

Bu çerçevede, Bitcoin, para arzının mutlak kıtlığını sağlamak için yaygın olarak kabul edilen ilk mekanizma olarak anlaşılabilir. Tasarım gereği, Bitcoin paraları dağıtmak veya kimin hangi paraları tuttuğunu takip etmek için merkezi bir otoriteye sahip değildir. Sonuç olarak, para yatırma ve doğrulama işlemlerinin yapılması klasik muhasebecilik sistemlerinden önemli ölçüde daha zordur. Bu arada Bitcoin, işlemlerin geçerliliğini doğrulamak da dahil olmak üzere defter tutma sistemini sürdürmeleri için teşvik etmek amacıyla taraflara özel kontrollü bir şekilde yeni para birimleri ihraç eder [1].

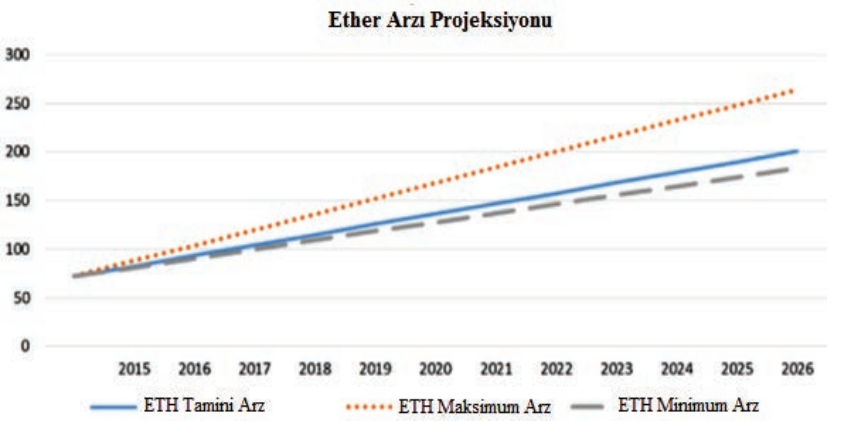
10.3.1.2. Bitcoin Yazılımı ve Bitcoin Adresi

Bir işletim sistemine Bitcoin yüklemek için öncelikle Bitcoin yazılımını indirmek gerekir. Piyasada birçok Bitcoin yazılımı bulunur (örneğin Bitcoin-Qt). Bu yazılım, Bitcoin'in kurucusu tarafından ortaya çıkarılan, Bitcoin uçtan uca açık kaynak yazılımının ilk versiyonudur. Kulanıcıların bu yazılımı kullanabilmeleri için bir Bitcoin cüzdanına sahip olmaları gerekmektedir. Bir Bitcoin cüzdanı normal bir cüzdanda olduğu gibi bakmayı, paylaşmayı ve harcamayı mümkün kılar. Kullanıcının aynı zamanda Bitcoin ağında kimliğini belirleyen bir Bitcoin adresine ihtiyacı vardır. Bir Bitcoin adresi kullanıcıyı doğrulayan bir isim ya da bir kimliğe benzer [6].

10.3.2. Ethereum

Sadece madencilikle üretilebilen Bitcoin'den farklı olarak, bir kitle fonlama kapsamında ön satış ile önemli miktarda ether Ağustos 2014'de piyasaya sürülmüştür. Satışa katılanlara altmış milyon ether ve para birimi geliştiricileri ile Ethereum Vakfı'na 12 milyon ether verilmiştir. Para birimi Ağustos 2015'de işlem görmeye başlamış, daha sonra para madenciliğiyle, teorik olarak 9,3 ile 16,8 milyon ether arasında değişen, her 15-17 saniyede bir 5 ila 8 ether tutarında bir yıllık yeni arz gerçekleşmiştir. Madenciliğin ilk yılında, Ağustos'a kadar yüzde 14,8 büyüyerek 10,7 milyon yeni ether üre-

tilmiştir. Maks ve min senaryolarına göre ether arzı projeksiyonu Şekil 10.3'de sunulmuştur [4].



Şekil 10.3. Maks ve min senaryolarına göre ether arzı projeksiyonu [4]

Ether'in ilk satışı, 22 Temmuz 2014-2 Eylül 2014 tarihleri arasında, 1 Bitcoin başına 2000 ETH oranında Ethereum Vakfı'nın önsatışı sırasında gerçekleşmiştir. Bitcoin'in fiyatının o zamanki değerine göre, etherin ilk değeri 0,316 ila 0,35 ABD doları arasındadır. O tarihten sonra iki yıl içinde, etherin değeri önemli bir artış sağlayarak başlangıçtaki değerinin yaklaşık 40 katı değere ulaşmıştır. Ancak, bu artış kurulduğu günden bu yana Bitcoin'in satın alma gücündeki artış kadar büyük değildir. Bitcoin'in yedi yılda geldiği nokta Ethereum'un iki katı civarındadır. Şekil 10.4'de Ekim 2017-Ocak 2019 tarihleri arası Ethereum / Dolar paritesi grafiği yer almaktadır [9].

Şekil 10.4. Ekim 2017-Ocak 2019 Ethereum / Dolar paritesi [9]

Sonuç olarak, Bitcoin'den daha yüksek bir ihraç oranına sahip olan ether, öngörülebilir gelecekte gelişmekte olan ülke para birimleriyle benzer büyüme oranlarına sahip olacaktır. Ethereum Vakfı, para biriminin geleceği için büyük takdir yetkisine sahip olarak yeterince kodlayıcı insan gücü, işlem gücü ve para yığınlarını kontrol ediyor olsa bile, ihraç planlarının ne zaman olacağını bile belirtmediklerinden, bunları sürdürme güvenilirliğini gösterememektedir. Tüm bu etkenler, etherin bir değer saklama aracı olarak çarpıcı bir talebinin mümkün olmadığını göstermektedir [4].

10.3.3. Ripple

Ripple isimli özel bir şirket tarafından üretilen ve yine Ripple olarak adlandırılan ve diğer para birimleri ve finansal araçların ödemelerini ağ üzerinden yapmak için kullanılan bir sanal paradır. Finans kurumları, aracılar ve Ripple ile çalışan bireyler, gerçekleştirmek istedikleri her işlem için işlem ücretlerini ödeyecekleri bir para birimi satın alacaklardır. Gerçekleşen her bir işlemde, bunun için kullanılan XRP geri dönüşü olmayan bir şekilde imha edilir, yani arz sürekli olarak daralır [4].

Başlangıçta 100 milyar XRP para birimi üretilmiş; bunların 20 milyarı para biriminin oluşturucuları tarafından elde tutulmuş ve diğer 80 milyar XRP, faaliyetleri finanse etmek için Ripple Labs'a verilmiştir. Ağustos 2016 itibariyle, bunların yaklaşık 64 milyarı hala Ripple Labs'a ait iken, kullanıcılar, geliştiriciler, satıcılar, ağ geçitleri ve piyasa yapıcılar arasında yaklaşık 15 milyar XRP dağıtılmıştır [4]. Şekil 10.5'de 2017-2019 Ripple / Dolar paritesi grafiği yer almaktadır.

Şekil 10.5. 2017-2019 Ripple / Dolar paritesi [10]

İlk uluslararası bankalararası ödeme Ripple ağı kullanılarak Temmuz 2016'da yapıldı. Ancak bu ödeme iki banka arasındaki bir ticari işlem değil sadece bir test işlemi oldu. Ripple'ın gelecekteki başarısı, dünya çapında mevcut uygulamaları toptan terk eden ve Ripple'a güvene dayalı bir sisteme geçen bankalara ve düzenleyicilere bağlıdır. İşlemlerin fiyatı standart bir para biriminde kote edilseydi, potansiyel kullanıcılara maliyet indirimi sunma şansına sahip olabilirdi. Ancak halihazırda sadece varsayımsal gelişmelerin reklamını yapabilmektedir.

10.4. Kripto Paranın Özellikleri ve Normal Paraya Göre Üstünlükleri

Geleneksel para ile kripto para karşılaştırıldığı zaman aşağıdaki özelliklere ve üstünlüklere sahip olduğu görülmektedir [5]:

- **Geri dönülemez ve izlenebilir:** Kripto parada ödeme ve transfer işlemleri geri dönülemez işlemlerdir. Ayrıca, bütün kullanıcıların işlemi izlenebilir ve bu işlemler blokzincirlerde kalıcı olarak kaydedilir.
- **Bir merkeze bağlı değildir ve anonimdir, yani sahibi bilinmez:** Kripto para yapısının içinde ne herhangi bir üçüncü taraf organizasyon yer alır, ne de bankalar gibi merkezi bir yönetimi bulunur. Dolayısıyla işlem bilgilerine göre kullanıcıların gerçek kimliğine ulaşılamaz.
- **Güvenlidir ve izin gerektirmez:** Kripto paranın güvenliği, suçluların kıramayacağı kadar sağlam olan kamu anahtarı kriptografisi ve blokzincir oybirliği mekanizması ile sağlanır. Ayrıca herhangi bir otoriteden izin almaksızın kullanıcılar kripto para ile müşterilerine ulaşırlar.
- **Hızlı ve küreseldir:** Kripto para işlemleri hızlıdır ve dünya genelinde kullanılmaktadır.

10.5. Sanal Paranın Türkiye'de ve Dünya'da Kullanımı ve Ülkelerin Yaklaşımları

Ülkelerin kripto para birimlerine ilişkin takındıkları tavır ve aldıkları güvenlik önlemleri birbirinden farklıdır. Buradaki temel sorun, kripto para birimlerinin herhangi bir meşru otoriteye bağlı olma-

ması ve kötü amaçlarla kullanılmasıdır [32]. Kripto para birimlerine karşı sergilenecek yaklaşımın tüketicinin korunmasını, bilgi gizliliğini, hukuki altyapıyı sağlaması gerekmektedir. Kısacası, kripto para birimlerine dair tüm riskler ve durumlar dikkate alınarak, yasal düzenlemelerin hayata geçirilmesi ve kullanıcıların kripto para(şirketler ve bireyler) mağduru olmamalarını sağlayacak güvenlik önlemlerinin alınması gerekmektedir. Yalnız, kripto para birimlerinin teknolojik altyapısından ve mimarisinden ötürü durum oldukça zordur.

Kripto para birimlerine ilişkin bir düzenlemenin tam manasıyla etkin olabilmesi için uluslararası boyutta bir çalışmaya ihtiyaç vardır [33]. Bunun sebebi, kripto paraların online olmaları ve belli bir ülkenin yasal güvencesinde bulunmayışlarıdır. Dolayısıyla, çok sayıda belirsizliğin olduğu bu ortamda, ülkelerin kripto para birimlerine karşı takındıkları yasal tutumlar farklılık arz etmektedir. Bazı ülkelerin merkez bankaları kripto para birimlerinin riskleri konusunda uyarılarda bulunmuşlardır. Bitcoin en bilindik ve en sık kullanılan kripto para birimi olduğu için, açıklamalar daha çok onun özelinde yoğunlaşmıştır. Örneğin, Alman Federal Finansal Denetleme Otoritesi (BaFin) [34], Belçika Merkez Bankası [35] ve Fransa Merkez Bankası [36], Bitcoin'in gözetiminin herhangi bir meşru otorite tarafından yapılmaması, fiyatının aşırı dalgalanma yaşaması, kara para aklama ve terörün finansmanında kullanılması ve taşıdığı siber güvenlik riskleri konusunda uyarılarda bulunmuşlardır. Bunun ötesinde, çok sayıda ülkenin merkez bankası Bitcoin'in para birimi olarak kabul edilemeyeceğini belirtmişlerdir. Bunlara örnek olarak Finlandiya Merkez Bankası [37] ve İsveç Merkez Bankası [38] verilebilir.

Bazı ülkeler kripto para birimlerinin kullanımını çeşitli şartlara bağlamışlardır. Örneğin, Fransız Maliye Bakanlığı 2014 yılında yayımladığı yasal bir düzenleme ile kripto para birimlerine ilişkin hesapların kullanımına kimlik doğrulama zorunluluğu getirmiş, kazanılan gelirleri ise vergiye bağlamıştır [39]. Bazı ülkelerde ise kripto para birimlerine ilişkin faaliyetler yasaklanmıştır. Çin Merkez Bankası 2013 yılında bir duyuru yayımlayarak, finansal kuruluşların Bitcoin ile alışveriş yapmamaları gerektiğini belirtmiştir [40].

Sanal para birimlerinin Türkiye'deki yasal statüsü 6493 Sayılı Kanun'a dayanmaktadır. Bu kanuna göre Türkiye'deki elektronik para kuruluşları ve ödeme kuruluşları Bankacılık Düzenleme ve Denetleme Kurumu'nun (BDDK) denetimi altındadır. Her ne kadar e-para ile kripto para farklı şeyler olsa da, BDDK kripto para birimleri ile ilgili ilk resmi açıklamayı 25 Kasım 2013 tarihinde yapmıştır. BDDK yaptığı açıklamada Bitcoin ve benzeri kripto paralar ile gerçekleştirilen işlemlerde tarafların gerçek kimliklerinin bilinmemesinden dolayı, bu paraların yasadışı faaliyetlerde kullanılabileceğine dikkat çekmiştir [41]. Bunun haricinde, siber güvenlik penceresinden bakılarak, dijital cüzdanların çalınabilmesi, kaybolabilmesi veya sahiplerinin bilgileri dışında kötü niyetli kişiler tarafından kullanılabilmesi hususunda uyarılar yapılmıştır.

Türkiye'de kripto para alımı, satımı ve kullanımı hiçbir yasa ile düzenlenmemiştir ve 6493 Sayılı Kanun'a göre kripto paralar e-para olarak kabul edilemezler. Dolayısıyla, aslında bu para birimlerinin kullanımı yasak değildir. Buradan hareketle, Türkiye'de çeşitli girişimler olmuştur. BTCTurk web sitesi Türkiye'de Bitcoin borsası olarak faaliyet gösteren ilk girişimdir. Yalnız, hiçbir banka BTCTurk ile çalışmayı kabul etmediği için 2016 yılında siteden TL yatırma ve çekme işlemleri durdurulmuştur. Bunun haricindeki işlemler devam etmektedir. BTCTurk haricinde Türkiye'de Bitcoin borsası olarak faaliyet göstermiş bir diğer site Takascoin'dir. Takascoin de vergisel nedenlerle kapanmıştır. Daha sonraları, Koinex isimli takas platformu kurulmuştur. Platformda bulunan çeşitli kripto para birimleri arasında takas gerçekleştirilebilmektedir. Ayrıca, Türkçe hizmet sunması ve Türkiye içindeki tüm bankalar ile anlaşmasının olması kullanıcılar açısından büyük bir avantajdır.

Türkiye'de geçmişte sanal para veya kripto para üretme çalışmaları olmuştur. Bunlara örnek olarak E-lira ve Turcoin verilebilir. Fakat, çeşitli sebeplerden ötürü, bu çalışmalar sonuçsuz kalmıştır. Ayrıca, ülkemizde ödeme aracı olarak Bitcoin kullanan şirketler çok az sayıdadır. Bu şirketler coinmap.org sitesi üzerinden incelenebilir [42].

10.6. Blokzincir ve Blokzincirde Ortaya Çıkabilecek Riskler

Bu alt başlıkta blokzincir, blokzincirin riskleri, bu riskleri ortaya çıkartan çeşitli sebepler ve bu risklerin doğurabileceği olası sonuçlar incelenecektir. Blokzincir 1.0 ve Blokzincir 2.0 teknolojileri farklılık gösterdiğinden, bu alt başlıkta anlatılacak olan risklerin bazıları hem Blokzincir 1.0 için hem de Blokzincir 2.0 için geçerli iken, kalan kısmı ise sadece Blokzincir 2.0 için geçerlidir. Buna uygun olarak, riskler iki ayrı başlık altında ele alınacaktır.

İnternet üzerinde yoğun bir şekilde fotoğraf, yazı, video ve benzeri veri transferi yapılmaktadır. Bu tür verilerin dışında değer atfettiğimiz varlıkların transferinde blokzincir teknolojisi kullanılmaktadır. Örneğin önceki bölümlerde bahsettimiz Bitcoin'in paylaşımı Blokzincir teknolojisinden yararlanılarak yapılmaktadır. Bunun dışında bankacılık, e-ticaret ve ödemeler, hisse senetleri ve borsalar, e-noter, bulut bilişim ve güvenli bulut depolama gibi uygulama alanları da vardır. Blokzincirde merkezi bir sunucu veya güvenilir bir otorite kaldırılarak, merkezi güven internet üzerinde dağıtılabilmektedir. Blokzincir teknolojisi genel olarak Bitcoin ve Ethereum'da kullanılmaktadır [13].

Blokzincirde iki temel kavram vardır. Bunlardan ilki "Kayıt"tır. Blokzincir kayıtları, ilgili blokzincirdeki her türlü içeriktir. Demirbaş girdileri, para transferi bilgileri, müşteri kayıtları bunlara örnek olarak verilebilir. İkinci temel kavram ise "Blok"tur. Kayıtların birleştirilerek belirli aralıklarla blokların içine yazılması işlemlerinde blokzincirin tasarımına göre kaç kayıt olacağı ve hangi işlemlerden sonra bir blok oluşturulacağı belirlenmektedir. Blokların oluşturulmasında kriptografik özet algoritmaları ve e-imza kullanılmaktadır. Blokzincirde her katılımcı başlangıçtan itibaren kayıtların bir kopyasını saklar. Bu kayıtların değiştirilmesi özetleri de değiştirdiğinden, kayıtlar değiştiği zaman çoğunluk bunu farkeder. Dolayısıyla güvenilir ortamda merkezi bir veritabanına ihtiyaç kalkar [13].

Tablo 10.2'de Blokzincir 1.0 ve 2.0'ın riskleri listelenmiş ve sebepleri gösterilmiştir.

Tablo 10.2. Blokzincir'in riskleri ve sebepleri [5].

Risk	Sebep	Etki Aralığı
Gizli Anahtar Güvenliği	Genel anahtar şifreleme şeması	Blok Zincir 1.0 ve 2.0
%51 Güvenlik Açığı	Konsensus mekanizması	
İllegal Faaliyetler	Kripto para birimi uygulaması	
İşlem Gizliliği Sorunu	İşlem tasarım hatası	
Çift Harcama	İşlem doğrulama mekanizması	
Zeki Sözleşmedeki Güvenlik Zaafları	Zeki Sözleşme Uygulaması	Blok Zincir 2.0
Düşük Fiyatlı İşlemler	Program yazma hatası	
Optimize Edilmemiş Zeki Sözleşme	EVM tasarım hatası	

10.6.1. Genel Riskler

Blokzincir 1.0 ve 2.0 için geçerli genel riskler alt başlıklarda açıklanmıştır.

10.6.1.1. Gizli Anahtar Güvenliği

Blokzincir teknolojisinde, kullanıcının gizli anahtarı yine kullanıcı tarafından üretilmektedir ve bu anahtar blokzincirde kullanıcının kimlik ve güvenlik bilgisi olarak kabul edilmektedir. Yani, bu özel anahtar üçüncü-parti bir kurum tarafından sağlanmamaktadır. Kullanıcının kendisi tarafından üretilen bu gizli anahtarın kaybolması veya çalınması durumunda, bu anahtarın kurtarılması bir daha mümkün olmamaktadır. Ayrıca, kötü niyetli kişiler tarafından kullanıcının gizli anahtarının çalınması durumunda, kullanıcının blokzincir hesabı bu kişilerin kontrolüne geçebilmektedir. Blokzincir ile ilgili süreçlerde kullanılan çeşitli algoritmaların zaafları da gizli anahtarın kötü niyetli kişilerin eline geçmesine imkan tanıyabilir. Örneğin, yapılan bir çalışmada, imzalama işleminde kullanılan Eliptik Eğri Dijital İmza Algoritması'nın güvenlik açığı barındırdığı belirtilmiştir [14].

10.6.1.2. %51 Güvenlik Açığı

Blokzincir teknolojisinin karşılıklı güven tesis etmek için kullandığı dağıtık uzlaşma mekanizması %51 güvenlik zafiyetini de beraberinde getirmektedir. Tüm blokzinciri kontrol altına alabilmek için, uzlaşma mekanizmasının doğurduğu bu güvenlik açığı kötü niyetli kişiler tarafından kullanılabilir. Örneğin, en popüler iki kripto paranın kullandığı (Bitcoin ve Ethereum) işin kanıtı tabanlı blok zincirinde bu durum şu şekilde ortaya çıkabilir: Eğer tek bir madencinin özetleme gücü, tüm blok zincirinin toplam özetleme gücünün %50'sinden daha fazlasına tekabül ediyorsa, %51 saldırısı başlatılabilir. 2014 yılının ocak ayında, "ghash.io" isimli madencilik havuzu bitcoin hesaplama gücünün %42'sine ulaşmıştır. Bu olaydan sonra, bir dizi madenci gönüllü olarak havuzdan ayrılmıştır [15]. Öte yandan, diğer kripto paraların kullanmış olduğu diğer blokzincir teknolojilerinde, bu saldırının ortaya çıkma durumu teknolojiye bağlı olarak farklılık göstermektedir [3].

10.6.1.3. İllegal Faaliyetler

Bazı kripto para kullanıcıları aynı kripto para birimi için birden fazla adrese sahip olabilmektedir. Blokzincirde kullanılan bu adresler sanal ortamda kullanıcıyı temsil etmektedir fakat bu adreslerin kullanıcıların gerçek kimlikleri ile bir bağlantısı yoktur. Bitcoin sistemi de tek bir kullanıcının birden çok adrese sahip olmasına imkan vermektedir. Bitcoin'in en bilindik ve en sık kullanılan kripto para birimi olmasından ötürü, bazı ticaret birimleri tarafından da ticari işlemlerde kullanılmaktadır. Bitcoin kullanıcıları bu ticaret ortamlarını kullanarak herhangi bir ürünün alım satımını kolaylıkla gerçekleştirebilmektedirler. Gerek birden fazla adres kullanımı gerekse de adreslerin gerçek kimlikleri yansıtmaması sebebiyle, yasal olmayan işlemlerin takibi ve cezalandırılması çok güçtür [6].

İllegal faaliyetlere örnek olarak fidye yazılım, kara para aklama ve yeraltı pazarı verilebilir.

Fidye Yazılım

Kötü niyetli kişilerin ve bilgisayar korsanlarının bitcoin kullanarak gerçekleştirdiği siber suçların en başında fidye yazılımı (Ransomware) gelmektedir. Bu saldırıları gerçekleştiren siber suçlular,

kurbanlarının bilgisayarlarına çeşitli şekillerde zarar vermektedirler ve daha sonrasında da bilgisayarları kurtarmak için fidye talep etmektedirler. Kısacası, bu bilgisayar korsanlarının asıl hedefi kurbanlarından para koparmaktır. Bu tarz saldırılarda kullanılan yazılımlar genellikle elektronik posta eklentileri şeklinde kullanıcılara gönderilmektedir. Eğer kullanıcılar bu eklentiye tıklarlarsa, fidye yazılımı arka planda çalışmaya başlamaktadır. Bu duruma en iyi örnek, 2014 yılında dünya üzerinde çok sayıda kullanıcıyı etkileyen "CTB-Locker" isimli fidye yazılımıdır [16]. Bu fidye yazılımı, elektronik posta eklentisi şeklinde kullanıcılara gönderilmiş, bu eklentiye tıklayan kullanıcıların bilgisayarlarının arka planında çalışmış ve bilgisayarlarda yüklü olan çok sayıda dosyayı şifrelemiştir. "CTB-Locker" isimli fidye yazılımından sonra, bir diğer meşhur saldırı da "WannaCrypt" saldırısıdır [17]. Bu fidye yazılımı 2017 yılında Windows işletim sisteminin bir güvenlik açığından faydalanarak yayılmış ve sadece 2 gün içerisinde dünya üzerinde yaklaşık 230.000 kişiyi etkilemiştir.

Kara Para Aklama

Kara para aklamak için de kripto paralar kullanılabilmektedir. Kripto paraların özelliklerine ve kullandığı alt yapıya bağlı olarak, kara para aklama için kullanılabilme riskleri farklılık göstermektedir [18]. Ayrıca, kripto para özelinde geliştirilen bazı uygulamalar da kara para aklamaya imkan tanıyabilir. Örneğin, "Dark Wallet" isimli bir bitcoin uygulaması, bitcoin işlem bilgisini şifreleyerek bitcoin işlemini bütünüyle gizli bir hale getirmektedir [19]. Bununla birlikte, bu uygulama geçerli para ile geçerli olmayan parayı karıştırmak suretiyle kara para aklamaya imkan vermektedir.

Yeraltı Pazarı

Yeraltı pazarları, kripto para birimini kullanarak internet üzerinden çeşitli ürünlerin satışını yapan isimsiz pazarlardır. Aslında bu pazarların isimleri vardır (sanal), fakat bir önceki cümledeki "isimsiz" ifadesi, asıl kimlikleri belli olmayan manasında kullanılmıştır. Ne yazık ki, bu yeraltı pazarlarının belirli bir kısmı uyuşturucu ve ilaç gibi satışı yasak olan çeşitli ürünleri satmaktadır. Bitcoin, daha önceki bölümlerde bahsedilen çeşitli özellikleri dolayısıyla yeraltı pazarında en sık kullanılan sanal para birimidir. Örneğin, "Silk Road"

uluslararası ölçekte internet üzerinden zararlı ürünler de dahil olmak üzere çeşitli ürünlerin satışını yapan ve para birimi olarak da bitcoin kullanan gizli bir pazardır [20].

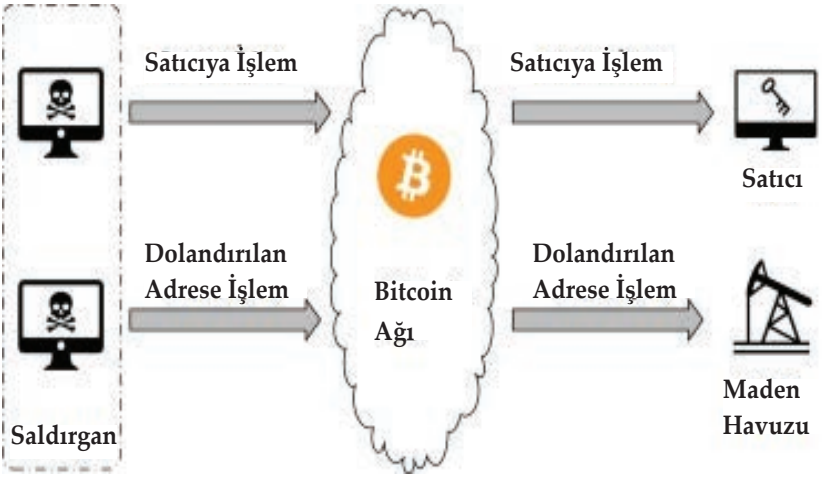
10.6.1.4. İşlem Gizliliği Sorunu

Blok zinciri teknolojisinde kullanıcıların işlem mahremiyetini sağlamak için çeşitli prosedürler uygulanmaktadır. Normalde, kullanıcıların işlemleri izlenebilmektedir, yalnız bu uygulanan prosedürler sayesinde mahremiyetin korunması sağlanmaktadır. Kullanılan kripto para birimine, ve doğal olarak kullanılan blok zinciri teknolojisine bağlı olarak alınan bu önlemler farklılık göstermektedir. Kimi sanal para birimlerinde tek seferlik hesaplar kullanılırken, kimi para birimlerinde ise kullanıcılar işlem sırasında geçerli olmayan paraları (mixin) da ekleyebilmektedirler. Örnek verecek olursak, Bitcoin para biriminde, kullanıcılar tek seferlik hesaplar kullanmaktadırlar. Monero para biriminde ise geçerli olmayan paraların eklenebilmesine izin verilmektedir. Monero'da uygulanan bu prosedür ile saldırgan harcanan asıl paraların bağlantısını bulamaz. Ne yazık ki, yapılan bir çalışmada Monero'da uygulanan bu geçerli olmayan paraların katılması prosedürünün bazı zaaflar içerdiği ve bu zaaflar sayesinde kötü niyetli kişilerin işlem mahremiyetini ortadan kaldırabileceği tespit edilmiştir [21].

10.6.1.5. Çift Harcama

Çift harcama, bir kullanıcının işlemler için aynı kripto parayı çok kez kullanmasıdır. Normalde, blokzincir teknolojisinin konsensüs özelliği işlemleri doğrulayabilmektedir. Buna rağmen, çift harcamanın önüne geçmek mümkün değildir [22]. Bu durumu şu şekilde açıklayabiliriz: İşin kanıtı tabanlı blokzincirde, iki işlemin başlangıç ve doğrulama aşamaları arasında geçen süreyi saldırgan kendi çıkarı için kullanabilir. Yani, bu süre içerisinde bir saldırı başlatabilir. İlk işlemin çıktısı elde edilip, aynı kripto para ikinci işlem geçersiz sayılmadan önce tekrar kullanılırsa bu durum çift harcamaya tekabül etmektedir. Aslında, burada yapılan bir saldırıdır.

Şekil 10.6'da Bitcoin'deki hızlı ödemeye karşı yapılan çift harcama saldırı modeli gösterilmiştir.



Şekil 10.6. Bitcoin'deki hızlı ödemeye karşı yapılan çift harcama saldırı modeli [5].

10.6.2. Blokzincir 2.0'a Özgü Riskler

Blokzincir 2.0'a özgü riskler alt başlıklarda sunulmuştur.

10.6.2.1. Zeki Sözleşmedeki Güvenlik Zaafları

Blokzincir mekanizmasında çeşitli programlar yürütülmektedir. Bu kullanılan programların barındırdığı hatalardan ve/veya zaaflardan ötürü, zeki sözleşmeler de dolaylı olarak güvenlik zaafları barındırabilir. Yapılan bir çalışmada, zeki sözleşmelerde ortaya çıkabilecek 12 farklı güvenlik zafiyeti incelenmiştir ve bu güvenlik zafiyetlerinin hangi sebepten ötürü ve hangi seviyede ortaya çıktıkları belirtilmiştir [23]. Yine, gerçekleştirilen başka bir çalışmada, tanımlanmış dört farklı güvenlik zafiyetini tespit etmek için kullanılan bir sembolik yürütme programı geliştirilmiştir [24]. Geliştirilen bu program kullanılarak 19.366 tane Ethereum zeki sözleşmesi incelenmiş ve bunların 8833 tanesinin bu dört adet zaaftan en az birini barındırdığı tespit edilmiştir. İsmi "Oyente" olan bu program, "Güvenlik Geliştirmeleri" kısmında detaylı bir şekilde açıklanacaktır.

10.6.2.2. Düşük Fiyatlı İşlemler

Ethereum'da her bir işlemin belirli bir gaz değeri vardır [25]. Gaz değeri işlem tarafından tüketilen hesaplama kaynaklarının büyük-

lüğü ile orantılıdır. Bu hesaplama kaynaklarına örnek olarak bant genişliği ve kaplanan hafıza alanı verilebilir. Ne yazık ki, her bir operasyonun tüketmiş olduğu kaynağın büyüklüğü net bir biçimde hesaplanamamaktadır. Dolayısıyla, gaz değerlerinin ayarlanmasında yanlışlıklar olabilmektedir. Normalde yüksek kaynak tüketen işlemlere düşük gaz değeri atanması kötü niyetli kişilerin kullanabileceği bir güvenlik zafiyeti doğurmaktadır. Bilgisayar korsanları bu tarz işlemleri kullanarak Hizmet Aksattırma Saldırısı (DoS) gerçekleştirebilirler. Örneğin, saldırganlar intihar (SUICIDE) işlemini kullanarak bir DoS saldırısı gerçekleştirmişlerdir [26]. Bu işlem kullanılarak 19 milyon sahte hesap oluşturulmuş, bu sayede gereksiz hard disk kullanımı meydana gelmiş ve işlemler çok yavaşlamıştır. Yaşanan bu ve benzeri saldırılardan sonra, yedi yüksek kaynak tüketen işlemin gaz değerleri EIP 150'de (Ethereum İyileştirme Önerisi) güncellenmiştir.

10.6.2.3. Optimize Edilmemiş Zeki Sözleşme

Herhangi bir kullanıcı, Ethereum'da konuşlandırılmış akıllı bir sözleşme ile etkileşime girdiğinde, belirli bir miktarda gaz fatura edilir. Bu gaz, Ethereum'da kripto-para olan Ether ile takas edilebilir. Ne yazık ki, bazı zeki sözleşmelerin üretimi (geliştirilmesi) ve dağıtılması (görevlendirilmesi) yeteri kadar optimize edilmemiştir. Yapılan bir çalışmada, yedi adet yüksek gaz maliyeti olan şablon tespit edilmiştir [27]. Ayrıca, aynı çalışma kapsamında, zeki sözleşmelerde görülen 3 farklı yüksek gaz maliyetli şablonu tespit edebilen "Gasper" isminde bir program geliştirilmiştir. Bu üç yüksek gaz maliyetli şablondan ilki ölü koddur. Zeki sözleşmenin blokzincirde dağılımı sırasında gaz tüketimi bytecode'un boyutu ile ilişkilidir. Dolayısıyla, ölü kodlar çalışmasa bile fazladan tüketime sebep olmaktadır. İkinci yüksek gaz maliyetli şablon opak yordamdır. Zeki sözleşmedeki bu opak yordamların sonuçları hep aynıdır ve Ethereum sanal makinasını boşuna çalıştırmaktadır. Bu da fazladan gaz tüketimi demektir. Yüksek maliyetli şablonlardan sonuncusu ise döngü içindeki pahalı işlemlerdir. Normalde, döngü dışına alınabilecek bu işlemler fazladan tüketime sebep olmaktadır. "Gasper" programı kullanılarak yapılan bir analizde, Ethereum'da konuşlan-

dırılmış zeki sözleşmelerin %80'inden fazlasının bu üç şablondan en az birine sahip olduğu bulunmuştur.

10.7. Blokzincir Sistemlerine Yapılmış Saldırı Örnekleri

Bu bölümde blokzincir sistemlerine yönelik saldırılara alt başlıklar halinde örnekler verilmiştir.

10.7.1. DAO Saldırısı

Bir kitle fonlama şirketi olan DAO, 28 Mayıs 2016 tarihinde Ethereum'da konuşlandırılmış bir zeki sözleşmedir. DAO, blokzincirde konuşlandırıldıktan sadece 20 gün sonra bir saldırıya uğramıştır ve saldırgan bu saldırısında zeki sözleşmenin yeniden giriş zafiyetini kullanmıştır [23]. Saldırgan, geri dönme fonksiyonunda DAO'ya withdraw() fonksiyon çağrısı içeren kötü niyetli bir zeki sözleşme geliştirmiş ve bunu yayınlamıştır. Saldırının hemen öncesinde DAO'nun değeri 150 milyon dolar seviyesine kadar çıkmıştır. Kötü niyetli kişi/kişiler gerçekleştirdikleri saldırı sonucunda yaklaşık olarak 60 milyon dolar çalmışlardır.

10.7.2. BGP Ele Geçirme Saldırısı

Sınır Geçiş Protokolü (BGP) standart bir yönlendirme protokolüdür ve IP paketlerinin hedeflerine nasıl yönlendirildiğini düzenler. Kötü niyetli kişiler blok zincirinin ağ trafiğini durdurmak için BGP yönlendirme protokolünü kullanmaktadırlar [28]. Yalnız, BGP ele geçirme saldırısının gerçekleştirilebilmesi, ağ operatörlerinin kontrolünün ele geçirilmesine bağlıdır. Maalesef, bazı Bitcoin madencilik havuzları merkezi bir yapıya sahiptir. Saldırganlar bu tarz madencilik havuzlarına BGP ele geçirme saldırısı gerçekleştirirlerse, Bitcoin ağını bölebilirler veya blok yayılma hızını yavaşlatabilirler. Gerçekleştirilen bir saldırıda, saldırganlar kendileri tarafından kontrol edilen bir maden havuzuna trafiği yönlendirmişler ve yaklaşık olarak 83.000 ABD doları tutarındaki kripto para birimini iki aylık bir süre zarfında kurbanlarından toplamışlardır [29].

10.8. Blokzincirde Güvenlik Geliştirmeleri

Blokzincir sistemlerindeki güvenlik geliştirmeleri bu bölümde ele alınmıştır.

10.8.1. SmartPool

Konsensüs mekanizması olarak işin kanıtı tabanlı yaklaşımı kullanan blokzincirde hesaplama gücü ve madencilik havuzu çok önemlidir. Normalde blok zinciri teknolojisi merkezi olmayan bir yapıya sahiptir. Maalesef, madencilik havuzları dolaylı olarak bir güvenlik zafiyeti oluşturabilme riskini de barındırmaktadır. Eğer madencilik havuzunun hesaplama gücü blokzincirin toplam hesaplama gücünün %50'sinden fazla ise, %51 saldırısının başlatılabileceği daha önceki bölümde belirtilmişti. Blokzincir mekanizmasının merkezi olmayan yapısını bozan bu duruma çözüm olarak "SmartPool" isimli yeni bir madencilik havuzu sistematiği önerilmiştir [30]. Akıllı sözleşmeleri altyapısında kullanan SmartPool merkezi olmayan bir yapıyı bütünüyle desteklemektedir. Yeni bir veri yapısını kullanan bu yöntem güvenlidir ve tamamlanmış parçalar madenciler tarafından SmartPool sözleşmesine partiler halinde gönderilebildiği için standart yönteme göre daha da verimlidir. Bu yeni sistematiğin çalışması şu şekildedir:

1) SmartPool, madencilik görevleri bilgisini içeren Ethereum düğümlerinden işlemleri alır.
2) Madenci görevlere bağlı olarak hashing hesaplamasını yürütür ve daha sonra tamamlanmış parçaları SmartPool istemcisine geri döndürür.
3) Tamamlanan parçaların sayısı belirli bir miktara ulaştığında, bunlar Ethereum'da görevlendirilmiş SmartPool sözleşmesine sunulur.
4) Smartpool sözleşmesi parçaları doğrular ve istemciye ödülleri teslim eder.

10.8.2. Nicel Yapı

Blokzincir mekanizmasının güvenliğini artırıcı tedbirler ve yöntemler çoğunlukla blokzincirin performansını olumsuz etkilemektedir. Öte yandan, sadece blokzincirin performansını düşünerek güvenlik mekanizmalarını devre dışı bırakmak da mantıksız bir uygulama olacaktır. Kısacası performans ile güvenlik arasındaki dengenin iyi sağlanması ve optimum çözümlerin bulunması gerekir. Bu mak-

satla, işin kanıtı tabanlı blokzincirin çalışma performansını ve güvenlik mekanizmalarını analiz etmek için sayısal bir yapı çalışması geliştirilmiştir [31]. "Blokzincir uyarıcısı" ve "güvenlik modeli" adında iki bileşenden oluşan bu yapı çalışması performans ölçütlerini de dikkate alarak, ataklara karşı en iyi güvenlik önlemlerini çıktı olarak vermektedir. Burada, "Blokzincir uyarıcısı" blokzincirin yürütülmesini taklit ederek, çeşitli parametrelerle ilgili performans bilgilerini hesaplar. Bu parametreler içerisinde "vadesi geçmiş blok oranı" parametresi diğerlerine göre daha önemlidir ve "güvenlik modeli" bileşenine iletilmektedir. Güvenlik modeli bileşeni ise daha sonra en iyi güvenlik önlemlerini belirlemektedir.

10.8.3. Oyente

Ethereum zeki sözleşmelerdeki hataları tespit etmek için açık kaynak kodlu bir program olan "Oyente" geliştirilmiştir [24]. Bu program, zeki sözleşmelerin taşınabilir kodunu analiz etmek için sembolik yürütmeyi kullanmaktadır. Ayrıca, Ethereum Sanal Makinesi'nin (EVM) yürütme modelini takip etmektedir. "Oyente", görevlendirilmiş (dağıtılmış) sözleşmelerdeki hataları bulmak için Ethereum blok zincirinde depolanan akıllı sözleşmelerin taşınabilir kodlarını kullanmaktadır. Oyente, 6 farklı modülden oluşan bir mimariye sahiptir. Sistematiğinin girdileri ise zeki sözleşmenin taşınabilir kodları ve Ethereum genel durumudur. Oyente'yi oluşturan bu modüllerden "Core Analysis" ve "Validator" modülleri diğerlerine göre hassas ve önemli işleri yerine getirmektedir. "Core Analysis" modülü çeşitli analiz algoritmalarını barındırmaktadır ve zeki sözleşmede ortaya çıkabilecek 4 adet Güvenlik Zaafını (İşlem Sıralama Bağımlılığı, Zaman Damgası Bağımlılığı, Kötü İdare Edilmiş İstisnalar, Yeniden Giriş Zafiyeti) tespit etmeye çalışmaktadır.

10.9. Sanal Para İle Siber Güvenlik Arasındaki İlişki

Siber suç olayları her geçen yıl artmaktadır. İnternet suçluları sayısında azalma olmayacağı düşünülmektedir. Kripto para birimlerinin artmasıyla birlikte, bu siber suçluların artık internetteki suç faaliyetleri için yeni istekleri ve yeni motivasyonları vardır. Ayrıca, kripto para birimlerinin artışı da yeni tür suç faaliyetlerinin oluş-

masına neden olmuştur. Cryptojacking, Ransomware ve diğer benzer eylemlerin kripto para birimleri ile doğrudan bir ilişkisi vardır. Kripto para yatırımcıları da basit hedeflerdir - çünkü bazıları, kripto pazarlarının sunduğu yüksek değer artışının aklını çeldiği ilk yatırımcılardır. Yeni nesil siber suçlular, kripto para birimlerini çalmak için bazen eskimiş oltalama tekniklerinden farklı kimliğe bürünme gibi basit taktikleri kullanıyorlar. Bazen, bu saldırılar, saldırıya uğrayan kripto para birimi takasları veya fidye yazılımı saldırıları gibi daha ileri düzeyde olabilir [43].

Nihai ekosistem henüz belirlenemediğinden, teknoloji geliştikçe ve kullanıcı kabulü arttıkça, ilişkili risk alanları sürekli değişecektir. Kötü niyetli kişiler kripto para birimlerini çok çeşitli taktikler kullanmaktadırlar. Saldırılar kullanıcıları ve cüzdanlarını, takaslarını ve/veya kilit saklama servislerini ve kripto para birimlerini destekleyen ağları veya protokolleri hedefleyebilmektedir. Saldırganlar son birkaç yıl içinde daha çok kullanıcılara ve kripto para birimi borsalarına saldırarak para çalmakta, kripto para birimleri ağlarını ve protokollerini hedef alan saldırılar ise nispeten daha az olmaktadır [44].

Ayrıca, kişisel hatalardan kaynaklanan kayıplar da söz konusudur. Örneğin, Newport, UK'deki bir kişi 4 milyon £ değerinde Bitcoin içeren sabit diskini kaybetmiştir. Bu olay sanal cüzdanın mı yoksa para kaybolduğunda kullanıcıları koruyabilen bir üçüncü parti olan kredi/banka kartının mı daha güvenli olduğu sorusunu ortaya çıkarmıştır. Sanal paralar yasal olarak düzenlenmememiştir. Dolayısıyla Bitcoin'in miras bırakılma imkanı olmadığından, kullanıcı öldüğünde parası da ölmüş olacaktır. Bu durum, Bitcoin kullanımının kredi/banka kartı ile kıyaslandığında pratikteki olumsuzluğu olarak gösterilebilir [45].

Son kullanıcı açısından değerlendirildiğinde, sanal para türlerinden Bitcoin'in kullanılabilirliği ve güvenliği üzerine yapılan bir çalışmanın sonucuna göre, güvenlik açısından ankete katılan katılımcıların doğrulama yöntemleri hakkında yaptıkları yorumlardan Bitcoin ile negatif bir deneyime sahip oldukları tespit edilmiştir. Katılımcılar, kullanılan uzun kimlik kullanımı nedeniyle cüzdana giriş yapma-

nın zor olduğunu bildirmişlerdir. Ayrıca, cüzdan için tüm güvenlik kimlik doğrulama özelliklerini ayarlamak için gereken zaman ve çaba sorunlu olduğunu bildirmişlerdir. Bu son kullanıcılar kredi/banka kartını Bitcoin'e göre daha güvenli bulduklarını bildirmişlerdir [45].

10.9.1. Kripto Para Borsalarına Saldırı Örnekleri

Aşağıda, kripto para borsalarına yapılmış bazı güncel ve önemli saldırılara örnekler verilmiştir [44]:

- **Bancor:** Bancor Temmuz 2018'de, tanımlanamayan aktörlerin akıllı sözleşmeleri yükseltmek için kullanılan bir cüzdanı tehlikeye attığını itiraf etmiştir. İddiaya göre aktörler, 12.5 milyon ABD Doları 24.984 ETH ve 229.356.645 NPXS (Pundi X, yaklaşık 1 milyon ABD Doları) geri çektiler. Saldırganlar ayrıca Bancor'un yaklaşık 10 milyon dolarlık 3.200.000 BNT'sini de çaldılar. Bancor, planladığı uzlaşma ve güvenlik önlemlerinin ayrıntıları hakkında yorum yapmamıştır.

- **Bithumb:** Saldırganlar Haziran 2018'de, saldırganlar Güney Kore'nin en büyük kripto para birimi borsası Bithumb'tan 30 milyon dolar değerinde kripto para birimi çalmışlardır. Cointelegraph Japan'a göre saldırganlar Bithumb'ın sıcak (çevrimiçi) cüzdanını kaçırmışlardır.
- **Coinrail:** Coinrail, Haziran 2018'de, sisteminde "siber saldırı" olduğunu ve tahminen 40 milyar won (37.2 milyon $ değerinde) çalındığını itiraf etmiştir. Polis saldırıyı soruşturmaktadır, ancak daha fazla ayrıntı yayınlanmamıştır.
- **BitGrail:** BitGrail Şubat 2018'de, müşterilerin Nano'daki (XRB) 195 milyon ABD Doları değerindeki kripto para biriminin çalındığını iddia etmiştir.
- **Coincheck:** Ocak 2018'de, tanımlanamayan saldırganlar borsadaki sıcak cüzdandan 523 milyon NEM para (yaklaşık 534 milyon USD) çalmışlardır. Coincheck, NEM'in daha güvenli bir çoklu imzalı cüzdan yerine tek imzalı sıcak cüzdanda tutulduğunu ve çalınan paranın Coincheck müşterilerine ait olduğunu doğrulamıştır.

10.9.2. Siber Güvenlik Açısından Alınması Gereken Önlemler

Acemi kullanıcıların, kendilerini kandırmayı dört gözle bekleyen çevrimiçi avcılara avlanmadıklarından emin olmak için takip edebilecekleri basit taktikler şunlardır [43]:

- **Bilinmeyen Göndericilerden Gelen Ekler Açılmamalıdır:** Eskimiş bir tavsiye de olsa kullanıcıların güvenilir kaynaktan geldiğini düşünüp güvenerek açtığı ekler zararlı olabilmektedir. Bu dosyalar casus yazılım, virüs veya kötücül yazılım olabilmektedir. Şimdilerde fidye yazılımı artan bir tehdittir. Bu ekler içine gizlenmiş zararlı dosyalar içerebilmektedir – hatta bazen zararsız görünen bir jpeg görüntüsünün üzerinde bile fidye yazılımı olabilir. Fidye yazılımların çoğu eposta ile yayıldığından, güvenilir olduğundan emin olunmayan eklerin indirilmemesi kritik bir öneme sahiptir.
- **Bedava Para Olmadığı Unutulmamalıdır:** Birçok insan twitterda Elon Musk veya Vitalik Buterin gibi meşhur kişiler gibi davranan kişilerin oyununa gelmektedir. Bedava para yoktur ve kimse para dağıtmamaktadır. Yatırımın geri dönüş garantisi verilmesinde bile kullanıcılar cezbedilerek kandırılabiliyor. Daha fazla para geri vermek için sizden bir miktar para isteyen herhangi biri sizi kandırıyor olabilir.
- **İki Aşamalı Doğrulama Kullanılmalıdır:** Şifreniz çalınsa bile, bilgisayar korsanlarının hesabınıza erişememesini ve sahip olduğunuz başka bir cihaza erişmeden para birimlerinizi transfer etmemesini sağlayan bir sistem kurmak gerekli bir güvenlik önlemidir. Bu ikinci kimlik doğrulama biçimi, Google Authenticator, bir e-posta veya kısa mesaj şeklinde olabilir. Şifreyi girdikten sonra, bu ikinci doğrulamanın giriş yapmadan önce sağlanması gerekir.
- **Verilerinizi Düzenli Olarak Yedeklenmelidir:** Önlem, tedaviden daha iyidir. Verilerinizin düzenli olarak yedeklenmesi, özellikle yüksek öneme sahip dosyaların güvenliği için önemlidir. Bir fidye yazılımı saldırısı bilgisayarınızı etkiliyor olsa bile; bu düzenli yedeklemeler sayesinde tüm verileriniz güvende kalır.

- **Donanım Cüzdanları Kullanılmalıdır:** Kripto para biriminin değiş tokuşunun veya herhangi bir çevrimiçi depolama platformunun güvenlik önlemleri aslında bir kullanıcının elinde olmamasına rağmen para birimlerinizi güvende tutmanın en iyi yolu, onları bir donanım cüzdanında saklamaktır. Donanım cüzdanları, üzerlerinde kripto para depolayan gerçek fiziksel cihazlardır - ve kullanılmadıklarında, herhangi bir saldırıya karşı güvende olmalarını sağlayarak internetten kopuk kalabilirler. Şekil 10.7'de, donanım cüzdanına örnek gösterilmiştir.

Şekil 10.7. Donanım Cüzdanı [46].

Donanım cüzdanları kripto paraların siber güvenliği için önemli bir önlem olmakla birlikte, saldırganlar bu donanım üzerinde de açık bularak cüzdana sızmaya çalışmaktadırlar. Dolayısıyla bu donanıma sahip olmak tek başına bir çözüm olarak görülmemelidir.

10.10. Değerlendirmeler

Madeni paraların gerçek değerleri bulunmakta iken kağıt paraların gerçekte değeri olmayıp, hükümetlerin garantisi altında güvenilirlik meydana getirmektedir. Kripto paralar ise hükümet desteği olmadıkça daha da az güvenilir olduğu açıktır. Keza Tablo 10.1'de kripto paranın Aralık 2017-Ağustos 2018 tarih aralığındaki toplam piyasa değeri dikkate alındığında, 9 aylık kısa bir periyotta ne kadar

değişken bir finansal enstrüman olduğu görülecektir. Bu değişkenlik yatırımcıların kripto paralara olan güvenilirliğini etkilemektedir ve piyasa oyuncusu olmak isteyenleri korkutan önemli bir unsurdur.

Bununla beraber Şekil 10.2, Şekil 10.4 ve Şekil 10.5'te görüleceği üzere, 2017-2019 arası 3 büyük kripto paranın fiyat hareketliliği yatırımcılarda risk algısının artmasına neden olmuş ve dolayısıyla kripto paranın güvenilirliği yatırımcılar tarafından daha fazla sorgulanmaya başlanmıştır.

Kripto para alım-satım işlemlerini gerçekleştirmek için gerek yurtiçi kaynaklı gerekse de yurtdışı kaynaklı çok sayıda web sitesi bulunmaktadır. Kullanıcılar kripto para alım-satım işlemlerini bu sistemler aracılığıyla gerçekleştirebilirler fakat öncelikli olarak bu sistemlere kaydolmalı ve hesap açmalıdırlar. Türkiye'de faaliyet gösteren bazı web siteleri hesap oluşturma ve sisteme kaydolma esnasında T.C. kimlik kartının da açıkça göründüğü kişisel fotoğraf istemektedirler. Bu durum, kötü niyetli kişiler düşünüldüğünde bir risk teşkil etmektedir. Sistemde kayıtlı kişiler, kripto para satın almak için web sitesinin belirtmiş olduğu IBAN numarasına kendi şahsi hesaplarından TL vb. para birimleri ile EFT yapmak zorundadırlar. Yine bu EFT işlemi sırasında, web sitesinin belirtmiş olduğu kodun EFT'nin açıklama kısmına girilmesi gerekmektedir. Öte yandan, kripto para satarken de kullanıcılar kendi şahsi hesap numaralarını sisteme girmektedirler ve satılan kripto paraların TL vb. para birimi karşılığı kişisel hesaplara yatmaktadır. Bu işlemler sırasında Google doğrulama kodu veya mobil onay kodu işlem güvenliğini artırmak için sistem tarafından istenmektedir. Tüm bu süreç dikkate alındığında, kullanıcıların web sitesine güvenmekten başka yapabilecekleri pek de bir şey bulunmamaktadır. Burada, güvenliği sağlayacak ve gizliliği koruyacak olan web sitesi ve doğal olarak sistemin arka planında çalışan güvenlik ve gizlilik mekanizmalarıdır. Bölüm 10.6, 10.7 ve 10.8'de anlatıldığı üzere, çok sayıda güvenlik zaafiyeti vardır ve araştırmacılar da sürekli olarak bu güvenlik problemlerine çözüm üretmeye çalışmaktadırlar. Dolayısıyla, kripto para alım-satım hizmeti veren sistemlerin, güncel güvenlik geliştirmeleri takip edilerek sürekli güncellenmesi gerekmektedir.

Kaynakça

[1]. Böhme, R., Christin, N., Edelman, B., Moore, T., "Bitcoin: Economics, Technology, and Governance", Journal of Economic Perspectives, 29(2), 213–238, (2015).

[2]. Çarkacıoğlu A., "Kripto-Para Bitcoin", SPK Araştırma Raporu, (2016).

[3]. Geiregat, S., "Cryptocurrencies are (smart) contracts", Computer Law & Security Review, 34(5), 1144-1149, (2018).

[4]. Ammous, S., "Can cryptocurrencies fulfil the functions of money?", The Quarterly Review of Economics and Finance, 70, 38-51, (2018).

[5]. Li X., Jiang P., Chen T., Luo X., Wen Q., "A survey on the security of blockchain systems", Future Generation Computer Systems, In Press, (2017).

[6]. Volety T., Saini S., McGhin T., Liu C.Z., Choo K.R., "Cracking Bitcoin wallets: I want what you have in the wallets", Future Generation Computer Systems, 91, 136-143, (2019).

[7]. Tüm Kripto Paralar, https://tr.investing.com/crypto/currencies [Erişim Tarihi: 17.02.2019].

[8]. Bitcoin, https://www.bloomberght.com/doviz/bitcoin [Erişim Tarihi: 17.02.2019].

[9]. Ethereum, www.bloomberght.com/doviz/ethereum [Erişim Tarihi: 17.02.2019].

[10]. Ripple, http://dovizgrafik.com/kripto/ripple [Erişim Tarihi: 17.02.2019].

[11]. Genel Grafikler, https://coinmarketcap.com/tr/charts [Erişim Tarihi: 17.02.2019].

[12]. En Yüksek Piyasa Değerine Sahip Kripto Paralar, https://www.99cryptocoin.com/tr/coinsbymarketcap/ [Erişim Tarihi:17 Şubat 2019].

[13]. Blokzincir, http://blokzincir.tubitak.gov.tr/bz-calistay/blok-zincir.html [Erişim Tarihi:18 Şubat 2019].

[14]. Mayer, H., "Ecdsa security in bitcoin and ethereum: a research survey", 2016, http://blog.coinfabrik.com/wp-content/uploads/2016/06/ECDSA-Security-in-Bitcoin-and-Ethereum-a-Research-Survey.pdf [Erişim Tarihi:18 Şubat 2019].

[15]. Hajdarbegovic, N., "Bitcoin miners ditch ghash.io pool over fears of 51% attack", 2014, http://www.coindesk.com/bitcoin-miners-ditch-ghash-iopool-51-attack/ [Erişim Tarihi:18 Şubat 2019].

[16]. Alliance, S., "Know your ransomware: Ctb-locker", 2017, https://www.secalliance.com/blog/ransomware-ctb-locker/ [Erişim Tarihi:18 Şubat 2019].

[17]. Wikipedia, "Wannacry ransomware attack", 2017, https://en.wikipedia.org/wiki/WannaCry_ransomware_attack [Erişim Tarihi:18 Şubat 2019].

[18]. Treasury, H., "UK national risk assessment of money laundering and terrorist financing", 2015, https://www.gov.uk/government/uploads/ system/uploads/attachment_data/file/468210/UK_NRA_October_2015_final_web.pdf [Erişim Tarihi:18 Şubat 2019].

[19]. Cody, W., Amir, T., "Darkwallet", 2017, https://darkwallet.is/ [Erişim Tarihi:18 Şubat 2019].

[20]. Christin, N., "Traveling the silk road: A measurement analysis of a large anonymous online Marketplace", The 22nd International Conference on World Wide Web, 2013, pp. 213–224.

[21]. Miller, A., Möser, M., Lee, K., Narayanan, A., "An empirical analysis of linkability in the monero blockchain", 2017. ArXiv preprint: arXiv:1704.04299.

[22]. Karame, G.O., Androulaki, E., Roeschlin, M., Gervais, A., Čapkun, S., "Misbehavior in bitcoin: A study of double-spending and accountability", ACM Transactions on Information and System Security, 18(1), 1-32, 2015.

[23]. Atzei, N., Bartoletti, M., Cimoli, T., "A survey of attacks on ethereum smart contracts (sok)", International Conference on Principles of Security and Trust, 2017, pp. 164–186.

[24]. Luu, L., Chu, D.-H., Olickel, H., Saxena, P., Hobor, A., "Making smart contracts smarter", The 2016 ACM SIGSAC Conference on Computer and Communications Security, 2016, pp. 254–269.

[25]. E. community, "The ''yellow paper'': Ethereum's formal specification", 2017, https://github.com/ethereum/yellowpaper [Erişim Tarihi:18 Şubat 2019].

[26]. Rivlin, B., "Vitalik buterin on empty accounts and the ethereum state", 2016, https://www.ethnews.com/vitalik-buterin-on-empty-accounts-and-theethereum-state [Erişim Tarihi:18 Şubat 2019].

[27]. Chen, T., Li, X., Luo, X., Zhang, X., "Under-optimized smart contracts devour your Money", IEEE 24th International Conference on Software Analysis, Evolution and Reengineerin, SANER, 2017, pp. 442–446.

[28]. Apostolaki, M., Zohar, A., Vanbever, L., "Hijacking bitcoin: Routing attacks on cryptocurrencies", IEEE Symposium on Security and Privacy, 2017, pp. 375–392.

[29]. D. SecureWorks, "BGP hijacking for cryptocurrency profit", 2014, https://www.secureworks.com/research/bgp-hijacking-for-cryptocurrency-profit [Erişim Tarihi:18 Şubat 2019].

[30]. Luu, L., Velner, Y., Teutsch, J., Saxena, P., "Smart pool: Practical decentralized pooled mining", USENIX Security Symposium, 2017, pp.1409-1426.

[31]. Gervais, A., Karame, G.O., Wüst, K., Glykantzis, V., Ritzdorf, H., Capkun, S., "On the security and performance of proof of work blockchains", The ACM SIGSAC Conference on Computer and Communications Security, 2016, pp. 3–16.

[32]. Baron, B., O'Mahony, A., Manheim, D., Dion-Schwarz, C., "National Security Implications of Virtual Currency", Rand Corporation, 2015.

[33]. He, D., Habermeier, K., Leckow, R., Haksar, V., Almeida, Y., Kashima, M., Kyriakos-Saad, N., Oura, H., Sedik, T.S., Stetsenko, N., Yepes, C.V., "Virtual Currencies and Beyond: Initial Considerations", International Monetary Fund, 2016(3), 2016.

[34]. Münzer, J., "Bitcoins: Supervisory Assessment and Risks to Users". 2014, https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Fachartikel/2014/fa_bj_1401_bitcoins_en.html [Erişim Tarihi:18 Şubat 2019]

[35]. Belçika Merkez Bankası. 2014, https://www.nbb.be/doc/ts/enterprise/press/2014/cp140114en.pdf [Erişim Tarihi:18 Şubat 2019]

[36]. Fransa Merkez Bankası, "The Dangers Linked to the Emergence of Virtual Currencies: The Example of Bitcoins", Focus, 10(5), 2013.

[37]. Heikkinen, P., 2014, "Bitcoin Involves Risks", https://www.suomenpankki.fi/en/media-and-publications/news/ 2014/bitcoin-involves-risks/ [Erişim Tarihi:18 Şubat 2019]

[38]. İsveç Merkez Bankası, "The Swedish Retail-Payment Market". Riksbank Studies. Stockholm, 2013.

[39]. Macheel, T., 2014, "French Government Outlines New Regulations for Bitcoin Market Transparency", http://www.coindesk.com/french-government-outlines-new-regulations-bitcoin-market-transparency/ [Erişim Tarihi:18 Şubat 2019]

[40]. Hern, A., 2013. "Bitcoin Price Tumbles After Warning from Chinese Central Bank". The Guardian, https://www.theguardian.com/

technology/2013/dec/05/bitcoin-price-tumbles-chinese-central-bank-warning [Erişim Tarihi:18 Şubat 2019]

[41]. BDDK, 2013. "Basın Açıklaması", https://www.bddk.org.tr/ WebSitesi/turkce/Duyurular/Basin_Aciklamalari/12574bitcoin_hk_basin_aciklamasi.pdf [Erişim Tarihi: 18 Şubat 2019]

[42]. Cointurk, 2014, "Türkiye'de Bitcoin Kabul Eden İşletmeler", http://coin-turk.com/turkiyede-bitcoin-kabul-eden-yerler/ [Erişim Tarihi:18 Şubat 2019]

[43]. Geekflare, 2018, "Cryptocurrency And Cyber Security – Are they Frenemies?", https://geekflare.com/cryptocurrency-and-cyber-security [Erişim Tarihi: 22 Temmuz 2019]

[44]. Fireeye, 2019, "Cryptocurrency and Blockchain Networks: Facing New Security Paradigms", https://www.fireeye.com/blog/threat-research/2019/01/cryptocurrency-blockchain-networks-facing-new-security-paradigms.html [Erişim Tarihi: 22 Temmuz 2019]

[45]. Alshamsi, A., Andras, P., "User Perception of Bitcoin Usability and Security Across Novice Users", International Journal of Human-Computer Studies, 126, 94-110, 2019.

[46]. Cryptocoinzone, 2019, "Which is the Best Bitcoin Hardware Wallet" https://www.cryptocoinzone.com/bitcoin-wallet/which-is-the-best-bitcoin-hardware-wallet [Erişim Tarihi: 22 Temmuz 2019]

Twitter'da Arkadaş Önerilerinin Teknoloji ve Bilgi Yönetimi Bakış Açısıyla Siber Güvenliğe Etkisi

BÖLÜM 11

A. Oğuzhan ALKAN

TWITTER'DA ARKADAŞ ÖNERİLERİNİN TEKNOLOJİ VE BİLGİ YÖNETİMİ BAKIŞ AÇISIYLA SİBER GÜVENLİĞE ETKİSİ

Hayatımızın her alanına nüfuz eden internete bağlı cihazların oluşturduğu nesnelerin interneti olarak adlandırılan yeni yaşam biçimi ve sosyal medya kullanımı toplanan büyük verinin analiziyle yeni yeni hizmetler sunulmasını sağlayarak hayatımızı kolaylaştırmakta, etkinliğimizi ve verimliğimizi arttırıp iş yapış şeklimizi ve günlük hayatımızı değiştirmektedir. Bunca olumlu yanıyla birlikte, sosyal medya aracılığı ile her türlü bilgi ve işlemin elektronik ortama taşınması ve kritik ve hassas bilgilerin de yoğun olarak sosyal medya uygulamalarında kullanılmasıyla birlikte güvenlik ihlallerini de hızla artırmaktadır. Bu bölümde, sosyal ağlarda teknoloji ve bilgi yönetiminin nasıl yapıldığına ve bu alanın siber güvenliğe etkisi açıklanacaktır. Bu kitap bölümünde ise bu sosyal ağlardan birisinde arkadaş önerilerinin nasıl oluştuğu, arka planda bu öneriler için uygun teknolojik sistemin ne olabileceği, bu konuya güvenlik bakış açısının ne olması gerektiğine dair bir öneride bulunulmuştur.

11.1. Giriş

Sosyal medya ve sosyal ağlar, ortak bir ilgiye yönelen, birbiriyle etkileşim içerisinde hareket eden bağlı bireyler veya kuruluşlardan oluşur. Günümüzde birçok sosyal medya platformu (Facebook, Linkedin, Snapchat, Twitter vb.) farklı alanlarda özelleşmiş olsa da, milyonlarca insan tarafından kullanılmakta, birçok insanın birden fazla sosyal medya hesabı bulunmakta ve kullanıcı sayısı da günden güne hızla artmaktadır. Web 2.0 teknolojisinden sonra internetin yayın ortamı kullanıcıların karşılıklı iletişim kurup geri dönüş-

lerinin alındığı daha interaktif bir ortam olmuştur. Neredeyse, tüm kullanıcıların sosyal hayatları ve hatta pratik yaşamları, bu ağlardaki faaliyetleriyle ilişkili olmuştur. Profillerinin tamamının veya bir kısmının paylaşılması, arkadaş grupları, izin dâhilinde ortak paylaşımların yapılması gibi özelliklerle ortak hobilere sahip kişileri bir araya getiren bir bilgi ve teknoloji yönetimi platformu haline gelmiştir.

Sosyal ağlar resmi olmadan benzer bir ilgi ile birbirine bağlanan bireylerin veya arkadaş gruplarının ortak bir platformu olarak tanımlanabilir. Bugün dünya üzerinde milyarlarca kişi bu ağları kullanıyor ve kullanım oranları da durmadan artıyor. Bazı ülkelerde insanlar sosyal medya organlarının hayatlarını nasıl etkilediği ve davranışlarını ne şekilde değiştirdiğinin farkındadır. Bu yüzden daha küçük yaşlardan, öğrencilere ve ailelere bilinçli sosyal medya kullanımı eğitimleri verilmektedir. Fakat tüm bunlara rağmen, insanların sosyal davranışlarını değiştirdiği de aşikârdır. Örnek olarak, on yıl önce hiç kimse yedikleri yemeğin veya gittiği tatilin fotoğraflarını paylaşmazken, şu anda günlük canlı yayınlar yapılmakta ve özel hayatın tüm zaman dilimleri sosyal ağlarda paylaşılmaktadır.

Bu popülerliğin arkasında ne olduğunu anlamak için önce sosyal ağları ve bu çalışmada esas alacağımız Twitter'ı tanımlamamız gerekiyor. Twitter kullanıcıların birçok kişi tarafından takip edilmesini sağlayan, kullanıcıların düşünce, duygu, haber gibi paylaşımlar yaptığı sosyal bir ağdır. 2006 yılında kurulan; günlük aktif 700 milyon civarında kullanıcısı olan, genel kullanıcı sayısının 1 milyara yaklaştığı ve ülkemizde ise 15 milyon civarında kullanıcısı olan bir sosyal ağdır.

Sosyal ağların bu denli kullanımının arkasındaki sebep ise sadece tanıdığınız insanlarla bir araya geldiğiniz bir platform değil, aynı zamanda yeni insanları ve yeni arkadaşları da bulduğunuz bir ortam yaratmasıdır.

Teknolojik tarafta arkasındaki sebep ise referans sistemleridir. Örnek olarak online alışverişin ve dijital pazarlama çalışmalarının artışı, sosyal medya ağları üzerinden satış sitelerine giriş yapılması arkadaş tavsiye sistemlerinin önemini son derece artırmıştır.

Benzer ürünlerin geriye dönük takip mekanizmalarına ve bölgelerdeki yoğun satış profillerine göre tavsiye edilen ürünlerin satışı artmıştır.

Sosyal ağlarda böyle bir öneri sistemi kullanıldığı belirgindir, arka planda kullandıkları teknik mekanizmayı açıklamamış olsalar da teknolojiyi doğru yönettikleri ve kullandıkları belirgindir. Gelecek bölümde, bu yaklaşım aktarılacak ve bilgi güvenliğinin nasıl sağlanacağına değinilecektir.

11.2. Problem Tanımı

Problemi tam olarak ortaya koymak için Twitter'ın çalışma mekanizmasını doğru analiz etmemiz lazım. Kullanıcıların metinsel olarak tweet diye adlandırılan yazıları paylaşmasına olanak sağlayan ve onu takip eden kullanıcıların görebildiği ve takipçilerin de aynı tweeti paylaşabildiği bir platformdur. Fakat takipçisi yok ise ya da yeni kayıt olmuş birisi ise Twitter'da bahse konu takip önerileri ile karşılaşır.

Örneğin; "Oğuzhan Alkan Twitter'da Okan Yeloğlu ile arkadaş oldu" bilgisi kayda değerdir. Çünkü bu bilgi sonucunda Oğuzhan Alkan'a Okan Yeloğlu'nun arkadaşlık önerileri benzerlik (aynı üniversite, ortak beğeni sayfaları, kurum, kuruluş, ilgi alanları, doğum yeri, yaş ortalaması vb.) oranının önem sırasına göre gelir. Bu bazen çeşitli sosyal medya organlarından olabileceği gibi, çeşitli web sitelerinden de veya internette dolaşırken "pop-up notification" şeklinde de gelebilir. Yine bazı durumlarda "tanıyor olabileceğiniz kişiler" butonu ile karşınıza çıkabilir ve var olan fotoğraflar üzerinden yüz taraması yapılarak, arkadaş olmadığınız kişileri de önermektedir.

Bu önerilerin arkasındaki kritik değerler; aynı ülkede aynı şehirde yaşayan insan olmanın yanı sıra popülaritesi yüksek hesap, eğlence, müzik, sanat, spor, siyaset organları arasından başlangıç olarak seçilir ve akabinde kullanıcı arasından bir seçim yaptığında bilgi yönetimi devreye girerek onunla ilişkisi bulunan daha anlamlı hesaplar önerilmeye başlar. Örnek olarak bu sosyal medya uygulamalarında okuduğunuz bölüm, çalıştığınız kurum ve ortak arkadaş sayınıza kadar bilgiler analiz edilip yönetilir ve bu ortak alanlara göre arkadaş önerileri belirlenir. Bu yüzden önerilerde aynı meslek

gruplarından kişileri görebilirsiniz. İlginize göre daha önce takip ettiğiniz sayfalar karşınıza çıkacaktır. Yani, kullanıcı hesap hakkındaki bilgi arttıkça, yönetimi daha kolaylaşır ve daha mantıklı arkadaş önerileri verilmeye başlar.

Twitter'ın bilgi yönetimine etkisine bir örnek verecek olursak; 2011 yılında Twitter üzerinde Bollen ve arkadaşları tarafından Dow Jones Industrial Average (DJIA) şirketlerinin hisse senetlerinin oranlarını tahmin için bir çalışma gerçekleştirilmiştir. Çalışmada günlük kapanış değerleri ile insanların Twitter'daki tutumları kullanılmış ve %86,7 oranla günlük artış/düşüş değerleri tahmin edilebilmiştir [3]. Twitter kullanıcılarının bilgileri toplanarak sonuca gidilmiştir. Arkadaş önerilerinin arkasında da bu bilgi yönetimi mekanizması yatmaktadır.

Fakat günümüzde teknolojinin hızla gelişmesi, yapay zekâ uygulamaları ve büyük veri çözümleri bu öneri mekanizmalarını teknolojik olarak bir sisteme oturtmakta ve otomatik olarak karşımıza çıkarmaktadır. Çalışmanın ilerleyen kısmında bu teknolojik yöntemlere değinilecektir. Büyük veriden nasıl değer elde edilir? Teknoloji yönetimi ile değer olarak karşımıza çıkacak doğru arkadaş önerileri yapmak adına teknoloji nasıl kullanılır? Bu ve benzeri sorulara çözüm önerileri bulmak gereklidir. Burada en temel husus, veriyi daha doğrusu büyük veriyi doğru okumak, yönetimini doğru yapmak, iyi analiz etmek ve eleme süzgecinden geçirmektir. Sosyal ağlardaki kullanıcıları, kullanıcıların takipçilerini veya takipçilerinin takipçilerini yani gelen tüm bilginin ölçümleri yapılarak, istatistiki bilgileri yani kullanıcılar arasındaki ilişkileri belirlemek için temel parametreleri ortaya koymak gerekmektedir.

11.3. Teknoloji Yönetimi ile Arkadaş Tavsiyesi

Twitter'ın 321 milyonu aşkın kayıtlı kullanıcısı vardır ve neredeyse günde 50 milyon tweet üretilmektedir. Twitter'da herkese açık ve özel hesaplardan oluşmaktadır. Bununla birlikte çok sayıda sahte Twitter hesabı ve sahte Twitter takipçileri adı verilen büyüyen bir iş ekosistemi oluşmuştur. Bu iş ekosisteminde sahte hesapların satılması sonucunda başka hesaplar sizi takip etmektedir.

Sahte takipçiler 1000 takipçi başına ortalama 18 $'lık bir fiyata satılmaktadır. Sahte hesapların toplam Twitter kullanıcılarının %4'ünü oluşturduğu tahmini dikkate alınırsa, pazarın büyüklüğü kolaylıkla öngörülebilir [12].

Dolayısıyla pek çok insan Twitter'da takipçi sayısının çok olmasını istese de bu durumun organizasyonlar ve bireyler için birçok tehdidi ortaya çıkabilmektedir. Mesela bir şirket için birçok sayıda sahte takipçi olması, gerçek takipçileri ile iletişim kurmasını engellemekte ve siber korsanlar için hedef niteliği taşımaktadır. Çünkü bir hacker birçok takipçisi olan bir hesabı ele geçirip üçüncü parti API gibi uygulamalara ciddi paralara satabilmektedir veya sizlerin hesabında zararlı linkler veya yazılımlar içeren birçok paylaşım yapabilir. Bu paylaşımlarda farklı hesapları da ele geçirebilir. Hesabınızı ele geçirdikten sonra kötü amaçlı kullanımın birçok senaryosunu aklınıza getirebilirsiniz.

Tavsiye sistemleri için en olumsuz senaryo işte bu hesaplardır. Diğer bir ifade ile satılan sahte hesapların gücünden yararlanarak, Twitter'da "Trend Olan Konular ve Hesaplar" aracılığı ile kolayca bir yönlendirme gerçekleştirilebilir. Bu da tavsiye sistemlerinin yanlış yönlendirmelerine sebep olur. Dolayısıyla çözüm olarak; tavsiye sistemleri için birçok teknolojik metot kullanılmaktadır.

Teknoloji yönetimini daha iyi anlatmak için grafik tabanlı bir öneri sistemini açıklayalım. Bu teknoloji; filtreleme ve karar verme olmak üzere iki temel işlemden oluşmaktadır; filtreleme yapılırken, işlenecek kullanıcıları azaltmak için daha yüksek olasılıklı düğümler kullanılır ve sıralama yapılır. Sıralama yapılırken kullanılan düğümlerin yoğunluğuna göre sıralamaya karar verilir.

11.3.1. Kullanılan Yöntemler

Literatürde pek çok tavsiye sistemi bulunmaktadır. Bu sistemler incelendiğinde; en başta dijital alanlarda kullanılan kalite filtresi gelmektedir. Twitter kullanırken haber akışınızda ilgilenmediğiniz konulara sizleri yönlendiren ve kişisel ilgi alanınızda görmek istemediğiniz birçok içerik karşınıza çıkmaktadır.

Kalite filtresini aktif hale getirdiğinizde, hesap kaynağı ve davranışı gibi çeşitli sinyalleri kullanarak gördüğünüz ve izlediğiniz Tweet'le-

rin kalitesi artabilir. Bu özellik sayesinde, yinelenen Tweet'ler veya otomatik görünen içerikler gibi düşük kaliteli içerikler filtrelenmiş olur. Takip etmediğiniz kişilerden ve yakın zamanda etkileşim kurmadığınız kişilerden ve hesaplardan, bildirim veya arkadaşlık isteği gelmez.

Bir diğer metot ise başka bir Twitter hesabını sessize almaktır. Sessize aldığınız hesabın Tweet'lerini görmeden o hesapla arkadaş kalmak adına harika bir seçenek sunar. Sadece takip ettiğiniz değil takip etmediğiniz hesapları da sessize alabilirsiniz ve bildirim akışlarınızda böylece bu hesapları görmezsiniz. Sadece bu hesaplar size mesaj gönderirse veya Tweet'lerde sizden bahsederlerse size bildirim gelir. Bu demek oluyor ki sessize almak, engellemekten farklıdır. Sessize alındığını bir hesabın öğrenme yolu ise yoktur. Ayrıca yine akıllı filtreleme metotları ile, belirli sözcük, ifade ve hashtag'leri barındıran Tweet'leri de sessize alabilirsiniz.

Engelleme özelliği ise belirli hesapların sizinle iletişim kurmasını, hesabınızı incelemesini ve sizin atmış olduğunuz Tweet'leri bir başkasının görmesine engel olur. Son olarak hassas içerik özelliği ile bir takım kritik medya görüntüleri belirmeden önce uyarı alabilirsiniz ve görmekten vazgeçebilirsiniz.

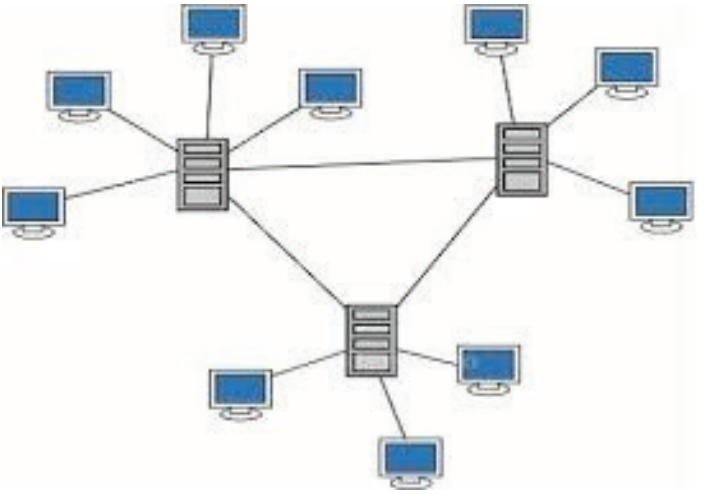
Tüm bu çözüm ve metotlar gereksiz bilgi yükünden kurtulmanızı, teknolojinin doğru yönetimi ile büyük verinin sosyal mühendislik saldırıları ile ele geçirilmesine engel olur ve siber saldırılara karşı korunmanızı sağlar.

11.3.2. Önerilen Sistem

Değinecek olduğum sistem, temel olarak sosyal ağların yapısal özelliklerine dayanmaktadır. Öneri mekanizması harekete geçerken önemli özelliklere sahip bir kullanıcı grubunu filtrelemek ve karar vermek için de sosyal ağların grafik topolojisini kullanmaktadır. Topoloji sonucunda ortaya çıkan kullanıcıların etrafında kümelenen kullanıcılar ve grafikte yanında ve yöresinde bulunan kullanıcılar, uzaklık sırasına göre önem derecesi verilerek karşımıza çıkmaktadır.

11.3.2.1. Filtreleme

Filtrelemeyi gerçekleştirmek için grafikte bahsettiğimiz kümelenme için katsayı(kümelenme katsayısı) kavramını bilmek gerekmektedir. Araştırmayı yaparken uyguladığımız yöntemde "rasgele seçilen birinden arkadaşınızı ya da arkadaşınızın bir arkadaşını tanıyor olmanın daha muhtemel" olduğu gerçeğini göz önünde bulunduruyuz. Böylece, filtreleme yaparken, kümelenme topolojisinde komşu düğümleri ve öneri mekanizmasında merkez düğüme yakın olan düğümleri seçerek başlarız.



Yukarıdaki topolojide her cihazı bir kullanıcı olarak düşünelim. Birbiriyle doğrudan ilişkili olan düğümleri seçmek öneri yapmak açısından daha mantıklıdır. Aksi takdirde iki ya da üç atlama ile ulaşacağımız arkadaş önerisi mantıksız olacaktır. Filtrelemenin temel mantığı da budur.

11.3.2.2. Karar Verme

Filtrelemeden sonra karar verme prosedürü ise katsayıların ölçümünün normalleştirilmesini içerir. Her bir düğümde var olan indeksleme değeri, en yakındaki öneri sürecinin bu düğümü ve merkezi düğümü arasındaki etkileşim gücünü ölçen bir işlemin sonucudur. Yani bir başka ifade ile arka planda teknolojinin doğru yönetiminin sonucudur diyebiliriz.

İndekslerin her biri kullanılarak arkadaş önerileri gerçekleştirilmektedir. Buradaki temel fikir, öneri adımında ana düğümün arkadaşlarını, elimizdeki arkadaş listesinin arkadaşına da dâhil ediyoruz. Son olarak arkadaş önerisi belirlenirken ise kabul edilen önerileri ilk % 10'luk öneri dilimine alarak, liste sıralamasını ve indeks değerini sürekli güncelleyen bir teknolojik metot kullanıyoruz. Belirttiğim gibi, sistemimizi kabul edilen arkadaş tavsiyelerinin ilk % 10'luk kısma alınması ile güncelliyoruz.

Özetle, sadece grafik topolojisini göz önünde bulundurduğumuzda bile teknoloji yönetiminin yanı sıra, bilgi yönetiminin sonucu olarak yukarıda anlattığımız gerçek arkadaş olmayan bazı popülaritesi yüksek kullanıcıları önermemizin bile mantıklı bir varsayım olduğunu düşünüyoruz.

11.4. Siber Güvenlik Bakış Açısıyla Değerlendirme

11.4.1. Genel Değerlendirmeler

Çalışmanın giriş kısmında bahsettiğimiz üzere siber uzay büyümesini durmadan sürdürmektedir ve büyüyen verinin güvenliği, yönetilmesi öncelik haline gelmiş durumdadır. Veri sızıntısı vakaları, siber saldırılar, ataklar, büyük veri güvenliği ve mahremiyetine kurumları yatırım yapmaya zorlamakta, güvenlik prosedürlerini yerine getirmeye mecbur bırakmaktadır. Bunun sonucu olarak dünya üzerinde pek çok siber saldırı vakası gerçekleşmiştir.

Dünya üzerinde yaşanan siber saldırılar sonucunda:

- 30 Milyar Sterlin civarında Birleşik Krallık, 100 Milyar dolar civarında Amerika'da siber saldırıların ülke ekonomisine zararı ölçüldüğünden; Birleşik Krallık 2 Milyar Sterlin, ABD ise 20 Milyar dolar bu alana yatırım yapacağını açıklamıştır.
- Oltalama saldırıları ile gerçekleşen fidye yazılımı 'WannaCry', 200'e yakın ülkede binlerce kurumda kesintilere neden olmuş ve verileri şifrelemiştir.
- Japonya'da 500 milyon dolarlık kripto para yok olmuştur.

- Sesleri dinleme özelliği bulunan casus yazılım Skygofree, WhatsApp'ın mesajlarına erişmiş ve sonucunda ciddi zararlar ortaya çıkmıştır.
- Siber saldırı eğitimleri Kuzey Kore'de ilgili öğrencilere verilmeye başlamıştır.
- Siber ordular İran'da caydırıcı güç olarak kurulmuştur.
- İngiltere'de 20 bin civarında siber güvenlik uzmanı yetiştirmek adına ilgili bakanlık bünyesinde özel bir kurum kurulmuştur.

Siber saldırıların ülkemize etkileri:

- Tüm nüfus kayıtlarının tutulduğu MERNİS hack'lenmiş ve veriler sızdırılmıştır.
- Milli Eğitim Bakanlığı'nın tüm öğretmen kayıtlarını tuttuğu İLSİS hack'lenmiş ve veriler sızdırılmıştır.
- Tüm dava dosyalarının ve adli vakaların tutulduğu UYAP hack'lenmiş ve veriler sızdırılmıştır.
- Rus savaş uçağını düşürmemizin hemen akabinde, tr. uzantılı sitelerin alan adı tahsisini yapan ODTÜ Alan Adı Servisi'ne ciddi bir saldırı olmuş ve birçok site ve altyapı (banka ATM'lerine kadar) kullanılamaz hale gelmiştir.

Yani birçok şifreleme algoritması geliştirilmesine ve güvenlik prosedürü uygulanmasına rağmen bu çapta büyük bilgi ve verilerin güvenliği tam olarak sağlanamamıştır. Çünkü büyük veri heterojen yapıdadır. Kaynağı ve altyapısı farklılık gösterdiği için güvenliğinin sağlanması zorlu süreçleri beraberinde getirmektedir. Twitter'da karşımıza çıkan arkadaş önerileri de bu büyük verinin doğru okunmasının ve anlamlandırılmasının karşılığıdır. Gizlilik ayarları doğru şekilde yapılmayan hesapların, tüm içeriklerine ve arkadaş çevrelerine ulaşılabileceği gibi, sık paylaşımlarda ve etiketlemelerde bulunulan kişiler üzerinden öneriler karşımıza çıkabilecektir. Bu zaman zaman spam şeklinde, zaman zaman pop-up notification aracılığı ile uygulama kullanımında karşımıza çıkabilmektedir. İşte bu durum tam olarak teknolojinin ve bilginin yönetimiyle ve doğru filtrelemelerin uygulanması ile kullanıcıların karşısına çıkmaktadır. Kimlik avı saldırıları ve şifrelere ulaşılarak hesapların ele geçirilme-

si, klon hesaplar ile ve ilgi alanlarında; hesap sahipleri tarafından takibi sürdürülen asılsız sayfalar üzerinden gelen oltalama mesajları ve linkleri ile gerçekleşmektedir. Kimi zaman takipçi sayısını artırmak için kabul edilen öneriler, insanların algısını yöneterek aslında gerçek arkadaşı olmayan kişiler üzerinden, insanların saldırılara maruz kalmasına ve hesaplarının ele geçirilmesine neden olmaktadır.

Burada yapılması gereken bilinçli bir Twitter kullanıcısı olarak, sosyal mühendislik saldırılarına karşı, hesapların güvenlik ayarlarının yapılması ve arkadaş önerilerinin bilinçsiz bir şekilde kabul edilmemesidir. Alınması gereken diğer tedbirler bir alt başlıkta detaylandırılmıştır.

11.4.2. Siber Güvenlik ve Mahremiyet Çözümleri

Günümüzde insanlar gerek sosyal medya hesaplarında (twitter, facebook etc.) gerekse internette zaman geçirirken istemli veya istemsiz olarak bilgi paylaşımına neden olmaktadır ve maalesef birçok bilgilerini bilinçsiz bir şekilde paylaşmaktadır. Önemsenmeden paylaşılan bu veriler, büyük veri teknolojisi için de özlük bilgilerimiz dâhil, tüm bilgiler işlenmektedir. Takibini yapamadığımız bu bilgiler bazen dijital pazarlama şirketlerine satılmakta ve iznimiz olmadan kullanılmaktadır. Ülkemizde kurulan KVKK (Kişisel Verileri Koruma Kurumu) 2016 Nisan ayından itibaren verilerimizi korumak adına devreye girmiş olsa da birey bazında bizler bilgilerimizi paylaşırken bilinçli olmak durumundayız.

Büyük veri güvenliği teknik çözümlerle sağlansa da, her kapıyı açan bir kilit üretildiği gibi her sisteme yönelik bir zafiyet de bulunmakta ve teknik çözümler bir süre sonra yetersiz kalmaktadır. Kriptoloji algoritmaları kırılmakta, her kuruluşun çözümü bir şekilde yetersiz kalabilmektedir. Yukarıda bahsettiğim örnekler, dünya devlerinin başına gelen saldırılardan alınmaktadır. Dolayısıyla teknik çözümlerin yanında sosyal mühendislik çözümlerine ve farkındalık çalışmalarına ağırlık verilmesi ve teknolojinin ve bilginin bilinçli bir şekilde yönetilmesi gerekmektedir.

Çözüm önerileri olarak;

i. Sorumlu Kişi Belirleme

Sosyal medya organlarından elde edilen büyük veriyi kullanan ve işleyen kurum ve kuruluşlar, paylaşılan verileri ve bulut mimarileri takip edecek, sosyal medyada kullanıcıların davranışlarını gözden geçirerek onlara hata yaptığında uyarılarda bulunacak bir departman oluşturabilir, böylece veri sızıntısını asgari düzeyde tutmak adına önemli bir adım atabilirler.

ii. Hukuki Yaptırımlarda Bulunma

Güvenlik prosedürü tanımlayarak, gereksiz bilgi ve verilerin sızdırılması ve üçüncü şahıslarla paylaşılması durumunda, cezai müeyyidelerde bulunarak caydırıcı güç kullanabilirler.

iii. Risk Analizi Yapma

Veri tabanında tutulan verilerin ve kritik altyapıların önem derecesine göre sıralanıp sınıflandırılması, gizlilik risk analizi yapılması ve o ölçüde korunması fayda sağlayabilir. Yapılan iş ve işlemler de aynı analize göre sınıflandırılarak, risk önemine göre yönetici onayına tabi tutulabilir.

iv. Takip Mekanizması

Sosyal medya organlarındaki verilerin sızdırılması ve izinsiz giriş trafiği gözlemlenerek ihlal tespit edildiğinde otomatik tepki verecek bir uygulama ve platform kullanmak da (SIEM gibi) teknik bir çözüm olarak sunulabilir. Bu ve bunun gibi birçok çözüm sosyal medyada farkında olmadan üçüncü şahıslar ile paylaştığımız, sahip olduğumuz teknoloji ile bilginin yönetiminin doğru bir şekilde yapılmasında ve kritik verilerin korunmasında ve belirli bir kalite düzeyinde kalmasında ve zararın minimize edilmesinde ciddi önem arz etmektedir.

11.5. Değerlendirmeler

Sonuç olarak, sosyal medyayı günümüz dünyasında çok yoğun bir şekilde insanlar farklı aktiviteler için kullanıyor. Bu platformlar hem çok eski bir arkadaşın bulunabildiği ve yeni arkadaş edinilebilen hem de sosyal çevrenizin tüm bilgilerine anında kolayca erişebile-

ceğiniz bir medya organı haline gelmiştir. Ortak bir ilgi ile birbirine bağlanan kişilerden oluşan bu ortamlarda arkadaş öneri sistemleri, e-ticaretin sonucu olarak ortaya çıkmış, internet üzerinde satış yapan kurumların daha önce satın alınan ürüne göre reklam kampanyalarını yürüterek satışlarındaki artışı gözlemlemesiyle sosyal medya ağlarında da teknolojinin ve bilginin yönetilmesine odaklanarak kullanılmaya başlanmıştır. Şu anda bu arkadaş önerileri sistemi sosyal medya organları tarafından ciddi şekilde kullanılmaktadır. Her ne kadar mekanizmaları belirtilmemiş olsa da bugün için kullanılan yöntemlerin temelinde bilgi ve teknoloji yönetimi olduğu aşikârdır. Çünkü bu yöntemler genellikle sosyal ağın grafik topolojisi (teknoloji yönetimi ile ilişkili olarak) ve arkadaşların arkadaşları (bilgi yönetimi ile ilişkili olarak) önerilerine dayanmaktadır.

Örnek olarak Instagram, Facebook ile bağlantılıdır ve arkadaş önerilerinde karşınıza ilk olarak Facebook arkadaşlarınız çıkar, bu platformlara rehberiniz bağlıysa, önerilerde rehberinizdeki arkadaşlarınızı da görebilirsiniz. Twitter'da daha önce sayfasını incelediğiniz ve takip ettiğiniz sayfalar, önerilerde üst sıralarda karşınıza çıkmaktadır. Arkadaş önerileri arasında **profiline bakan kişiler**, profilime kim baktı, profilime bakanları nasıl öğrenirim gibi sorularla karşılaşmış olmanız da arka planda bilginin ve teknolojinin yönetiminin önemini doğrular niteliktedir. Fakat sosyal medya verilerini kullanarak yorumlama yapan ve analiz gerçekleştiren kişilerin karşılaştığı problemler ise paylaşım yapan kişilerin Twitter'da paylaşım yaparken; emoji, kısaltma ve farklı dillerde halk ağızı ile paylaşım yapmasıdır. Dolayısıyla sosyal medya hesapları üzerinden halkın görüş ve düşünce analizi ile duygu yorumlaması yapmak zorlaşmaktadır. Dolayısıyla tüm siber saldırıların temelini oluşturan sosyal mühendislik saldırıları ve sosyal ağlar aracılığı ile siber istihbarat faaliyetleri, bilgi ve veri toplama aracılığı ile oltalama saldırıları, kısaca veri bilimciliği alanında sosyal medya uygulamaları tam bir veri kaynağı niteliği taşımaktadır.

Özetle, Twitter, Facebook gibi uygulamaların artması ile siber tehdit ve tehlikeler olağan üstü artış göstermekte olup bu durum ülkeler, kurumlar ve bireyler için sosyal mühendislik saldırılarında hayati hale gelmektedir. Tüm bu büyük veri paylaşımının bilinçli bir şekilde yapılması ve kullanıcıların farkındalık eğitimleri ile desteklenmesi gerekmektedir.

Bu konuda atılması gereken adımlar ve alınması gereken tedbirler aşağıda maddeler halinde verilmiştir:

- Twitter'da güvenli bir hesap oluşturmanın ilk adımı zor bir şifre seçmektir ve şifre sıfırlama adımlarında e-posta ve telefon numarası ile iki adımlı güvenli doğrulama altyapısı oluşturulmalıdır.
- Kimlik hırsızlıklarının en fazla yapılan yolu oltalama saldırılarıdır. Gerek e-postanıza gerekse de direkt SMS yoluyla gelen ve içeriği bilinmeyen linklere asla tıklanmamalıdır.
- Kullanılan hesaba ek güvenlik sağlamak adına kullanılan tarayıcıları güncellemek veya güncel tarayıcı kullanmak ve tehditlere karşı yayımlanan yamaların güncel tutulması gerekmektedir.
- Giriş onaylama adımı kullanarak, farklı bir cihazdan hesabınıza giriş yaptığınızda, ek bir güvenlik olarak size e-posta bildiriminde bulunulur. Böylece, hesabınızın ele geçirildiğinden şüphelenirseniz, hesabınızı kendiniz sıfırlayarak güvenli hale getirebilirsiniz.
- Olumsuz durumlarda karşılaşıldığında kullanıcıların "Hukuki Yaptırımlarda Bulunma" hakkını kullanma, karşılaşılabilecek tehdit ve tehlikeleri öngörmek için "Risk Analizi Yapma" ve nasıl bir takip mekanizmasının çalıştığının bilinmesinin önemini bir kez daha hatırlatmak isteriz.
- Sosyal medya şirketlerinin kullanıcı davranışlarını gözden geçirerek yapılan hatalarda ve yapılmayan eksikliklerde uyarı gönderecek sistemleri sunmaları için adım atmalarını istemek gerekmektedir.
- Son olarak, sosyal medya uygulamalarında yaygın olarak kullanılan arkadaş önerilerinin bizlere sağladığı katkılar kadar bizleri de olumsuzluklara iteceği veya olumsuzluklarla karşılaşmamıza sebep olabileceğinin farkında olunmalı, gerek kişisel mahremiyetimize gerekse arkadaşlarımızın da mahremiyetini ihlal edebileceğinin farkında olunmalı, bu bölümde açıklanan diğer hususlara dikkat edilmesi, farkındalığın artırılması, gereken önlemlerin alınması, karşılaşılacak ihlalleri ve oluşabilecek zararları en aza indirecektir.

Kaynaklar

[1] Yang, M. C., & Rim, H. C. (2014). Identifying interesting Twitter contents using topical analysis. *Expert Systems with Applications*, 4330–4336.

[2] Omand, S., Bartlett, J., & Miller, C. (2012). Introducing Social Media Intelligence(SOCMINT). *Intelligence and National Security*, 801-823.

[3] Agnihotri, R., Kothandaraman, P., Kashyap, R., & Singh, R. (2012). Bringing Social into Sales- The Impact of Salespeoples Social Media Use on Service Behaviors and Value Creation. *Journal of Personal Selling & Sales Management*, 333-345.

[4] Alkan, M. (2012). *Siber Güvenlik ve Siber Savaşlar.* Ankara: Siber Güvenlik Siber Savaşlar TBMM İnternet Komisyonu.

[5] Ernst, M. Sosyal ağ ve öneri sistemleri, 2013 (7 Nisan 2016).

[6] Silva, N.B., Tsang, I.R., Cavalcanti, G. D. ve Tsang, I.- J. Genetik algoritma kullanarak grafik tabanlı bir arkadaş önerme sistemi. Evrimsel Hesaplamada (CEC), 2010 IEEE Kongresi (2010), IEEE, pp. 1–7.

[7] Bollen, J., Mao, H., & Zeng, X. (2011). Twitter mood predicts the stock market. *Journal of Computational Science*, 1-8.

[8] S. Savaş, N. Topaloğlu, Sosyal Medya Verileri Üzerinden Siber İstihbarat Faaliyetleri, 2016

[9] Haber, Mynet (2015, 07 04). *Sultanahmet'te Çinli sandıkları Koreli turist grubuna saldırdılar*. 08 10, 2015 tarihinde Mynet Haber: http://www.mynet.com/haber/guncel/sultanahmette-cinli-sandiklari-koreli-turist-grubuna-saldirdilar-1909429-1

[10] Cumhuriyet. (2015, 07 09). *Bu sefer de Çinli sanılan kadını dövdüler*. 08 10, 2015 tarihinde Cumhuriyet:

[11] Weichselbraun, A., Gindl, S., & Scharl, A. (2014). Enriching semantic knowledge bases for opinion mining in big data applications. Knowledge-Based Systems, V.69, October 2014, Pp.78-85; https://doi.org/10.1016/j.knosys.2014.04.039

[12] Avcı, G. (2004). İstihbarat Teknikleri: Aktörleri - Örgütleri ve Açmazları. İstanbul: Timaş Yayınları.

[13] Özdağ, Ü. (2010). İstihbarat Teorisi. Ankara : Kripto Yayınları.

[14] Otte, E., & Rousseau, R. (2002). Social network analysis: a powerful strategy, also for the information sciences. Journal of Information Science, 441-453.

https://doi.org/10.1177/016555150202800601

[15] Blogger, G. (2012, 05 24). *Tools for Transparency: A How-to Guide for Social Network Analysis with NodeXL*. 08 15, 2015 tarihinde Sunlight F: https://sunlightfoundation.com/blog/2012/05/24/tools-for-transparency-a-how-to-guide-for-social-network-analysis-with-nodexl/

[16] Otte, E., & Rousseau, R. (2002). Social network analysis: a powerful strategy, also for the information sciences. *Journal of Information Science*, 441-453.

[17] Blogger, G. (2012). *Tools for Transparency: A How-to Guide for Social Network Analysis with NodeXL*. 08 15, 2015 tarihinde Sunlight F: https://sunlightfoundation.com/blog/2012/05/24/tools-for-transparency-a-how-to-guide-for-social-network-analysis-with-nodexl/

[18] Fitton, L. Gruen, M.E. Poston, L. (2010). Twitter for Dummies, USA: Wiley Publishing.

Siber Güvenlik Teknolojileri

BÖLÜM 12

Ali Hakan IŞIK

SİBER GÜVENLİK TEKNOLOJİLERİ

Günümüz bilişim teknolojilerindeki hızlı gelişmelere ve internet bağlantı kapasitesindeki üstel büyümeye bağlı olarak siber güvenlik teknolojilerinde kayda değer ilerlemeler görülmektedir. Verinin bilgiye dönüşümünde önemli bilgi birikimine sahip olunmasına rağmen siber güvenlik konusunda halen farkındalık ve teknoloji sorunları ile karşılaşılmaktadır. Bilgi ve iletişim teknolojileri, protokol, yazılım ve donanımlardaki gelişmeler, siber güvenlik ihtiyaçlarını tam olarak karşılayamamaktadır. Bu nedenle, yazılım tabanlı çözümler ile söz konusu ihtiyaçlar giderilmeye çalışılmaktadır. Bu durum, hız ve kapasite kaybına neden olmaktadır. Ayrıca, siber güvenlik alanında dünyanın önde gelen firmalarının kaydedeğer parasal kayba uğramalarına bağlı olarak, siber güvenlik teknoloji yatırımlarına hız verilmiştir. Bu noktada, sosyal medya, sağlık, nesnelerin internet, bulut bilişim, yapay zekâ, büyük veri önemli yatırımların yapıldığı temel siber güvenlik teknolojileri arasında yer almaktadır. Bu kitap bölümünde, söz konusu temel alanlardaki yenilikçi siber güvenlik teknoloji çözümleri ile anti-virüs, anti-casus, anti-spam filtreler, IDS/IPS, güvenlik duvarları ve hibrit sistemler, şifreleme teknolojileri, açık anahtar altyapısı, erişim kontrol teknolojileri ayrıntılı olarak irdelenmiştir. Son olarak, bu bölümde gelecekteki siber güvenlik teknolojileri araştırmalarının yönelimi konusunda değerlendirmeler paylaşılmıştır.

12.1. Giriş

Ülkelerin, şirketlerin veya kurumların BT altyapıları büyük ölçüde bilgisayar ağlarına, bilgi teknolojilerine, BT çözümlerine bağımlıdır. Siber saldırılar, bilgi teknolojisine olan bağımlılık arttıkça daha çekici ve potansiyel olarak daha da felaket ile sonuçlanma eğilimindedir. McAfee ve CSIS (Stratejik ve Uluslararası Çalışmalar Merkezi)

raporuna göre küresel siber suç maliyetleri 2017'de 600 milyar doları aşmıştır [1]. Geçmiş siber suç rakamlarına dayanan tahminlere göre siber suçun, 2021 yılına kadar yılda 6 trilyon dolar zarara yol açacağı tahmin edilmektedir [2]. Siber suç, dünyadaki her şirket için en büyük tehdittir ve insanlık ile ilgili en büyük sorunlardan biridir. İnternetin anonim doğası nedeniyle tespit ve takibinin zor olması nedeniyle siber saldırılar gün geçtikçe artmaktadır. Sebepleri ise siber saldırıların fiziksel saldırılardan daha ucuz, hızlı ve daha az riskli olmasıdır. Siber saldırıların sadece bir bilgisayar ve internet bağlantısı ötesinde ilave masraf gerektirmemesi de söz konu saldırıların artışındaki diğer bir nedendir. Bilgi teknoloji sistemlerine yönelik saldırıların çok çekici ve kazançlı olduğu göz önüne alındığında, siber saldırıların sayısının ve karmaşıklığının büyümeye devam etmesi beklenmektedir [3]. Bu noktada, siber saldırıların önüne geçmek için siber güvenlik teknolojilerine olan yatırımlar ve araştırmalar üstel bir şekilde artmaktadır.

Bu kitap bölümü üç kısımdan oluşmaktadır. İlk bölümde, güvenlik teknolojilerine değinilmiştir. İkinci bölümde, sosyal, nesnelerin interneti, sağlık ve büyük veri alanlarındaki siber güvenlik teknolojileri ve son bölümünde ise belirtilen alanlardaki teknolojilerin birlikte çalışabilirliği ve gelecekteki olası katkıları ve karşılaşılabilecek olumsuz durumlar hakkında değerlendirmeler sunulmuştur.

12.2. Güvenlik Teknolojileri

Güvenlik teknolojileri bölümünde, anti-virüs, anti-casus, anti-spam filtreler, IDS/IPS, güvenlik duvarları ve hibrit sistemler, şifreleme teknolojileri, açık anahtar altyapısı, erişim kontrol teknolojileri ayrıntılı bir şekilde geçmişten günümüze kullanılan yaklaşımlar incelenmiş ve kısaca tanıtılmıştır.

12.2.1. Anti-virüs Yazılımları

Anti-virüs yazılımlar ile diğer zararlı yazılımların engellenmesi, tespit edilmesi ve kaldırılması için tasarlanmış yazılımlardır [4]. Anti-virüs yazılımları, çalıştırıldığında diğer bilgisayar yazılımlarını değiştirip, kendi kodunu ekleyerek kendisini çoğaltan virüslere karşı güvenlik önlemi sağlamaktadır. Anti-virüs, imza

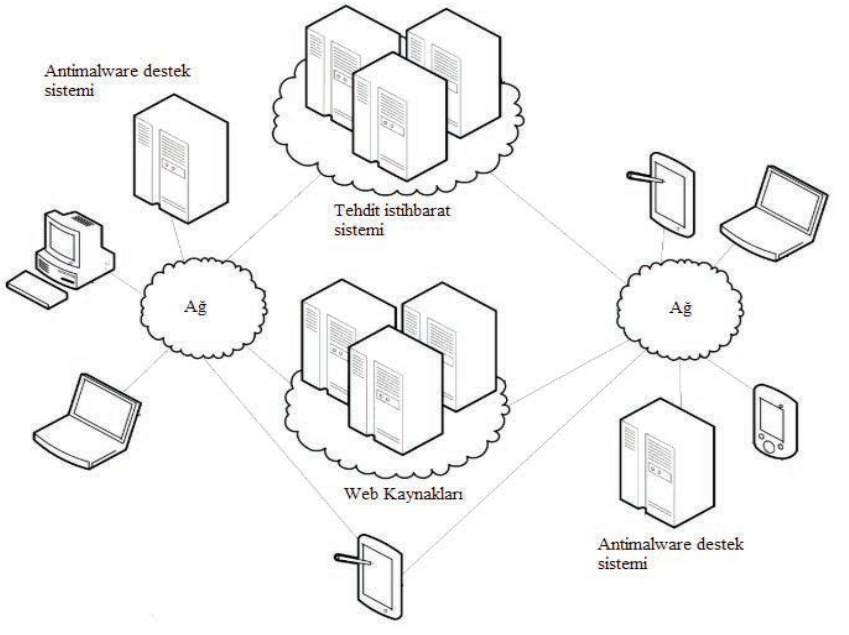
tabanlı ve davranış tabanlı algılama ile zararlı yazılımlara karşı koruma sağlamaktadır. İmza tabanlı algılamada, dosya tarama ve virüs imzalarını eşleştirme ile analiz yapılmaktadır. Böylece zararlı yazılım karantina altına alınmakta veya silinmektedir. Davranış tabanlı algılamada ise zararlı yazılımın bellek, ağ veya dosya sistemine zarar verebileceği dosya yükleme, bağlantı açma, sistem kaydı (registery) değiştirme, dosya oluşturma/değiştirme davranışı ile tehdit algılanmaktadır. Daha sonra ise belirlenen istenmeyen program davranışı engellenmektedir. Şekil 12.1'de ise davranışı daha iyi anlatmak için bir bilgisayar virüs karikatürü verilmiştir.

Şekil 12.1 Bilgisayar Virüsü [5]

12.2.2 Anti-casus Yazılımlar

Anti-casus yazılımları ise kötü amaçlı yazılımlar, truva atları, solucanlar gibi zararlı yazılımların engellenmesi, tespit edilmesi ve kaldırılması için tasarlanmış ve kullanılan yazılımlardır. Bu yazılımlar, truva atları, casus yazılımlar, fidye yazılımlar ve Trojanlar ile kullanıcıların bilgisi olmadan bilgisayarlara erişim sağlayıp, zarar vermek için geliştirilmiş kötü amaçlı yazılımlara karşı koruma sağlamaktadır [6]. Anti-virüs ile anti-casus arasındaki temel fark, anti-virüslerin internet veya harici bellek gibi bilinen kaynaklardan

gelen güncel ve/veya belirlenmiş tehditlere karşı, anti-casus yazılımların ise daha önce karşılaşılmamış kaynaklardan gelen zararlı olduğu kesin belirlenemeyen veya karar verilemeyen yazılımlara karşı koruma sağlamasıdır. Her ne kadar anti-casus yazılımlar, yapay zekâ teknikleri kullanarak kesin belirlenemeyen tehditlere karşı güvenlik önlemi sağladığı iddia edilse de yeterli eğitim verisi olmadan kötücül yazılımlara karşı söz konusu yazılımların yeterli koruma sağlayacağı önemli bir tartışma konusudur. Önümüzdeki yıllarda yeni nesil kötücül yazılım verilerin artması, kullanıcıların bilinçlenmesi ve kullanıcı geri dönüşleri ile daha etkin korumanın sağlanabileceği düşünülmektedir. Bu durum ile beraber birçok bilgisayar kullanıcısı, bilgisayarlarını kötü amaçlı yazılımlardan uzak tutmak için koruma yazılımlarına güvenmesi ve kullanmasına rağmen, zararlı yazılımların yaygınlaştığı, bazı sahte yazılımların kullanıcılara yüksek ücretlerle satılıp, herhangi bir koruma önlemi sağlamadığı son araştırmalar ile ortaya konulmaktadır [7, 8]. Şekil 12.2'de görüldüğü gibi ağ üzerindeki web kaynakları anti-casus yazılım sistemleri ile hem desteklenmekte hem de korunmaktadır.



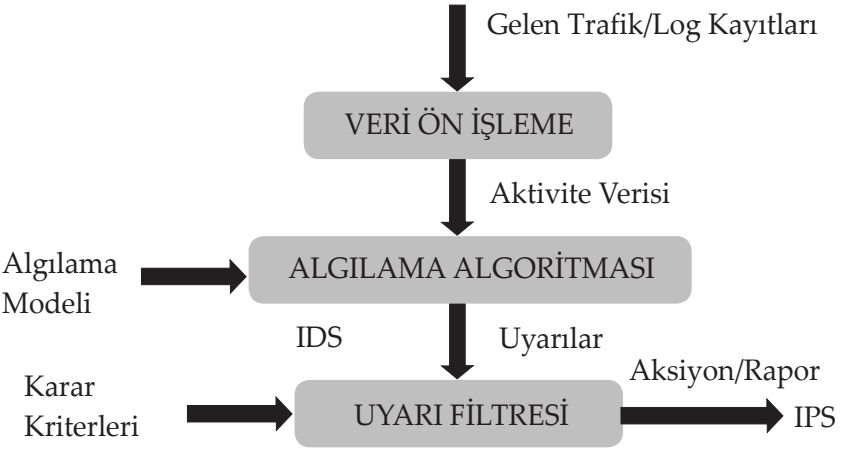
Şekil 12.2. Anti-casus sistem mimarisi [9]

12.2.3 Mesaj Sağanağı (Anti-spam) Filtreleri

Mesaj sağanağı bilgileri, internet erişiminin yaygınlaştığı günümüzde kurumsal şirketlerden bireysel kullanıcılara kadar pek çok unsura önemli zararlar vermektedir. İnternet trafiğinde spam bilgilerin büyüklüğü gerçek bilgilerin büyüklüğünden kat ve kat fazla olduğu ortaya konulmuştur [10]. Bu kapsamda, söz konusu e-posta mesaj sağanağı ve benzeri bilgilerin engellenmesi amacıyla anti-spam filtreler sıklıkla kullanılmaktadır. Söz konusu filtreler, mesaj sağanağını tanımlayıp, genel özelliklerini belirlemekte ve tanıma göre de filtreleme yapmaktadır. Bu süreçteki en önemli sorun, yaygın olarak kullanılmakta olan basit e-posta aktarım protokolünün (SMTP), mesaj kaynağı kimliğini kontrol etmede güvenilir bir mekanizma sağlamamasıdır. Bu sorunu çözmek için gönderen kimliğinin tanımlanması amacıyla SPF (Sender Policy Framework), DMP (Designated Mailers Protocol), TEOS (Trusted E-Mail Open Standard) ve benzeri yazılım ve protokoller geliştirilmiştir [11-13]. Günümüzde anti-spam filtrelemede makine öğrenmesi veya yapay zekâ yöntemleri sıklıkla kullanılmaktadır. Öğrenmeye dayalı anti-spam filtreleme ile spam sorununa önemli bir çözüm getirilmiştir. Söz konusu filtreleme, spam ve gerçek e-postaların otomatik olarak sınıflandırılması olarak tanımlanmaktadır [14]. Böylece kullanıcıların gereksiz zaman kaybı yaşamasının önüne geçilmekte ve zaman tasarrufu sağlanmakta ve verimlilik ise artmaktadır. Çeşitli spam filtreleme algoritmaları, e-posta iletimi aşamalarında uygulanmaktadır. Söz konusu aşamalar, yönlendirici, gidilecek e-posta sunucusu, gidilecek e-posta kutusudur. Birçok spam filtreleme yöntemi, yapay zekâ tabanlı öğrenmeye dayalı sınıflandırma tekniklerini kullanmaktadır. Söz konusu yöntemlerde e-posta mesajlarının büyüklüğü, içeriği, başlığı öznitelik olarak kabul edilip, elde edilen veriler işlenerek sınıflandırma gerçekleştirilmektedir. Resim tabanlı filtrelemede ise OCR ve benzeri öz nitelik çıkarma teknikleri ile elde edilen veriler kullanılmaktadır. Bu alanda literatürde en çok kullanılan yöntemler naive bayes, destek vektör makineleri ve kNN olduğu görülmüştür. Söz konusu bilinen algoritmalar dışında, anti-spam filtrelemeye özel yeni algoritmalar da geliştirilmektedir [14, 15].

12.2.4. Saldırı Tespit ve Önleme Sistemleri (IDS/IPS)

Bilgi ve veri akışlarının koruma altına alınması, geçmişten günümüze en önemli çalışma alanlarından biri olmuştur. Bu kapsamda, saldırı tespit ve önleme sistemleri bilgi güvenliği için en önemli araçlardan biri haline gelmiştir. Modern IDS'nin gelişmesinden önce, izinsiz giriş tespiti, anormal durumların log ve benzeri kayıt dosyaları üzerinde incelenmesinden oluşmaktaydı. Fakat günümüzde yeni araştırmalar ile saldırılar tespit edilebildiği gibi saldırı olmadan olası örüntülerde belirlenebilmektedir [16]. Literatürdeki IDS çalışmaları, anormal durumların istatistiksel, bilgi ve makine öğrenmesi tabanlı analiz edilmesi üzerine odaklanmıştır. İstatistik tabanlı anormal durum analizinde, normal aktivite hakkında önceden bilgi gerekli olmayıp, kötü amaçlı faaliyetlerin doğru bildirimi ile tek değişkenli, çok değişkenli ve zaman serisi model ile analiz gerçekleştirilmektedir. Bilgi tabanlı anormal durum analizinde, yüksek öneme sahip bilgiler açıklama dilleri, uzman sistemler ve sonlu durum makineleri ile değerlendirme yapılmaktadır. Makine öğrenmesi tabanlı anormal durum analizinde ise yüksek kaynak tüketimi ile bayes ağları, markov modelleri, nöral ağlar, bulanık mantık, genetik algoritma ve kümeleme teknikleri kullanılarak örüntünün sınıflandırılması yapılmaktadır [17, 18].



Şekil 12.3. IDS/IPS bilgi güvenliği mekanizması [19]

Son yıllarda DDoS ve diğer saldırıların artması sonucunda IDS'in yanı sıra bu saldırıları engelleyecek IPS cihazlarına yoğun ihtiyaç

duyulmaya başlanmıştır. Şekil 12.3'de verilen ve son yıllarda bilgi güvenliği için IDS ve IPS sistemleri beraber kullanılmaktadır. Öncelikle IDS'lerde bulunan algılama algoritmaları ile tehditler algılanmakta daha sonra çeşitli uyarı filtrelerinin bulunduğu IPS'ler ile tehditler raporlanmakta ve/veya tehditlere karşı çeşitli aksiyonlar oluşturulmaktadır [19].

12.2.5. Güvenlik Duvarları ve Hibrit Sistemler

Güvenlik duvarları, iki ağ arasında ilk güvenliği sağlayan ortak bir güvenlik savunma cihazıdır. Statik paket filtreleme özelliğine sahip güvenlik duvarları, ana bilgisayar/hedef adres veya bağlantı noktası numaraları gibi başlık alanları bilgisine göre gelen ilgili paketlere izin vermekte veya ret etmektedir. Bu cihazlar, pakette kötü amaçlı kod algılama yapamamakta ve her bir paketi ayrı bir bilgi olarak değerlendirilmektedir. Fakat paket filtrelemeli güvenlik duvarları, temel durum denetimine sahiptir. Bu cihazın kullanıldığı altyapılarda istemci sunucudan bilgiyi talep etmekte ve bu talebe karşı sunucudan cevap almaktadır. Söz konusu cihaz, durum koruması amacıyla durum tablolarını bellekte tutmaktadır. Durum denetimli paket filtrelemeli güvenlik duvarlarında ise çoklu port ihtiyacının olduğu ftp uygulamalarında kullanılmaktadır. Bu cihazlar, her protokol için yükü incelemekte, gerekli portu açmakta veya kapatmaktadır. Vekil güvenlik duvarları ise yerel ağı internetten izole etme yeteneğine sahiptir. Bu cihazların en önemli dezavantajı, çok fazla ağ kaynağına ihtiyaç duymasıdır. Tek başına IDS/IPS veya güvenlik duvarları önemli güvenlik önlemi sağlasa da, kural tabanlı çalışan kodlamalar ve öğrenen cihazlar insan tarafından tasarlandığından hata yapma ihtimali mevcuttur. Bu nedenle, günümüzde veri güvenliği için hibrit ve dağıtık sistemler yaygın bir şekilde kullanılmaya başlanmıştır. Bu değişimdeki en önemli itici güç, maliyetlerin düşürülmesi ve yapısal değişiklikler için modüler bir sistem tasarlanması ihtiyacıdır [20, 21].

12.2.6. Şifreleme Teknolojileri

Şifreleme, düz metnin yetkisiz kişiler tarafından anlaşılamayacak şekilde şifreli metin olarak adlandırılan bir forma dönüştürülmesi olarak tanımlanmaktadır. Yetkili bir kişi, yalnızca bir güvenlik

anahtarı kullanarak verilerin (şifreli metin) anlaşılabilir verilere şifrelenmesinden sonra bilgiye erişebilmektedir. Siber güvenlikte kod çözme gücü, anahtar ve şifreleme algoritmasının kalitesine bağlıdır. Şifreleme, temelde simetrik ve asimetrik algoritmalara dayanmaktadır. Simetrik algoritmalar, şifre metni oluşturmak için düz metin ve bir bilinen anahtar kullanmaktadır. Simetrik algoritmalar, çok fazla hesaplama gücüne ihtiyaç duymazlar. Siber güvenlik alanında en çok kullanılan simetrik algoritmalara örnek; DES, 3DES, AES, IDEA, Blowfish ve Twofish olarak verilebilir.

12.2.7. Açık Anahtar Altyapısı

Asimetrik şifreleme algoritmaları olarak bilinen açık anahtar altyapısı genel-özel (public-private) anahtar çiftini kullanmaktadır. Bir anahtar şifreleme, diğer anahtar ise şifre çözme için kullanılmaktadır. Şifreleme anahtarı şifreli mesajlar göndermek isteyen herkese gönderilir iken şifre çözme anahtarı (özel anahtar) gizli olarak saklanmaktadır. Günümüzde şifreleme algoritmalarının gücünü artırmak için asimetrik algoritmalardan faydalanılmaktadır. Bunlardan en önemlileri, kimlik tabanlı şifreleme (identity based encryption), öznitelik tabanlı şifreleme (attribute-based encryption) ve öznitelik tabanlı şifreleme (ABE), şifreleme şeması (cryptographic scheme) gibi algoritmalardır. Kimlik tabanlı şifreleme (IBE), herhangi bir metin parçasının geçerli bir ortak anahtar olarak çalışabileceği genel anahtar şifrelemesidir. Bu yöntem, ilk olarak Shamir tarafından önerilmiştir [22]. Söz konusu yöntem, karşılıklı iki kullanıcının güvenli bir şekilde iletişim kurmasını ve herkese açık veya özel anahtarlar değiştirmeden birbirlerinin imzasını doğrulamasını sağlamaktadır [23]. ABE, bir kullanıcıyı tanımlamak için rasgele bir dize olarak ortak anahtar kullanarak IBE'yi genişletmiştir. Bethencourt ve diğerleri, özel anahtarların öznitelik kümeleriyle etiketlendiği ve şifreli metinlerin VE veya VEYA geçitlerinden oluşan erişim yapılarıyla ilişkili olduğu ilk ABE'yi geliştirmiştir [24]. Şifreleme şeması yönteminde ise güvenilir olmayan sunucuya herhangi bir bilgi sızmadan şifrelenmiş verilerde arama yapılabilmesi sağlanmaktadır [25].

12.2.8. Erişim Kontrol Teknolojileri

Erişim kontrol teknolojilerindeki kullanıcıların doğrulanması, kimlik doğrulamayla başlatılmaktadır. Sıklıkla kimlik doğrulandıktan sonra kullanıcılar bir bilgi sistemine erişmektedir. Erişim kontrol teknolojileri, kullanıcıların ve sistemlerin diğer sistem ve kaynaklar ile nasıl iletişim kurup, etkileştiklerini kontrol etmektedir. Bu teknolojiler, kaynağın kullanılabilirliğini, bütünlüğünü ve gizliliğini kontrol etme, kısıtlama, izleme ve koruma yeteneğine sahiptir.

Bilginin güvenlik altına alınması için çeşitli erişim kontrol modelleri kullanılmaktadır. Bunların en önemlilerinden bazıları; MAC (Zorunlu Erişim Kontrolü), DAC (İsteğe Bağlı Erişim Kontrolü), RBAC (Rol Tabanlı Erişim Kontrolü) dir [26]. MAC ile DAC arasındaki temel fark erişim modelidir. MAC ile erişimde kullanıcı oluşturulan izin düzeyi ve altındaki kaynaklara erişebilmektedir. DAC ile erişimde ise izin düzeyi bulunmamaktadır. DAC'da kullanıcı kimliğine göre erişim sağlanmaktadır. RBAC'da ise roller ve ayrıcalıklar tarafından tanımlanmış erişim mekanizması ile güvenlik sağlanmaktadır.

Diğer bir erişim kontrol teknolojisi ise biyometrik kontroldür. Biyometrik özelliklerden en yaygın olarak; parmak izleri, el geometrisi, retina taraması, iris tarama, ses tanıma, imza dinamiği, klavye dinamiği, yüz taraması gibi özellikler ile erişim kontrolü sağlanmaktadır. Biyometrik erişim teknolojisi, biyolojik ve davranış öznitelikleri ile gerçekleştirilmektedir. Bu teknolojide kart ve benzeri ilave donanıma ihtiyaç olmaması, erişim cihazının taşınmaması ve şifre hatırlanmasına ihtiyaç olmaması en önemli avantajlar arasında yer almaktadır [27]. Fakat, biyometrik özelliklerinin depolandığı sistemlere yetkisiz erişim sağlanıp, ele geçirilmesi durumunda söz konusu biyometrik erişim özniteliklerinin değiştirilememesi en önemli dezavantajdır.

Ülkemizde son yıllarda E-imza ile erişim kontrolü yaygın bir şekilde kullanılmaya başlanmıştır. E-imza, özellikle elektronik ortamda hazırlanan bilginin doğrulanması için kullanılan donanım ve şifre doğrulamanın beraber gerçekleşmesini sağlamaktadır. E-imzanın, ıslak imzanın yerine kullanılması ile çeşitli resmi işlemlerin

internetten ortamında yapılabilmesi ve doğrulanması sağlaması nedeniyle zaman ve maliyet tasarrufu sağlamaktadır [28].

Captcha, Carneige Mellon Üniversitesi tarafından tasarlanan, özellikle webdeki bilgilerin güvenliği için kullanılan, kullanıcının robot olmadığını yazı veya soru cevaplanması ile erişim kontrolü yapan teknolojidir [29].

12.3. Güncel Siber Güvenlik Teknolojileri

Güncel siber güvenlik teknolojileri bölümünde, sosyal siber güvenlik teknolojileri, nesnelerin interneti için siber güvenlik teknolojileri, sağlık için siber güvenlik teknolojileri, büyük veri için siber güvenlik teknolojileri ayrıntılı bir şekilde geçmişten günümüze kullanılan yaklaşımlar ile incelenmiştir.

12.3.1. Sosyal Siber Güvenlik Teknolojileri

Sosyal siber güvenlik, insan davranışındaki siber ortama bağlı (cyber-mediated) değişiklikleri tanımlama, anlama ve tahmin etmeyi sağlayan yeni bir bilim alanıdır. Sosyal siber güvenlik, siber tehditler altında toplumun temel özellik ve karakterini sürdürmesi için gerekli siber altyapıyı inşa etmektedir. Böylece, fikirlerin özgürce ifade edilebildiği özgür ve açık bilgi ortamı sağlanması amaçlanmaktadır. Sosyal siber güvenlik, bilgi hareketinin bilgisayar sistemleri altyapısını riske atmaması gerektiği ve aktörlerin bireyleri, grupları ve toplulukları gereksiz yere etkileyecek veya manipüle edecek şekilde siber ekosisteme zarar vermemesi gerektiği fikrine dayanmaktadır [30, 31].

Sosyal siber güvenlik, doğası gereği çok disiplinli, çok-metodolojik, çok düzeyli bir hesaplamalı bilimdir. Sosyal siber güvenlik yaklaşımı, teknolojinin mesajlaşma (Kim ne zaman mesaj alır, erişir ve görüntüler) ve grup bilgisini (kim kiminle ne zaman iletişim kurar, grup ve aktör tanımlama) etkilemek için nasıl kullanılabileceğini incelemektedir.

Sosyal siber güvenlik alanında saldırılar dört temel basamaktan oluşmaktadır. Bunlar [32, 33];

- bilgi toplama,
- ilişki kurma,
- kişi veya sisteme erişim ve
- uygulamadır.

Söz konusu saldırıları önlemek için siber güvenlik altyapı teknolojileri hızla gelişmeye devam etmektedir. Günümüzde, düşük güçle çalışan akış şifreleme teknikleri ve cihaz kimlik doğrulaması teknikleri kullanılarak, sistemde gizlenen siber tehlikeleri tespit etmek için büyük miktarda kayıt (log) ve iletişim verilerinin analiz edilmesi dahil olmak üzere güvenlik operasyonuna bağlı iş yükünün azaltılmasına odaklanılmıştır. Bu kapsamda, düşük güçle çalışan akış şifreleme teknikleri, kriptografi için ISO/IEC 29192 uluslararası standardına (Düşük kapasiteli cihazlar için şifreleme) uygun hale getirilmeye çalışılmaktadır. Bu yöntemle, AES'in dokuzda biri kadar güç tüketimi ve yirmi kat daha hızlı şifreleme işlemi yapılmaktadır. Şifrelemede standart S-Box'lar (yer değiştirme kutusu) kullanılmaktadır [34].

12.3.2. Nesnelerin İnterneti için Siber Güvenlik Teknolojileri

Nesnelerin interneti (IoT- Internet of Things), ev otomasyonu, endüstriyel süreçler, insan sağlığı gibi farklı alanlara ait sayısal ve fiziksel dünya arasındaki sıkı bağları ifade etmektedir [35, 36]. IoT sistemlerde, saldırı tespit sistemleri (IDS-Instrusion Detection Systems) sıklıkla kullanılmaktadır. IDS, ağların ve bilgi sistemlerinin korunması için önemli bir araç olmuştur. Bu sistemler, izinsiz kullanıcıların bilgi sistemlerine karşı yürüttüğü eylemleri tespit etmektedir. IDS'ler sensörler, analiz motoru ve raporlama sisteminden oluşmaktadır. Sensörler, trafik istatistikleri, paket başlıkları, servis istekleri, işletim sistemi çağrıları ve dosya sistemi değişiklikleri gibi ağ veya ana bilgisayar verilerini toplamaktadır. Analiz motoru, toplanan verileri araştırıp, devam eden izinsiz girişleri tespit etmektedir. Analiz motoru bir saldırı tespit ettiğinde, raporlama sistemi bir uyarı oluşturmaktadır. IDS'ler ağ tabanlı IDS (NIDS) ve Host tabanlı IDS (HIDS) olarak sınıflandırılabilmektedir [37, 38].

Bu alanda Chakrabarty ve arkadaşları, akıllı şehir IoT mimarilerinin güvenliği için yazılım tabanlı ağlar (Software Defined Networks - SDN) kullanılmasını önermişlerdir [39]. Vucinic ve arkadaşları ise akıllı şebekelerde uçtan uca (E2E End-to-End) güvenliği ve IoT'de erişim kontrolü için yeni bir ölçeklenebilir nesne güvenlik mimarisi sunmuşlardır [40]. Valdivieso ve arkadaşları, akıllı ortamda geleneksel ağlardaki mevcut modülerlik sorununu ortadan kaldırmak için SDN mimarisi önermiştir [41]. Gaur ve arkadaşları, akıllı şehirlerde uzak sensör sistemlerinin ve verilerin etkileşimini kolaylaştırmak için akıllı şehir mimarisi sunmuşlardır [42]. Moosavi ve arkadaşları, IoT tabanlı sağlık sistemleri için güvenli ve verimli doğrulama ve yetkilendirme anaçatısı (framework) önermişlerdir [43].

12.3.3. Sağlık için Siber Güvenlik Teknolojileri

Siber güvenlik teknolojilerinin en yoğun kullanıldığı alanlardan biri de sağlıktır. Sağlık alanındaki siber güvenlik düzenlemeleri, tıbbi uygulamaları düzenlemek için belirlenen yasal kurallardır. Bu konu ile ilgili yasalar ve düzenlemeler bulunmaktadır. Bunlardan en önemlikerinden biri sağlık sigortası taşınabilirlik ve sorumluluk yasası (HIPAA) dır. Bu yasa, sağlık bilgi sistemlerinin iyileştirilmesine yönelik çok adımlı bir yaklaşımdır. Söz konusu yasada, hastalara sağlık bilgilerine erişmeleri için yasal ve bireysel hakları sağlamaktadır. Günümüzde insanlar tıbbi verilerini bulutlara yedeklemeye başlamıştır [44, 45].

12.3.4. Büyük Veri için Siber Güvenlik Teknolojileri

Günümüzde büyük veri her çalışma alanında bulunmaktadır. Büyük veri, büyük bir değer ve şans içermektedir. Bununla birlikte, büyük veriler birçok güvenlik riski ve gizlilik koruma sorunlarını da beraberinde getirmektedir. Güvenlik ve gizlilik sorunları, büyük verinin temel karakteristiklerinden olan ve 5V'ler içinde yer alan hız, hacim ve çeşitlilikte önemli sorunlar meydana getirmektedir. Bu nedenle, geleneksel güvenlik mekanizmaları büyük veri güvenliği için uygun değildir.

Gizlilik koruma teknikleri bakımından büyük veride üç temel sınflandırma bulunmaktadır. Bunlar veri karmaşıklaştırma,

veri şifreleme ve veri anonimleştirme teknikleridir. Veri karmaşıklaştırma tekniğinde, orijinal veri kümesinin hassas bilgileri rastgele değişkenler, offset ekleme, bulanık veri kümeleri oluşturma ve benzeri anonim karmaşıklaştırma yoluyla değiştirilmektedir. Veri şifrelemede, veri madenciliği yöntemleri kullanılarak hassas verinin gizlenmesi sağlanmaktadır. Veri anonimleştirmede ise imza, gizli paylaşım teknolojisi, k veya t anonimliği kullanılarak verilerin gizlilik koruması sağlanmaktadır [46, 47].

Literatürdeki büyük veri güvenliği çalışmaları özellikle altyapı güvenliği, veri gizliliği veya veri yönetimi üzerine odaklanılmıştır [48]. Altyapı güvenliği kapsamına Hadoop güvenliği, iletişim güvenliği, mimari güvenliği, kimlik doğrulama, kullanılabilirlik (availability) girmektedir. Veri gizliliği kapsamına; kriptografi, erişim kontrolü, gizlilik, gizlilik-koruma sorguları, anonimleştirme, sosyal ağlarda gizlilik, diferansiyel gizlilik girmektedir. Veri yönetimi kapsamına ise; depolama güvenliği, politikalar, yasalar veya hükümet, paylaşım algoritmaları girmektedir. Literatürdeki çalışmaların söz konusu alanlardan özellikle veri gizliliği veya mahremiyeti üzerine odaklandığı görülmüştür [49].

Günümüzde, büyük veri güvenliği alanındaki temel çalışma alanları aşağıda sunulmuştur. Bunlar [50];

- Kriptografi ve büyük veri
- Büyük verilerde saldırı tespiti ve büyük veri iletim yönetimi
- Büyük veri için depolama ve sistem güvenliği
- Büyük veri adli bilimi
- Büyük veri doğrulama ve bütünlük koruma
- Büyük verilerin erişim kontrolü
- Büyük verilerde gizlilik analiz ve büyük veriyi geri alma ile
- Büyük veri ile veri füzyonudur.

Literatürde büyük verinin gizlilik ve güvenliği beş farklı şekilde sınıflandırılmaktadır. Bunlar; Hadoop güvenliği, bulut güvenliği, izleme ve denetleme, anahtar yönetimi ve anonimleştirmedir. Hadoop, temelde güvenlik için geliştirilmemiş, büyük veri ile

ortaya çıkan dağıtık veri işleme anaçatısıdır. Hadoop üzerindeki güvenlik iki yöntem ile sağlanmaktadır. İlk yöntemde, kullacının ve düğümün oluşturduğu hash fonksiyon değerleri karşılaştırılıp, kimlik doğrulama için SHA-256 hash tekniği kullanılarak sisteme erişim sağlanmaktadır. İkinci yöntemde ise MapReduce ile beraber RSA, AES ve RC6 rasgele şifreleme teknikleri kullanılmaktadır. Hadoop Dağıtılmış Dosya Sistemi (HDFS - Hadoop Distributed File System) güvenliği için ise üç temel yöntem kullanılmaktadır. İlk yöntemde, bilet verme veya servis biletine dayalı Kerberos mekanizması ile kimlik doğrulama gerçekleştirilmektedir. İkinci yöntemde ise Bull Eye algoritması ile hassas veriler sürekli görüntülenmektedir. Bu algoritma, orijinal veriler ile çoğaltılan veriler arasındaki ilişkileri yönetmek için kullanılmaktadır. Son yöntemde ise düğümlerdeki gecikme ve veri kullanılabilirliği sorunları için ana - yedek mekanizması kullanılmaktadır.

Büyük veride izinsiz giriş algılama mimarisi ile izleme, Merkle Hash Ağaçları ile denetleme gerçekleştirilmektedir. Anahtar yönetimi için ise Kuantum kriptografisi, çevrimiçi anahtar oluşturma ve benzeri teknikler kullanılmaktadır. Büyük verideki anonimleştirme için ise K-anonimlik tabanlı metrikler, uyarlamalı anonimleştirme modeli ve iki fazlı kümeleme algoritması kullanılmaktadır [51-54].

12.4. Değerlendirmeler

Yenilikçi tekniklerin ortaya çıkışı ile beraber mobil cihazlar, bulut bilişim, veri analizi, nesnelerin interneti ve benzeri bilgi iletişim teknolojilerin etkin bir şekilde sunulması sağlanmıştır. Fakat bu teknolojiler ve bağlı cihazların çeşitli özellikteki verileri, daha yüksek güvenlik ve gizlilik risklerine maruz kalmaktadır. Bu nedenle, siber güvenlik teknolojilerine önemli bir ihtiyaç olduğu görülmektedir. Siber güvenlik teknolojileri alanında geleneksel güvenlik mekanizmaları, gizlilik ve güvenlik için yeterli ve uygun değildir. Bu kapsamda gelecekteki siber güvenlik araştırma yönlerinin birbiri ile entegre çalışan, veri akışların tüm standartlarının belirlendiği, takip edilebilir, red edilemez teknolojiler alanına odaklanacağı düşünülmektedir. Bu kapsamda blok zincir teknolojisinin öne çıkacağı var sayılmaktadır. Bilgi teknolojilerin, merkezi olmayan ve dağıtık yapıda olmaya devam edeceği düşünüldüğünde, blok

zincir teknolojisinin veri anonimleştirme ve geriye dönük kayıt değiştirememeyi destekleyerek, inkâr edilemezliği sağlaması önemlidir. Bu nedenle siber güvenlik teknolojileri alanında, önümüzdeki yıllarda çeşitli özgün blok zincir uygulamalarının sıklıkla görüleceği düşünülmektedir.

Ayrıca, büyük miktarda kayıt ve iletişim verilerinin analiz edilmesi için düşük güçle ve yüksek hızla çalışan hibrit siber güvenlik teknolojilerinin geliştirileceği, yazılım alanında ise ticari işletim sistemlerinin yanında açık kaynak işletim sistemlerini de destekleyen, asenkron yazılım çözümlerinin daha popüler olacağı öngörülmektedir.

Kaynaklar

[1] Security Intelligence, (2018). https://securityintelligence.com/news/global-cost-of-cybercrime-exceeded-600-billion-in-2017-report-estimates, Erişim: 01.01.2019.

[2] Security Report, (2018). https://cybersecurityventures.com 2017-Cybercrime-Report, Erişim: 01.01.2019.

[3] Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. Journal of Computer and System Sciences, 80(5), 973-993.

[4] Patil, B. V., Jadhav, R. J. (2018). Computer Virus and Anti-virus Software–A Brief Review. IJAME, 4(2), 1-4.

[5] Nachenberg, C. (1997). Computer virus-anti-virus coevolution. Communications of the ACM, 40(1), 46-51.

[6] Stallings, W., Brown, L., Bauer, M. D., Bhattacharjee, A. K. (2012). Computer security: principles and practice. Upper Saddle River, NJ, USA, Pearson Education.

[7] Sukwong, O., Kim, H. S., Hoe, J. C. (2011). Commercial Anti-virus Software Effectiveness: An Empirical Study. IEEE Computer, 44(3), 63-70.

[8] Stone-Gross, B., Abman, R., Kemmerer, R. A., Kruegel, C., Steigerwald, D. G., & Vigna, G. (2013). The underground economy of fake anti-virus software. In Economics of information security and privacy III (55-78). Springer, New York, NY.

[9] Teddy, J., Bean, J. D., Dalcher, G. W., Hetzler, J. (2017). U.S. Patent No. 9,614,865. Washington, DC: U.S. Patent and Trademark Office.

[10] Blanzieri, E., Bryl, A. (2008). A survey of learning-based techniques of email spam filtering. Artificial Intelligence Review, 29(1), 63-92.

[11] SPF, http://openspf.org/faq.html Erişim: 01.01.2019.

[12] Designated mailers protocol, http://www.pan-am.ca/dmp/draft-fecyk-dmp-01.txt, Erişim: 01.01.2019.

[13] Schiavone V, Brussin D, Koenig J, Cobb S, Everett-Church R (2003) Trusted e-mail open standard: a comprehencive policy and technology proposal for email reform. http://www.cobb.com/spam/teos/, Erişim: 01.01.2019.

[14] Metsis, V., Androutsopoulos, I., Paliouras, G. (2006). Spam filtering with naive bayes-which naive bayes?, CEAS, 17, 28-69.

[15] Caruana, G., Li, M. (2012). A survey of emerging approaches to spam filtering. ACM Computing Surveys (CSUR), 44(2), 9.

[16] Fuchsberger, A. (2005). Intrusion detection systems and intrusion prevention systems. Information Security Technical Report, 10(3), 134-139.

[17] Garcia-Teodoro, P., Diaz-Verdejo, J., Maciá-Fernández, G., Vázquez, E. (2009). Anomaly-based network intrusion detection: Techniques, systems and challenges. computers & security, 28(1-2), 18-28.

[18] Ashoor, A. S., & Gore, S. (2011). Difference between intrusion detection system (IDS) and intrusion prevention system (IPS). In International Conference on Network Security and Applications, 497-501. Springer, Berlin, Heidelberg.

[19] Patel, A., Qassim, Q., & Wills, C. (2010). A survey of intrusion detection and prevention systems. Information Management & Computer Security, 18(4), 277-290.

[20] Beg, S., Naru, U., Ashraf, M., Mohsin, S. (2010). Feasibility of intrusion detection system with high performance computing: A survey. Int. J. Advances in Computer Science, 1, 26-35.

[21] Diaz-Verdejo, J. E., Garcia-Teodoro, P., Muñoz, P., Maciá-Fernández, G., De Toro, F. (2007). A Snort-based approach for the development and deployment of hybrid IDS. IEEE Latin America Transactions, 5(6), 386-392.

[22] Shamir, A. (1984). Identity-based cryptosystems and signature schemes. In Workshop on the theory and application of cryptographic techniques (pp. 47-53). Springer, Berlin, Heidelberg.

[23] Boneh, D., Franklin, M. (2001). Identity-based encryption from the Weil pairing. In Annual international cryptology conference, 213-229, Springer, Berlin, Heidelberg.

[24] Bethencourt, J., Sahai, A., Waters, B. (2007). Ciphertext-policy attribute-based encryption. In Security and Privacy, 2007. SP'07. IEEE Symposium, 321-334. IEEE.

[25] Boneh, D., Di Crescenzo, G., Ostrovsky, R., & Persiano, G. (2004). Public key encryption with keyword search. In International conference on the theory and applications of cryptographic techniques, 506-522, Springer, Berlin, Heidelberg.

[26] Asija, R., Nallusamy, R. (2014). A Survey on Security and Privacy of Healthcare Data, 3rd Annual global Healthcare Conference, 1-11, Singapore.

[27] Ozkaya, N., Sagiroglu, S. (2008). Translating the fingerprints to the faces: A new approach. In 2008 IEEE 16th Signal Processing, Communication and Applications Conference,1-4.

[28] Sağıroğlu, Ş., & Alkan, M. (2005). Her Yönüyle Elektronik İmza (E-İmza). Grafiker, Ankara, 3(5), 33.

[29] Von Ahn, L., Blum, M., Hopper, N. J., & Langford, J. (2003). CAPTCHA: Using hard AI problems for security. In International Conference on the Theory and Applications of Cryptographic Techniques, 294-311. Springer, Berlin, Heidelberg.

[30] Carley, K. M., Cervone, G., Agarwal, N., Liu, H. (2018). Social cyber-security. In International Conference on Social Computing, Behavioral-Cultural Modeling and Prediction and Behavior Representation in Modeling and Simulation, 389-394, Springer, Cham.

[31] Hatfield, J. M. (2018). Social engineering in cybersecurity: The evolution of a concept. Computers & Security, 73, 102-113.

[32] Conteh, N. Y., Schmick, P. J. (2016). Cybersecurity: risks, vulnerabilities and countermeasures to prevent social engineering attacks. International Journal of Advanced Computer Research, 6(23), 31.

[33] Mouton, F., Leenen, L., Venter, H. S. (2016). Social engineering attack examples, templates and scenarios. Computers & Security, 59, 186-209

[34] Kaji, T., Yamada, I. T., Nakano, T., & Serita, E. S. (2013). Cyber Security Technologies for Social Infrastructure Systems. Hitachi Review, 62(7), 397.

[35] Atzori, L., Iera, A., Morabito, G. (2010). The internet of things: A survey. Computer networks, 54(15), 2787-2805.

[36] Zarpelão, B. B., Miani, R. S., Kawakani, C. T., & de Alvarenga, S. C. (2017). A survey of intrusion detection in Internet of Things. Journal of Network and Computer Applications, 84, 25-37.

[37] Miorandi, D., Sicari, S., De Pellegrini, F., Chlamtac, I. (2012). Internet of things: Vision, applications and research challenges. Ad hoc networks, 10(7), 1497-1516.

[38] Lin, Y., Zhang, Y., Ou, Y. J. (2010). The design and implementation of host-based intrusion detection system. In 2010 Third International Symposium on Intelligent Information Technology and Security Informatics (595-598). IEEE.

[39] Chakrabarty, S., & Engels, D. W. (2016). A secure IoT architecture for Smart Cities. In 13th IEEE Annual Consumer Communications & Networking Conference (CCNC), ,812-813, 2016.

[40] Vučinić, M., Tourancheau, B., Rousseau, F., Duda, A., Damon, L., & Guizzetti, R. (2015). OSCAR: Object security architecture for the Internet of Things. Ad Hoc Networks, 32, 3-16.

[41] Valdivieso Caraguay, A. L., Benito Peral, A., Barona Lopez, L. I., & Garcia Villalba, L. J. (2014). SDN: Evolution and opportunities in the development IoT applications. International Journal of Distributed Sensor Networks, 10 (5), 735142.

[42] Gaur, A., Scotney, B., Parr, G., McClean, S. (2015). Smart city architecture and its applications based on IoT. Procedia computer science, 52, 1089-1094.

[43] Moosavi, S. R., Gia, T. N., Rahmani, A. M., Nigussie, E., Virtanen, S., Isoaho, J., Tenhunen, H. (2015). SEA: a secure and efficient authentication and authorization architecture for IoT-based healthcare using smart gateways. Procedia Computer Science, 52, 452-459.

[44] Liu, Y., Zhang, Y., Ling, J., Liu, Z. (2018). Secure and fine-grained access control on e-healthcare records in mobile cloud computing. Future Generation Computer Systems, 78, 1020-1026.

[45] Liu, X., Xia, Y., Yang, W., Yang, F. (2018). Secure and efficient querying over personal health records in cloud computing. Neuro computing, 274, 99-105.

[46] Fang, W., Wen, X. Z., Zheng, Y., Zhou, M. (2017). A survey of big data security and privacy preserving. IETE Technical Review, 34(5), 544-560.

[47] Castro, S., & Pushpalakshmi, R. (2017). A Survey on Big Data Security and Related Techniques to Improve Security. Asian Journal of Applied Science and Technology (AJAST), 1(5), 113-116.

[48] Ahmad, S., Azam, M.A., Blessy, J. A., (2018). A Survey on Security and Privacy of Big Data, International Journal of Engineering Research in Computer Science and Engineering, 5 (4), 96-100.

[49] Moreno, J., Serrano, M. A., Fernández-Medina, E. (2016). Main issues in big data security. Future Internet, 8(3), 44.

[50] Cloud Security Alliance, Top ten big data security and privacy challenges, https:// cloudsecurityalliance.org, Erişim: 01.01.2019.

[51] Terzi, D. S., Terzi, R., Sagiroglu, S. (2015). A survey on security and privacy issues in big data. In Internet Technology and Secured Transactions (ICITST), 2015 10th International Conference (202-207). IEEE.

[52] Sahafizadeh, E., Nematbakhsh, M. A. (2015). A survey on security issues in Big Data and NoSQL. Advances in Computer Science: an International Journal, 4(4), 68-72.

[53] Saraladevi, B., Pazhaniraja, N., Paul, P. V., Basha, M. S., Dhavachelvan, P. (2015). Big Data and Hadoop-A study in security perspective. Procedia computer science, 50, 596-601.

[54] Chandra, S., Ray, S., Goswami, R. T. (2017). Big Data Security: Survey on Frameworks and Algorithms. In Advance Computing Conference (IACC), 2017 IEEE 7th International (48-54).

Biyometrik Sistemlerde Güvenlik ve Mahremiyet

BÖLÜM 13

Bilgehan ARSLAN
Prof. Dr. Şeref SAĞIROĞLU

BİYOMETRİK SİSTEMLERDE GÜVENLİK VE MAHREMİYET

Güvenli yaşama isteği, içinde bulunduğumuz dijital dünyada artık temel ihtiyaç olarak görülmektedir ve günden güne bu istek artmaktadır. Kimlik ve erişim güvenliği başta olmak üzere, güvenli yaşam sürebilmek için güvenli mekânlar ve şehirlerde yaşayabilme, güvenli sağlık hizmeti alabilme, güvenli alışveriş yapabilme, güvenli seyahat edebilme ve bilginin güvenliğini sağlama her bireyin arzusudur. Riskler ve tehditler karmaşıklaştıkça, güvenliğin sağlanabilmesi ve ihlal edenlerin belirlenmesi için, geliştirilen savunma yöntemlerinde biyometrik güvenlik teknolojileri devreye girmektedir. Kamu hizmetinden sınır kontrolüne, bankacılıktan şehir güvenliğine kadar sayısız alanda kullanılan biyometrik sistemler; kişisel ve kurumsal açıdan değerlendirildiğinde hayatı kolaylaştırsalar da güvenlik ve gizlilik açısından zafiyet oluşturabilecek niteliklere de sahiptir.

Yapay zekâ temelli teknolojilerin sunduğu avantajlar kullanılarak geliştirilen araç, teknik ve yöntemlerin hem savunma hem de saldırı amacıyla kullanılması ile birlikte, siber dünyada iyi ile kötünün arasındaki savaş yeni bir boyut kazanmaktadır. Doğal olarak biyometrik temelli güvenlik mekanizmaları da bundan etkilenmektedir. Özellikle biyometrik tabanlı kimlik doğrulama sistemlerinde oluşacak tehditler, siber güvenlik kapsamında üzerinde durulması ve dikkat edilmesi gereken konulardan birisi olarak görülmektedir. Bu bölümde; mevcut saldırıları anlamaya ve gelecek saldırılara karşı savunma yöntemleri geliştirebilmeye yardımcı olmak için:

- biyometrik sistem bileşenleri ve bu bileşenlerin çalışma mekanizmaları,

- biyometrik sistemleri tehdit eden unsurları ve olası saldırı senaryoları,
- biyometrik sistemlere yapılan saldırılar için geliştirilen savunma yöntemlerinin incelenmesi,
- biyometrik sistemin geliştirilmesi için uygulanması gereken prosedürler, kullanılması gereken standartlar ve
- biyometrik sistemlerin siber saldırılara karşı direncini arttıracak yeni yaklaşımlar

üzerinde durulmuş, bu hususlar dikkate alınarak açıklamalar yapılmış ve son bölümde ise genel değerlendirmelere yer verilmiştir.

13.1. Giriş

Genel olarak güvenlik; tehlikeye veya kayba karşı korunma sağlama, varlığı emniyet altına alma işlemlerini kapsamaktadır. Güvenliği sağlayabilmek adına uygulanacak her prosedür hangi ortamın güvenli kılınacağına göre değişiklik göstermektedir. Söz konusu biyometrik sistemlerin güvenliği olduğunda; biyometrik veri güvenliğinin, biyometrik yöntemlerle korunan verilerin güvenliğinin, biyometrik uygulamaların ve kullanılan ağın güvenliğinin sağlanabilmesi için uygulanan prosedürler düşünülmelidir. Biyometrik sistemlerin günümüzde temel kullanım alanlarından biri kimlik yönetimidir. Biyometrik sistemler, özellikle erişim kontrolü ve yetkilendirme, kimlik doğrulama, şifre yönetimi ve rol dağılımları gibi kimlik yönetim sistemlerinin sorumlu olduğu alanlarda yaygın bir biçimde kullanılmaktadır. Biyometri temelli uygulamalar, bilinen (PIN, şifre vb.) veya sahip olunan (anahtar, kart, kimlik, vb.) bilgiyi temel alarak korumaya, güvenlik sağlamaya veya arttırmaya yönelik uygulamaların eksikliklerini gidermek adına geliştirilen alternatif yaklaşımlardır [1,2]. Kimlik yönetiminin gerçekleştirilmesi hedeflenen uygulama ortamlarında sadece bilgi tabanlı ölçümlerle korunma yapıldığı takdirde, kullanıcı tarafından belirlenen şifreye göre güvenlik seviyesi belirlenmiş olunur. Kullanıcının basit olarak seçeceği şifrenin tahmin edilebilmesi, karmaşıklığı arttırabilmek adına kullanılan rakam/harf/ASCII karakterlerin kombinasyonlarından dolayı şifrenin unutulabilmesi, şifrenin yetkisiz kişilerle paylaşılması gibi senaryoların gerçekleşme ihtimali, tasarlanan

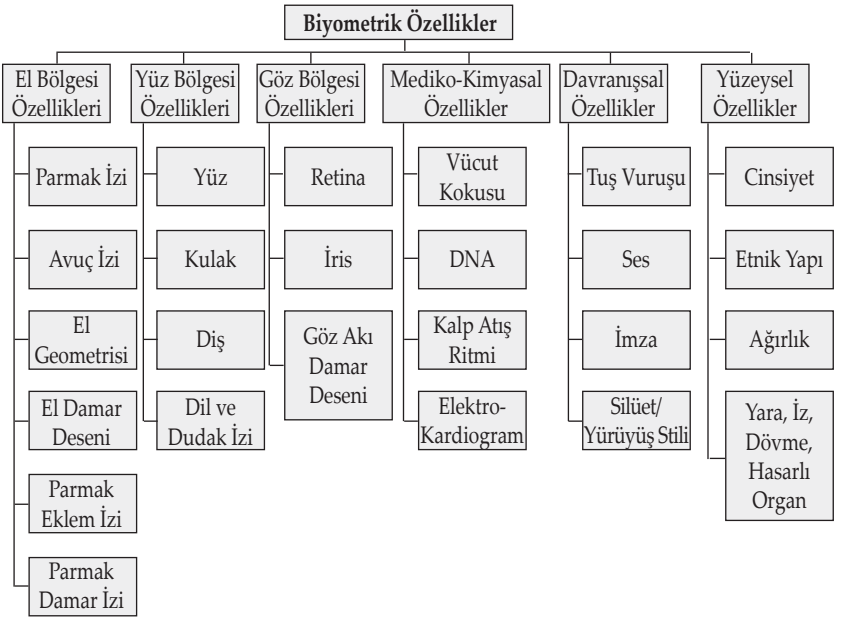
güvenlik sisteminin sağladığı hizmete bakılmaksızın kullanılan uygulamaların zafiyete uğradığı ve sistemlerin devre dışı kaldığı anlamına gelir. Bu sebeple özellikle temel hedef "Güvenilirlik Seviyesi Yüksek Platformlar" olduğunda, biyometrik sistemler cazip çözümler sunabilmektedir. Fakat bu üstünlüklere rağmen, bu sistemlerde kullanılan biyometrik karakteristik verinin olası bir güvenlik zafiyetinden kaynaklı çalınması halinde klasik bir şifre gibi yenilenemeyeceği ve değiştirilemeyeceği gerçeği, olayın ciddiyetini bizlere göstermektedir. Bu gerekçelerden dolayı, biyometrik verilerin güvenliği ve veri mahremiyeti ihlalleri her zaman üzerinde önemle durulan konulardan olacaktır.

13.2. Biyometrik Tanıma ve Bireysel Çeşitliliğin Temelleri

Biyometri kelimesi farklı kaynaklarda; "bio" ve "metron" yani "yaşam" ve "ölçüm" kelimelerinin bir araya gelmesiyle ortaya çıkan bir kelime, biyolojik bilgiyi değerlendirme ve analiz etme işlemine dayalı bir bilim, istatistik yöntemlerinin tıp ve biyoloji alanlarına uygulanması, insan bünyesindeki fiziksel (parmak izi, iris, vb.) veya davranışsal (yürüme şekli, vb.) özellikler kullanarak tanımlama yapabilme veya insanın ayırt edici özelliklerin tespit edilerek bu özelliklerin tanıma için kullanılması işlemi olarak tanımlanmaktadır [3,4]. Daha kapsamlı bir ifadeyle biyometri "bir kontrol mekanizması tarafından otomatik olarak tespit edilebilen, kişiyi tanımlamak amacıyla seçilmiş fiziksel veya kişisel bir özelliği tanıma ayracı olarak kullanıp bireyler arası farktan yararlanarak tespit yapabilen mekanizma" olarak tanımlanmaktadır [3,4].

Biyometri temelli tanıma, hepimizin yıllardır yaptığı bir işlem olup; birbirimizi isimlerimizden, yürüyüşümüzden, seslerimizden veya yüzlerimizden tanımlayabilme durumudur. Daha evvel yaşanan karşılaşma eylemi sonrası kişiye ait hafızada yer edinmiş karakteristik ve fiziksel bilgileri kullanarak aynı kişiyi tekrar tanıyabilmek, insan hafızasının bir veri tabanı olarak kullanıldığı bir biyometrik tanıma sürecidir. Buna örnek olarak; bir bireyin doğumundan ölümüne kadar, duyu organları sayesinde sürekli olarak elde ettiği bilgilere ve hafızasında tuttuğu verilere dayanarak, kişileri hayatı boyunca kendiliğinden tanıması gösterilebilir. Hatta kişi daha yakından tanıdığı bireyleri ses veya koku gibi daha spesifik özellikler

sayesinde de tanıyabilmektedir. Gelişmiş hallerine aşina olduğumuz biyometrik sistemlerin ampirik modelleri yüzlerce yıl öncesinden beri kullanılmaktadır. Şekil 13.1'de gösterildiği gibi kişiyi betimleyen biyometrik ve biyolojik içerikli karakteristik özelliklere ek olarak, günümüzde beğeni, tıklama, paylaşma ve indirme gibi davranışsal özelliklerin de yer aldığı binlerce özellik ayırt edici unsur olarak kullanılmaktadır.



Şekil 13.1. Biyometrik özelliklerin detaylı olarak sınıflandırılması [6]

En çok kabul gören yaklaşımlar dikkate alındığında, biyometri fizyolojik veya davranışsal özellikleri kullanarak bireyin kimliğini belirleme veya doğrulama bilimi olarak ifade edilmektedir [5]. Biyometri, ayırt edici özelliklerine dayanarak bireyi tanımlamanın bir yöntemi olarak düşünülmektedir. Bu ayırt edici özellikler; imza, ses ve tuş vuruşu gibi bireyin zaman içerisinde öğrendiği ve bir eylem sonucunda ölçülebilen davranışsal biyometrik özellikler ile yüz, parmak izi, el geometrisi ve iris gibi bireyde doğuştan var olan, her daim ölçülebilen fizyolojik biyometrik özelliklerdir.

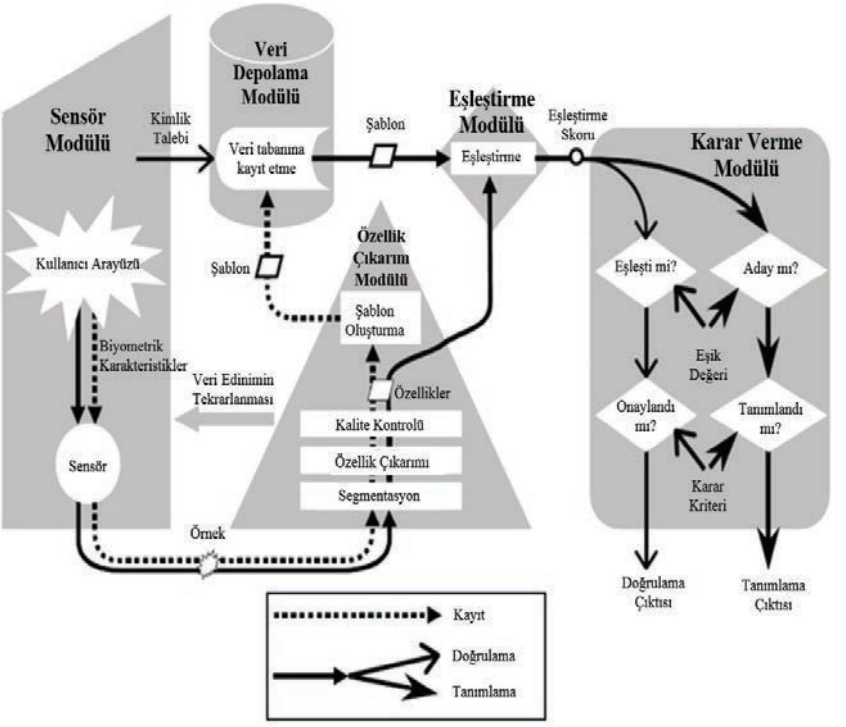
Şekil 13.1'de bireyi diğerlerinden eşsiz kılan biyometrik karakteristik özelliklerin sınıflandırılması yapılmıştır. Bahsedilen bu özelliklerin bir veya birkaçı bireyi tanımlayabilmek için yeterli olmaktadır [7].

Biyometrik sistem, ilk önce kayıt sırasında uygun bir sensör kullanarak kullanıcının biyometrik özelliğinin bir örneğini kaydetmektedir. Daha sonra, karakteristik özellik çıkarıcı olarak adlandırılan ayrıştırıcı algoritmalar kullanılarak, biyometrik numuneden göze çarpan özellik vektörleri çıkartılmaktadır. Sistem çıkarılan bu özellikleri, bir isim veya kimlik numarası gibi diğer tanımlayıcılarla birlikte veri tabanında bir şablon veya iz olarak saklamaktadır. Kimlik doğrulaması için, kullanıcının sensöre başka bir biyometrik örnek sunması gerekmektedir. Bu örnekten çıkarılan özellikler, sistemde yer alan kimliğin şablonu ile bir biyometrik eşleştirici aracılığıyla karşılaştırılmaktadır. Eşleştirici, şablon ile sorgu arasındaki benzerlik derecesini temsil eden bir eşleşme skoru döndürmektedir. Eşleşme skoru sistem için önceden tanımlanmış eşik değerinin üstünde ise, doğrulanması istenen kimliğe aitlik iddiası kanıtlanmış olunur.

Şekil 13.2'de bir biyometrik sisteme ait olan beş temel bileşen ve bu bileşenlere ait detaylar verilmiştir [8-10]. Bu bileşenler; sensör modülü, özellik çıkarımı modülü, veri depolama modülü, eşleştirme modülü ve karar modülü olarak adlandırılmıştır.

Sensör modülünde, biyometrik ayırt edici karakteristikler istenilen veriyi toplayabilen uygun bir sensör (parmak izi okuyucu, kamera, tarayıcı vb.) tarafından yakalanır ve dijital forma dönüştürülebilmesi için biyometrik özelliğin bulunduğu alan taranır. Sensör modülü dijitalleştirdiği veriyi özellik çıkarma modülüne iletir. Özellik çıkarım modülü sensör tarafından toplanan ham verileri işleyerek biyometrik bir şablon oluşturur. Sensör modülünden gelen veri çok önemlidir, eğer gerektiği kadar karakteristik veriyi bünyesinde barındırmıyorsa veya gelen veride yüksek oranda gürültü varsa özellik çıkarım modülü istenilen başarıyı elde edemez. Veri depolama modülünde özellik çıkarım modülünden gelen veriler, veri tabanına kaydedilir. Eşleştirme modülü ise doğrulama için alınan örnek ile veri tabanındaki kayıtlı şablonlarla eşleştiren algoritmaları kullanarak karşılaştırma işlemi yapar ve bir eşleşme skoru üretir. Elde edilen eşleşme skoru, bireyi kabul edip etmemeye karar veren modüle iletilir. Karar modülü ise önceden tanımlanmış eşleşme skoru ile eşleştirme modülünden gelen skoru karşılaştırır. Eğer skor,

güvenlik eşiğinden büyükse eşleştirme modülü bireyi kabul eder, aksi takdirde reddeder [9]. Sonuç olarak, bu beş bileşen herhangi bir biyometrik sistemde, ham biyometrik verileri toplamak, işlemek ve anlamlı sonuçlar elde etmek için kullanılmaktadır.



Şekil 13.2. Biyometrik Sistemlerin Temel Bileşenleri [10]

13.3. Biyometrik Sistemler ve Güvenilirlik

Güvenliği sağlayabilmek adına uygulanacak her prosedür hangi ortamın güvenli kılınacağına göre değişiklik göstermektedir. Söz konusu biyometrik sistemlerin güvenliği ise;

- biyometrik verinin güvenliği,
- biyometrik yöntemlerle korunan verinin güvenliği,
- biyometrik uygulama bileşenlerinin güvenliği ve
- kullanılan ağın güvenliğinin sağlanabilmesi için uygulanan prosedürler

dikkate alınmalıdır [11]. Tanımlama (identification), doğrulama (verification), kanıtlama (authentication) ve yetkilendirme (authorization) süreçlerini yönetmek için büyük bir rol üstlenen biyometrik sistemlerin güvenilir kılınmasını sağlayan kriterler göz önünde bulundurularak; verilerin toplanma, depolanma ve değerlendirme süreçlerinde kullanılan sistemlerin ve altyapıların zayıf yönleri ve olası tehditler tespit edilerek gerekli korumayı yapabilecek kapsamlı çözümlerin geliştirilmesi hedeflenmelidir. Diğer bir ifadeyle, biyometrik tabanlı doğrulama mekanizmalarında kullanılan tüm bileşenlerin belirlenmesi, tasarlanması, geliştirilmesi ve kullanılması sırasında güvenlik zafiyeti yaratacak bütün ihtimallerin devre dışı bırakılması gerekmektedir [11,12].

Bir biyometrik sistemi güvenli olarak tanımlayabilmek için aşağıda verilen yedi temel kriterin sağlanması gerekmektedir. Bu kriterler aşağıda sırasıyla açıklanmıştır [13,14,15,16]:

(1) Teklik veya tekillik: Karakteristik veri kişiye özgü olmalı ve ayırt edici özellik taşımalıdır.

(2) Kalıcılık: Bireyin biyometrik özelliği zamanla değişiklik göstermemelidir, çünkü eşleştirmede kullanılan algoritma kalıcı özellikleri kullanarak sonuç üretir.

(3) Evrensellik: Biyometrik özellik bireyler için yeterli derecede farklı olmalı ve zamanla değişmemelidir, böylece her bir kişi ayrı ayrı tanımlanabilir.

(4) Toplanabilirlik: Biyometrik özelliği elde etmek, sayısallaştırmak ve verilerin temsili özellik setlerini çıkarmak için verilerin toplanabilir veya elde edilebilir olması gerekir.

(5) Performans: Biyometrik sistemlerde kullanılan verilerin çıkarılması, toplanması ve saklanması sürecinde kullanılan tüm yazılım ve donanım mekanizmaları uygun performans kriterlerine sahip olmalıdır.

(6) Kabul edilebilirlik: Uygulamanın kullanılacağı hedef popülasyondaki bireyler, toplanacak biyometrik özelliklerini sisteme sunmaya istekli olmalıdır.

(7) Tehdidi önleme veya tehdide dayanıklılık: Davranışsal özellikler söz konusu olduğunda, bir bireyin özelliklerinin yapay nesneler

(örneğin, sahte parmaklar) kullanılarak taklit edilebilir olmaması veya tehdide dayanıklı olması gerekmektedir.

Bahsedilen kriterleri sağlayamayan bir biyometrik sistemin güvenliğinin risk altında olacağı aşikârdır. Biyometrik sistemlerin kullanım amaçları ve alanları göz önüne alındığında en ufak bir açıklığın kaotik sonuçlar doğurabileceği açıktır. Bu sebeple;

- biyometrik sistemi oluşturan tüm donanım temelli bileşenler ve sistemin sonuç üretebilmesi için kullanılan tüm yazılım tabanlı bileşenler verilen kriterleri sağlamalı,
- biyometrik sistemlerin zafiyetleri belirlenmeli ve giderilmeli,
- risklerin ortadan kaldırılması için tüm yaklaşımlar, prosedürler, çözümler gözden geçirilmeli veya bu bakış açısıyla yeniden geliştirilmeli ve
- mevcut standartlardan faydalanılmalı, gerekirse yeni standartlar geliştirilmeli ve sonuçta güvenli bir biyometrik sistem tasarımı yapılmalıdır.

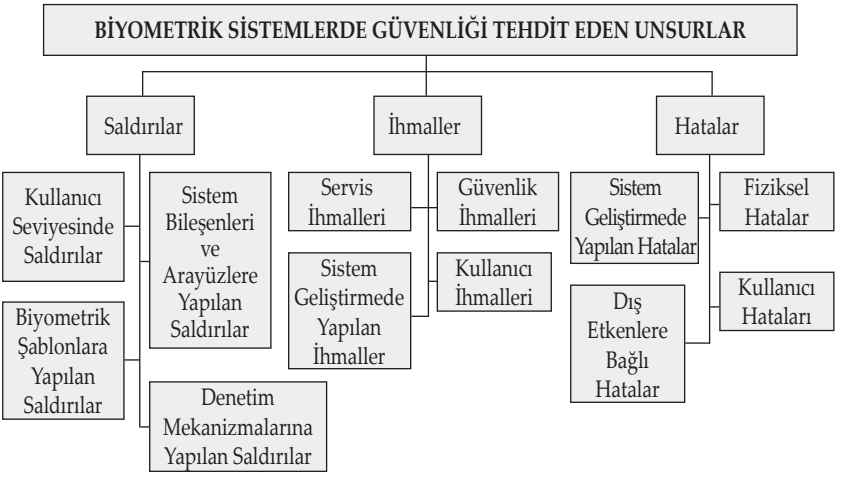
13.4. Biyometrik Sistem Güvenliğini Tehdit Eden Unsurlar

Biyometrik sistemler, geleneksel kimlik doğrulama sistemleriyle ilişkili sorunların çoğuna çözüm üretmekle birlikte, bu sistemlerin tasarımında güvenlik kriterlerinin göz ardı edilmesi durumunda, sistemin sunduğu üstünlükler kolaylıkla eksikliklere dönüşebilir. Burada bahsi geçen sistem güvenliğini tanımlamak için güvenlik açığı, saldırgan, tehdit gibi kavramlar doğru bir şekilde tanımlanması, saldırıları önlemek için kullanılan kontrol mekanizmaları ile önleyici tedbirlerin belirlenmesi gerekmektedir [17].

Biyometrik güvenlik sistemleri;

- sınır ve göç kontrolü, e-pasaport, seçim, e-sağlık, ehliyet, sosyal güvenlik gibi devlet bünyesinde kullanılan uygulamalar,
- elektronik veri güvenliği, e-ticaret, erişim kontrolü, kimlik yönetimi, kişisel güvenlik gibi ticari uygulamalar,
- ceza soruşturmaları, ceset tanımlama, terörist tespiti ve ebeveynlik tespiti gibi alanlar ile
- kriminal vakalarda suçlu tespiti ve delillendirmede

doğrulama/tanıma/kanıtlama hizmeti vermek üzere yaygın olarak kullanılmaktadır [19]. Biyometrik sistemlerin kullanıldığı ortam, sunduğu hizmet ve etkileşime geçtiği kullanıcı, saldırgan vb. tüm unsurlar, biyometrik sistemin hangi çalışma senaryosuna göre tasarlanması gerektiğini belirler. Farklı senaryolara bağlı olarak, biyometrik sistemlerde iç ve dış tehditler ile birlikte çeşitli güvenlik açıkları ortaya çıkmaktadır. Biyometrik sistemlerin açıkları, bunların niteliği ve kimlik doğrulama/tanıma/kanıtlama işleminin güvenliğini ihlal eden unsurları belirlemeye ve ayrıştırmaya yardımcı olmak için bir sınıflandırma yaklaşımı, Şekil 13.3'de verilmiştir. Bu sınıflandırmada:



Şekil 13.3. Biyometrik Sistemlerde Güvenliği Tehdit Eden Unsurlar [18]

- Biyometrik sistem hataları, uygulama geliştirme hatalarını, fiziksel hataları ve kullanım ortamı ile etkileşimden kaynaklanan harici hataları ve kullanıcı hatalarını içerir. Biyometrik sistemin geliştirilmesinde kullanım ortamı, kullanıcı kitlesi, kullanım amacı vb. unsurlar göz önünde bulundurulmalı ve olası risk senaryoları bu unsurlar dâhilinde değerlendirilir.
- Biyometrik sistem ihmalleri, istem fonksiyonlarının doğru uygulanamamasından dolayı oluşan sapma olarak tanımlanabilir. Sunulan hizmetin çalıştığı servisler, sistem geliştirilmesinde dikkat edilmeyen unsurlar, oluşan risk senaryolarını öngörememe,

sistem performans düşüklüğü, üretilen sonuçların geçerliliğinin azalması gibi sonuçlar doğurur.

- Biyometrik saldırılar ise kullanıcı veya saldırgan tarafından sistemi devre dışı bırakmak ya da atlatmak için tasarlanmış doğrudan veya dolaylı yoldan gerçekleştirilen eylemler olarak tanımlanmaktadır.

Şekil 13.4. Biyometrik Sistemlerin Açıklıkları [20]

Biyometrik sistemlerin güvenliğini tehlikeye sokabilecek risk faktörleri ve saldırı senaryoları Şekil 13.3 ve Şekil 13.4'de verilen hususlar temel alınarak farklı başlıklar altında değerlendirilmiş olup aşağıda maddeler halinde verilmiştir [21]. Bunlar;

(1) Biyometrik sistemdeki güvenlik açıklıkları büyük ölçüde sistem tasarımına, uygulama ve işletme yapısına, kullanılan biyometrik veri türlerine ve uygulanan yönetim politikalarına bağlıdır. Bu alanların her biri kendine ait farklı güvenlik açıklıklarına sebebiyet vermektedir. Bu sebeple uygun önlemlerin alınması için her bir bileşen kendi içinde ve birbirleri ile olan etkileşimleri açısından değerlendirilmelidir.

(2) Sistem tasarımı ve yapısı; sistemin donanım ve yazılım modüllerini, işlevleri ve iletişim protokollerini içeren modülleri ve diğer sistemler veya alt sistemler ile etkileşim içinde olan modülleri içerir. Sistem donanımının güvenliği hayati öneme sahiptir. Bilgi sistemlerine yapılan saldırıların çoğu ağ bağlantıları üzerinden uzaktan gerçekleşir. Biyometrik sistemin donanımı güvenli bir

yerde bulunmadığı takdirde saldırganlar tarafından kolayca hedef haline gelebilir. Bir biyometrik sistemin çalışma prensibinin temelinde kullanıcının bir donanım ile etkileşiminin söz konusu olması sebebiyle, donanımdan kaynaklı güvenlik açığı olumsuz etkiler oluşturabilir.

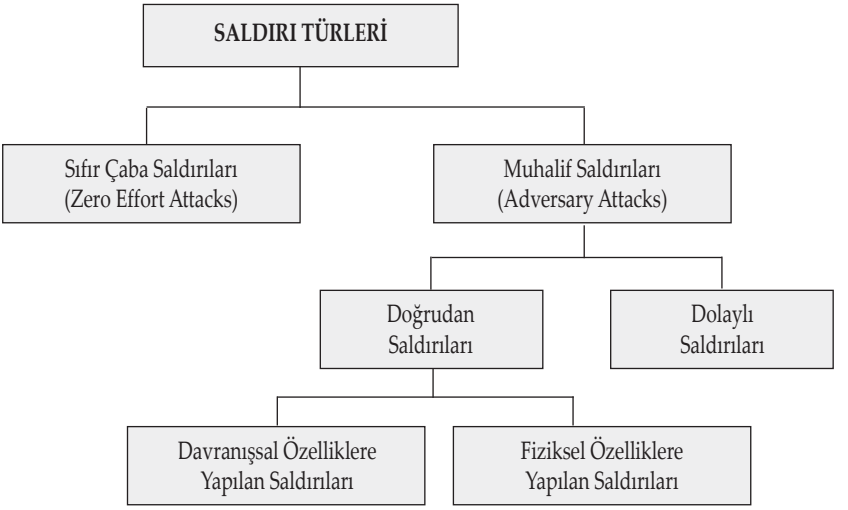
(3) Biyometrik veriler toplanır, işlenir ve sonucu bir iletişim kanalı üzerinden gönderilir. Biyometrik sistemin normal çalışmasının bir parçası olarak depolanır ve saklanır. Verilerin bütünlüğü ve gizliliği, her işlem aşamasında muhakkak muhafaza edilmelidir.

(4) Veri edinimi ve depolama sırasında, biyometrik verinin yapay olarak üretilen bir veri ile değiştirilmemesi garanti altına alınmalıdır. Sistem yazılımı ayrıntılı olarak test edilmeli ve saldırganın müdahalelerine karşı dirençli olmalıdır. Özellik çıkarımı için sistem tarafından alınan ve işlenen verinin güvenli bir hat üzerinden iletilmesi, değiştirilmemesi ve saldırgan tarafından sahte verinin iletilmemesi garanti altına alınmalıdır.

(5) Özellik çıkarımı modülünden çıkarılan verilerin güvenli bir şekilde veri tabanına gidebilmesi, aktarım sırasında bu verilerin değiştirilmemesi, veri tabanına sadece doğru kaynaktan veri akışının gerçekleşmesi, veri tabanına izinsiz biyometrik verinin yerleştirilememesi, değiştirilememesi veya silinmemesi gerekmektedir.

(6) Biyometrik sistemlerin ilişkili olduğu alt sistemlerde yer alan güvenlik açıklıkları ana mekanizma güvenliğine doğrudan ya da dolaylı yoldan etki etmektedir. Saldırganların biyometrik sisteme saldırı yapmak için söz konusu alt sistemleri bir araç olarak kullanmadığından emin olmak için önlemler alınmalıdır.

(7) Güvenlik açıklıklarına sebebiyet verecek bir diğer alan sistem yönetim ve işletme politikalarıdır. Biyometrik kayıt sürecine ilişkin politikalar, sistem güncellemeleri, yapılacak denetlemeler, arka planda çalışan altyapılar, çalışan personel ve kullanıcıların eğitim seviyeleri iyi değerlendirilmelidir. Bu alanlardan herhangi birinde gösterilen zafiyetin sisteme güvenlik açığı olarak geri dönüş yapacağı bilinmelidir.



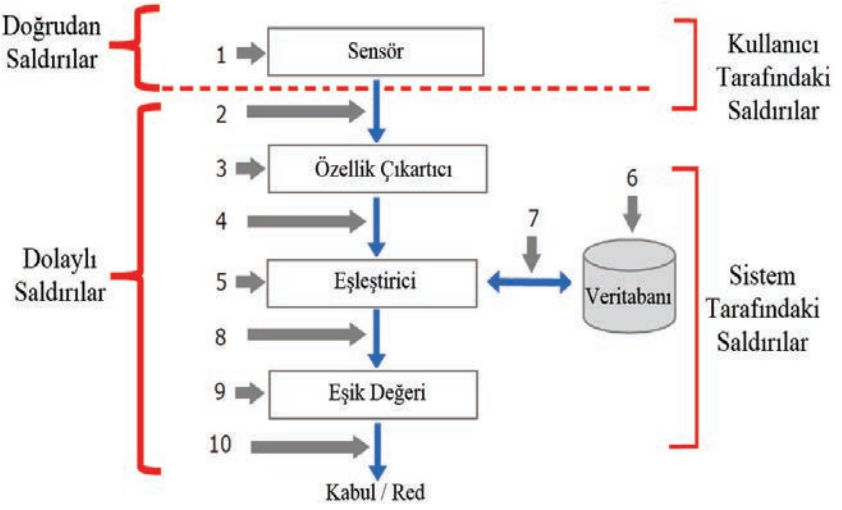
Şekil 13.5. Biyometrik Sistemlere Yapılan Saldırıların Sınıflandırılması [22]

Biyometrik tabanlı kişisel kimlik doğrulama sistemleri bilgiye dayalı geleneksel güvenlik sistemlerine kıyasla sayısız üstünlüklerine rağmen, güvenilirliklerini önemli ölçüde azaltabilecek eksiklikleri de bünyesinde barındırmaktadır. Bu eksiklikleri ifade edebilmek adına, biyometrik sistemlere yapılan saldırılar gerçekleştirilme biçimlerine göre sınıflandırılmıştır ve Şekil 13.5 ve 13.6'da verilmiştir. Bu şekillerdeki bazı hususlar aşağıda kısaca açıklanmıştır [9,22-24]:

- Sıfır çaba saldırıları içsel başarısızlık olarak da bilinir. Tüm biyometrik sistemlerde önlenmesi imkânsız olan bu tehdit, iki farklı denekten gelen iki biyometrik örneğin pozitif bir eşleşme üretecek kadar aynı olma ihtimalinden kaynaklanmaktadır.
- Muhalif (adversary) saldırılar; biyometrik sisteme kayıtlı olan kötü niyetli bir kullanıcının veya sisteme kayıtlı olmayan bir saldırganın onunla etkileşime giren sistemi daha önce düşünülmeyen bir şekilde atlamaya çalışması anlamına gelir. Bu muhalif saldırılar doğrudan ve dolaylı saldırılar olarak gruplandırılmıştır.
- Doğrudan saldırılar; biyometrik sistemin nasıl çalıştığı hakkında derin bilgi birikimi ve kullanılan eşleştirme algoritması, özellik vektörü biçimi vb. konularda uzmanlık alan bilgisi gerektirmeyen saldırılar olarak ifade edilmektedir. Bu saldırıların amacı; gerçek bir kullanıcının şablon bilgisini ele geçirmek veya gerçek

bir kullanıcıyı taklit etmeye çalışabilmek için sensöre sahte bir biyometrik şablon sunmaya çalışmaktadır.

- Dolaylı saldırılar doğrudan saldırıların aksine, saldırıyı başarılı kılmak için kimlik doğrulama sisteminin iç işleyişi hakkında bilgi birikimi gerektiren saldırılardır. Bir saldırganın dolaylı saldırılar gerçekleştirebilmesi için, sistem hakkında spesifik bilgilere sahip olması gerektiğinden, bu saldırılar gerçekleştirilirken biyometrik sisteme fiziksel ve mantıksal erişime ihtiyaç duyulmaktadır. Buna ek olarak bazı saldırılarda tersine mühendislik teknikleri de kullanılmaktadır.



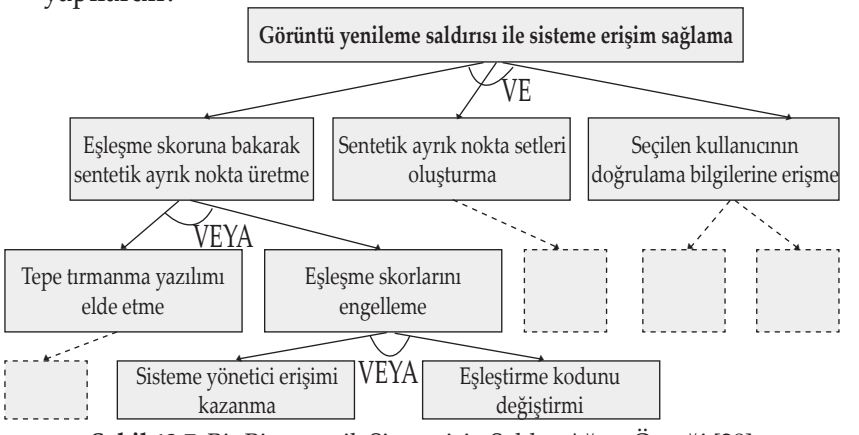
Şekil 13.6. Doğrudan ve Dolaylı Saldırıların Etkilediği Biyometrik Sistem Bileşenleri [25,26]

Bir biyometrik sistem oldukça karmaşık olabilir, sistemin tek bir bölümü bile birden fazla saldırıya maruz kalabilir ve her saldırı birden fazla koldan gerçekleştirilebilir. Karmaşık biyometrik sistemlerdeki göreceli tehdit seviyelerini anlamak için, saldırının hiyerarşisi, genellikle "saldırı ağacı" denilen yönlendirilmiş bir grafla ifade edilir. Ağacın tepesinde belirli bir saldırı yer alır. Bir sonraki aşamada bu saldırının tüm gereksinimleri gösterilir. Her ardışık seviyede, bir önceki madde için yerine getirilmesi gereken şartlar ayrıntılı olarak verilir. Gereksinimlerin koşullu yapıları, dal bağlantılarında VE ya da VEYA kullanımıyla ağaç yapısı olarak gösterilebilmektedir. Bazı

durumlarda, ağacın her düğümüne tehdit, zorluk, fırsat ve kaynak gereksinimi için göreceli bir puan verilir. Sistemdeki her tehdit, koruma stratejilerini belirlemek için ayrı ayrı ve toplu olarak ele alınabilir [21,27].

Saldırı ağaçları [21,27];

- güvenlik açıklıkları analizini basitleştirmeyi amaçlayan,
- savunma mekanizmaları geliştiren tasarımcının bir sistemin nasıl saldırıya uğradığını anlayabilmesini sağlayan,
- saldırıları engellemek için karşı önlemler geliştirmeyi kolaylaştıran,
- saldırının karmaşıklığını zihinsel olarak sindirmeye çalışmak yerine saldırının grafik olarak görüntülenmesine yardımcı olan,
- saldırının hedefini kök düğüm, bu hedefe ulaşmanın bir yolunun yaprak düğümler ile gerçekleştiği bir saldırının temsili halini ifade eden,
- bir saldırı ağacının nasıl oluşturulacağına dair bir dizi kural içeren,
- bu kurallar dâhilinde saldırı hedefleri, saldırgan işbirlikleri, saldırının basamakları, saldırganların arasındaki hiyerarşiler vb. sonuçları ağaç sayesinde bütüncül bir bakış açısıyla değerlendirilmesine yardımcı olan ve Şekil 13.7'de ise bir örneği verilen yapılardır.



Şekil 13.7. Bir Biyometrik Sistem için Saldırı Ağacı Örneği [28]

13.5. Biyometrik Saldırı Modelleri

Biyometrik sistemler geliştirme sürecinde uygun denetleme mekanizmaları ile test edilmediği takdirde saldırılara karşı savunmasız kalmaktadır. Bu sistemlerin erişim kontrolü, kontrollü giriş-çıkış denetimi, yetkilendirme vb. kritik alanlarda kullanıldığı düşünüldüğünde, saldırganlar tarafından sistemlere sızmak için gerekli motivasyonun oldukça yüksek olduğu bilinmektedir. Bu sistemlerde kullanılan ve her kişi için benzersiz olan biyometrik veri ele geçirildiği takdirde, bu verinin bilgi tabanlı şifreleme mekanizmaları gibi kolayca değiştirilememesinden kaynaklanan sorunlar ortaya çıkmaktadır. Bir biyometrik sistemin güvenilirliğini değerlendirebilmek için biyometrik sistemin gizliliğini, bütünlüğünü ve kullanılabilirliğini garanti altına almak gerekmektedir. Biyometrik sistemler için güvenli bir ortam geliştirmeye başlanmadan önce, ilk olarak oluşabilecek problemler açıkça tanımlanmalı ve üzerinde çalışılması gereken tehditler tespit edilmelidir. Bu nedenle, biyometrik sistemlerin güvenilirliğini kontrol etmek için saldırı modelleri geliştirilmiştir. Bu modellerde kullanılan farklı değerlendirme parametreleri ve bakış açıları ile güvenilirliği yüksek platformlar tasarlanması amaçlanmıştır.

Bir biyometrik sistemin bileşen tasarımının ve sistem entegrasyonunun konvansiyonel güvenlik analizini yapabilmek için tehdit modelleri ve olası güvenlik açıklıklarının ortaya çıkacağı senaryolar düşünülmelidir. Biyometrik sistemin kullanım amacı, kullanıldığı ortam ve kullanıcıları değerlendirilerek sistem bileşenlerine uygun bir tehdit modeli geliştirilmelidir. Bu tür bir sistemi modellemeden önce, saldırganların hangi tür kaynakları kullanabileceğini, geçmiş saldırı örnekleri ve gerçekleşmesi olası durumlar değerlendirilmelidir [29].

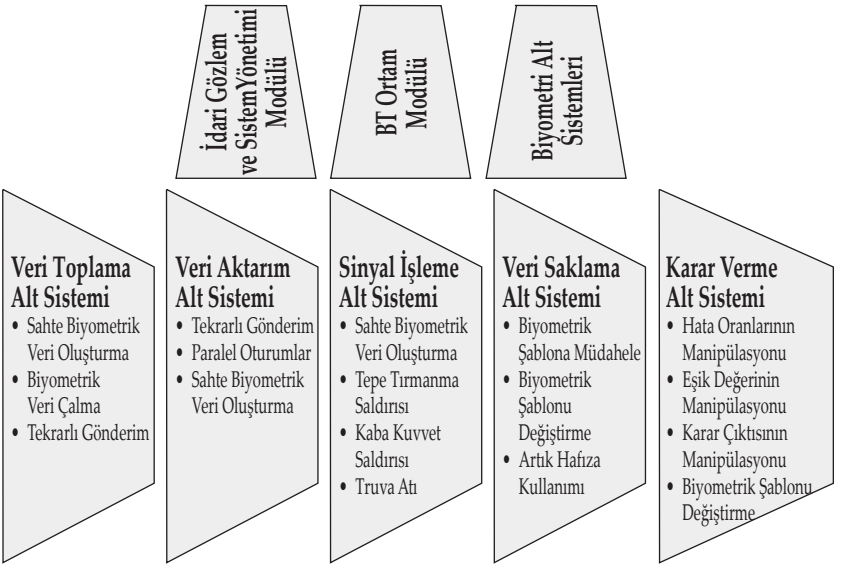
Biyometrik sistemlerin güvenlik açıklıklarını tespit edebilmek için ilk saldırı modeli Ratha ve arkadaşları tarafından önerilmiştir (Şekil 13.8). Bu modelde [30], biyometri temelli kimlik doğrulamanın güçlü ve zayıf yönleri ana hatları ile açıklandıktan sonra, sistemdeki zayıf bağlantı noktaları tespit edilerek bu zayıf bağlantıların tamamını ya da bir kısmını ortadan kaldırmak için yeni çözümler üretilmiştir. Modelde saldırının gerçekleşebileceği 8 kritik nokta; sahte biyomet-

rik, tekrarlı gönderim, öznitelik çıkarımı işleminin etkisiz kılınması, öznitelik vektörünün değiştirilmesi, eşleştiricinin etkisiz kılınması, veri tabanında saklanan şablonlara yetkisiz erişim, şablon verisinin değiştirilmesi ve eşleştirici sonucunun değiştirilmesi olarak tanımlanmıştır [30,31].

Şekil 13.8. Ratha Modeli Bileşenleri ve Saldırı Örnekleri [30]

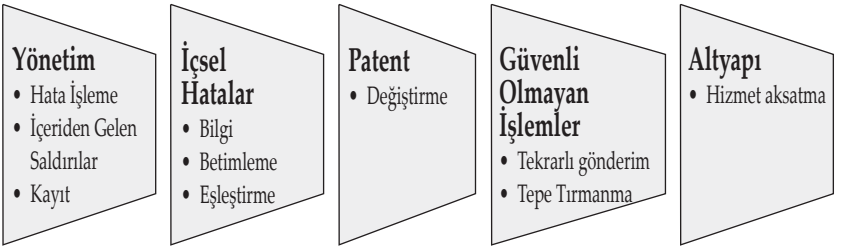
Biyometrik sistem bileşenlerine ve iletişim kanallarına yapılan spesifik saldırılar göz önüne alındığında, Ratha ve arkadaşlarının modelinin tehdit unsurlarını çok genel bir bakış açısı ile değerlendirdiği ve potansiyel saldırı noktalarının belirlenmesinde faydalı olabildiği belirtilse de, günümüz biyometrik sistemlerinin karmaşıklığı göz önüne bulundurulduğunda, bu modelin güvenlik açıklıklarının tespitinde yeteri kadar detaya inemediği görüldüğünden yeni modeller geliştirme ihtiyacı duyulmuştur [21,31].

Wayman [32] biyometrik sistemlerin çalışma mekanizmalarını anlayabilmek için makro bakış açısıyla sistem bileşenlerinin, mikro bakış açısıyla ise bileşenlerin kendi içindeki alt modüllerin incelenmesi gerektiğini düşünerek bir çerçeve önermiştir. Bu çerçevede potansiyel saldırı vektörlerinin daha detaylı analizinin gerçekleştirebilmesi için, biyometrik sistem bileşenleri olarak tanımlanan sensör modülü, özellik çıkarma modülü, eşleştirme modülü ve karar modülüne ek olarak bahsedilen bu modellerin iletişimleri de bir bileşen olarak tanımlanmıştır. Bu modelde sistem bileşenlerinin birbirleri ile olan ilişkileri modellenmiştir ve sistem üzerinde hizmet veren teknik cihazların güvenilirliği test edilmiştir [21,32].



Şekil 13.9. Bartlow ve Cukic Modeli Bileşenleri ve Saldırı Örnekleri [31,33]

Bartlow ve Cukic Modeli [33], Wayman'ın biyometrik sistem bileşenleri ve alt bileşenlerini içeren çerçeveden ilham alınarak geliştirilmiş bir saldırı modeli olup, Ratha'nın biyometrik sistemler için hassas noktaları belirlerken kullandığı yaklaşımı daha önemli ayrıntı düzeyleriyle birlikte değerlendirmiştir. Bartlow ve Cukic Modeli, Wayman'ın mantık mimarisinde kalabilmek için, her bir parçayı detaylandırırken idari ve çevresel özellikleri alt sistemler olarak modellemiştir. Wayman modeli sadece biyometrik sistemi ve alt bileşenlerini tanımlayabilmek için bir mimari önerirken, Bartlow ve Cukic modelinde yirmi potansiyel saldırı yapılabilecek nokta ve yirmi iki güvenlik açığı tanımlanmıştır [31,33].



Şekil 13.10. Fishbone Modeli Bileşenleri ve Saldırı Örnekleri [1]

Genel olarak biyometrik sistemlere yapılabilecek olası saldırıların değerlendirildiği modellerden farklı bir bakış açısı ile oluşturulan Fishbone Modeli [34], biyometrik sistemlerin zafiyetlerini tespit etmek üzere tasarlanmıştır. Bu modelde biyometrik sistemlerin, tasarımdan kaynaklanan içsel hatalar ve dışarıdan gelen saldırılar sebebiyle risk altında olduğu ifade edilmiştir. İçsel hatalar veri edinimi, özellik çıkarımında ve eşleştirme aşamalarında kaynaklanan arızalar olarak tanımlanırken, saldırılar ise alan bilgisine sahip kişilerin veya grupların motive olarak gerçekleştirdiği saldırılar olarak tanımlanmıştır [31,34].

13.6. Biyometrik Sistemlerin Güvenliği ve Mahremiyeti

Bilginin yaşadığımız çağa damgasını vuran bir varlık olduğu gerçektir. Günümüzde bilişim teknolojilerinin yaygınlaşması ve günlük hayatımızda yapmış olduğumuz iş ve işlemlerin elektronik ortamlarda hızla yapılmaya başlanması, bilgi güvenliğinin sağlanmasını zorunlu hale getirmektedir [35]. Siber güvenlik perspektifinden konuya bakıldığında bilginin açamadığı kapı yoktur. Bilgi aracılığı ile güç elde etmek ya da güç elde etmek için bilgiyi kullanmak, yapılacak eylemin saldırı mı ya da savunma mı olduğunu çok iyi anlamak ve tanımlamak gereklidir.

Bilgiyi koruyabilmek adına kimlik yönetimi sistemlerinde bugüne kadar kullanılan bilgi tabanlı güvenlik mekanizmaları yerini biyometri tabanlı yaklaşımlarına bırakmıştır. Hatta biyometrik yöntemlerin bile siber saldırılara karşı dirençsiz kaldığı durumlarda, çoklu-faktör ve çoklu-model biyometrik modeller, davranışsal biyometri gibi riski mümkün olduğunda azaltabilmek adına hibrit yöntemler ya da yardımcı yaklaşımlarla sistemleri güvenilir kılmak için alternatif çalışmalar yapılmaktadır [36]. Burada üzerinde durulması gereken asıl nokta; bilgiyi korumak için kullanılan yaklaşımların tam anlamıyla mükemmel olmadığı gerçeğidir. Kurumsal ya da kişisel bilgiyi korumak adına daha kritik bir bilgi olan biyometrik verilerin kullanılması riskli bir girişimdir. Bu sebeple, biyometrik sistemin tasarlanması sürecinde kullanıcıdan ve sistem bileşenlerinden kaynaklanabilecek tüm riskleri görebilmek ve karşılaşılabilecek problemleri çözmek için kapsamlı önerilerine ihtiyaç vardır. Bu bölümde; güvenlik sorunlarını ve risk faktörlerini asgariye indirmek için daha önce sunulan

çözüm önerileri gözden geçirilmiş, özetlenmiş ve sahip olduğumuz bilgi birikimine dayanarak bazı yeni önerilerde bulunulmuştur.

13.6.1. Veri Edinim Aşamasında Oluşabilecek Tehditler ve Çözüm Önerileri

Veri edinimi süreci; bireyden alınan ham biyometrik verinin, biyometrik sisteme adaptasyonunu sağlamak için dijitalleştirilmesidir [37]. Veri edinim aşaması biyometrik sistemler için çok kritiktir. Kullanılan ekipmanlar ve uygulama prosedürü iyi tasarlanmayıp veri edinim süreci iyi yönetilmez ise yeterli özellikte ve kalitede biyometrik veri toplanmaz. Veri edinim sürecinin düzgün bir şekilde tamamlanması tüm sistem başarısına doğrudan etki etmektedir. Buna ek olarak; veri edinim aşamasında ham veriye doğrudan erişebilme ihtimali, bu aşamanın saldırganlar tarafından hedef alınmasına yol açmaktadır. Tablo 13.1'de veri edinim aşamasında saldırganların hedefleri, saldırı türleri ve bu saldırılar için alınan tedbirler detayları ile açıklanmıştır. Veri edinim sürecinde gerçekleşebilecek saldırılar genel olarak sınıflandırılarak, bu saldırıları engelleyebilmek için çözüm önerileri geliştirilmiştir.

Veri edinim sürecinde gerçekleştirilen saldırılar aşağıda maddeler halinde verilmektedir. Bunlar:

- sahte veya dijital biyometrik verinin sisteme eklenmesi
- biyometrik verinin değiştirilmesi veya yetkisiz bir biyometrik verinin sisteme eklenmesi
- biyometrik verinin kopyalanması ve
- sistemi devre dışı bırakma ya da engellemedir.

Bu saldırılar için sunulan çözüm önerileri aşağıda maddeler halinde özetlenmektedir [38,39]:

- Sentetik olarak üretilmiş biyometrik veriyi tespit etmek için canlılık tespitine dayalı yaklaşımlar kullanılmalıdır.
- Bazı sensörler okunan biyometrik verileri hafızalarında geçici olarak saklayabilmektedir. Bu nedenle sensörlere yapılacak saldırılarına karşı sensör hafızaları düzenli olarak silinmelidir.
- Saldırganların sisteme erişimini engelleyebilmek adına farklı biyometrik özelliklerin kullanıldığı sistemler kullanılmalıdır. Bu durumda birden fazla biyometrik veri aynı anda doğrulanmaya çalışılarak sistem daha karmaşık hale getirilmelidir. Son olarak;

- Bir biyometrik karakteristik özelliğin yanında bilgi tabanlı bir şifreleme mekanizması kullanılarak sistem güvenliği arttırılabilir. Özellikle sistemin devre dışı bırakılmaya çalışıldığı saldırılarda, çok fazla sayıda erişim talebi yapan saldırgan askıya alınarak sistem güvenliği sağlanabilir.

13.6.2. Yazılım Bileşenlerini Tehdit Eden Unsurlar ve Çözüm Önerileri

Biyometrik sistemlerin özellik çıkarımı, özellik eşleştirme ve karar verme aşamalarında kullanılan yazılım bileşenleri ve bu bileşenlerin birbirleri ile iletişimini hedef alan saldırılar yazılım seviyesi saldırılar olarak ifade edilir. Tablo 13.1'de özellik çıkarımı, özellik eşleştirme ve karar verme aşamalarında saldırganların hedefleri, saldırı türleri ve bu saldırılar için alınan tedbirler detayları ile açıklanmıştır. Yazılım seviyesinde gerçekleşebilecek saldırılar genel olarak sınıflandırılarak, bu saldırıları engelleyebilmek için çözüm önerileri geliştirilmiştir.

Özellik çıkarımı, özellik eşleştirme ve karar verme sürecinde gerçekleştirilen saldırılar aşağıda maddeler halinde verilmektedir. Bunlar:

- öznitelik çıkarım modülüne yapılan izinsiz müdahaleler (sahte öznitelik çıkarma, öznitelik çıkarma algoritmalarını devre dışı bırakma, çıkartılan öznitelikleri ele geçirme vb.)
- eşleştirme modülüne yapılan izinsiz müdahaleler (Eşleştirme algoritmasını devre dışı bırakma, eşleşme skorunu değiştirme vb.)
- karar verme modülüne yapılan izinsiz müdahaleler ve
- bileşenleri devre dışı bırakma ya da engellemedir.

Bu saldırılar için sunulan çözüm önerileri aşağıda maddeler halinde özetlenmektedir:

- Özellik çıkarımı, eşleştirme ve karar verme modüllerinde kullanılan algoritmalar saldırılara karşı dayanıklı olacak şekilde geliştirmelidir.
- Doğru sonucu elde edene kadar sisteme erişip tekrar tekrar deneme yapılmasını engellemek adına, erişme talebi tekrarına bir limit konulmalı ve limit aşımı durumunda yapılan talepler askıya alınmalıdır.

- Bileşenleri hizmet veremez hale getirme ya da ürettikleri çıktıları baskılama, değiştirme vb. işlemleri gerçekleştirebilmek adına kullanılan zararlı yazılımlara karşı biyometrik standartlar kullanılmalıdır.
- Sistemin her bileşeninde güvenli yazılım geliştirme teknikleri dikkate alınmalıdır.
- Geliştirilen yazılımlar muhakkak test edilmelidir.

Tablo 13.1. Biyometrik Sistemlere Yapılan Saldırıların Hedefleri, Saldırı Türleri ve Savunma Yöntemleri [40]

Hedef	Tehdit	Önlem
Veri Toplama	Zehirlenme (Spoofing)	Canlılık Tespiti
		Meydan Okuma/ Karşılık Verme Temelli Kimlik Doğrulama
	Güvenilmeyen cihazın kullanımı	Simetrik veya asimetrik anahtar ile karşılıklı doğrulama
	Hizmet Dışı Bırakma	Dayanıklı Cihaz Kullanımı
Veri İşleme	Sahte Verilerin Eklenmesi	Saldırılara Karşı Test Edilmiş Gürbüz Algoritmalar
	Bileşen Değiştirme	Onaylanmış Bileşenler
Eşleştirme	Sahte Verilerin Eklenmesi	Saldırılara Karşı Test Edilmiş Gürbüz Algoritmalar
	Bileşen Değiştirme	Onaylanmış Bileşenler
	Eşleşme Skorunun Manipülasyonu	Hata Ayıklayıcı
	Tepe Tırmanma Saldırısı	Kaba Puanlama
		Güvenilir sensör (Karşılıklı kimlik doğrulama)
		Güvenli İletim Kanalı
	Tahminleme (FAR saldırısı)	Saldırılara Karşı Test Edilmiş Gürbüz Algoritmalar
		1:1 Eşleştirme
		Çoklu Biyometrik / Çok Faktörlü Doğrulama
	Tepe Tırmanma Saldırısı	Kaba Puanlama
		Karşılıklı Doğrulama
		Güvenli İletim Kanalı
Karar Verme	Eşik Değeri Ayarının Manipülasyonu	Saldırılara Karşı Korunaklı Fonksiyonlar
		Veri Koruma
	Eşleşme Sonucunun Manipülasyonu	Hata Ayıklayıcı
	Bileşen Değiştirme	Onaylanmış Bileşenler
Uygulama	Zararlı Yazılım	Standart Kullanımı
		Kod İmzalama

Tablo 13.1. (devamı) Biyometrik Sistemlere Yapılan Saldırıların Hedefleri, Saldırı Türleri ve Savunma Yöntemleri [40]

Hedef	Tehdit	Önlem
Depolama	Veri Tabanı Saldırıları (şablon okuma, şablon değiştirme vb.)	Saldırılara Dayanıklı Sunucu
		Veri Tabanı Erişim Kontrolü
		Şifrelenmiş ve Özetlenmiş şablon
		Akıllı Kartlar Vb. Cihazlarda Şablon Depolama
Ham Veri Aktarımı	Telekulak saldırısı	Şifrelenmiş Güvenli İletim Kanalı
	Tekrarlı gönderim saldırısı	Simetrik veya asimetrik anahtar ile karşılıklı doğrulama
		Dijital İmzalı Veri
		TTL etiketi
	Ortadaki adam saldırıları	PKI sertifikası
		Şifrelenmiş Güvenli İletim Kanalı
İşlenmiş Veri Aktarımı	Kaba kuvvet saldırıları	Süre Aşım Politikaları
	Telekulak saldırısı	Şifrelenmiş Güvenli İletim Kanalı
	Tekrarlı gönderim saldırısı	Simetrik veya asimetrik anahtar ile karşılıklı doğrulama
		Dijital İmzalı Veri
		TTL etiketi
	Ortadaki adam saldırıları	PKI sertifikası
		Şifrelenmiş Güvenli İletim Kanalı
Biyometrik Şablon Alımı	Kaba kuvvet saldırıları	Süre Aşım Politikaları
	Telekulak saldırısı	Şifrelenmiş Güvenli İletim Kanalı
	Tekrarlı gönderim saldırısı	Simetrik veya asimetrik anahtar ile karşılıklı doğrulama
		Dijital İmzalı Veri
		TTL etiketi
	Ortadaki adam saldırıları	PKI sertifikası
		Şifrelenmiş Güvenli İletim Kanalı
Eşleşme Skoru Aktarımı	Tepe Tırmanma Saldırısı	Kaba Puanlama
		Güvenilir sensör (Karşılıklı kimlik doğrulama)
		Güvenli İletim Kanalı
	Eşleşme Skorunun Manipülasyonu	Güvenli İletim Kanalı
		Simetrik veya asimetrik anahtar ile karşılıklı doğrulama
İletişim Kanalları	Bileşen Değiştirme	Onaylanmış Bileşenler
	Telekulak saldırısı	Şifrelenmiş Güvenli İletim Kanalı
	Eşleşme Sonucunun Manipülasyonu	Şifrelenmiş Güvenli İletim Kanalı

13.6.3. Depolama Aşamasında Oluşabilecek Tehditler ve Çözüm Önerileri

Biyometrik sistem tarafından kayıtlı kullanıcıların biyometrik şablonlarını saklamak için kullanılan veri depolama bileşeni, veri edinim aşamasında toplanan ve güvenilir bir şekilde işlenen biyometrik verinin veri tabanına kaydedilmesinden sorumludur. Tablo 13.1' de depolama aşamalarında saldırganların hedefleri, saldırı türleri ve bu saldırılar için alınan tedbirler detayları ile açıklanmıştır. Eşleştirme işlemi için kullanılacak verilerin saklandığı depolama bileşenine yapılabilecek saldırılar genel olarak sınıflandırılarak, bu saldırıları engelleyebilmek için çözüm önerileri geliştirilmiştir.

Veri depolama sürecinde gerçekleştirilen saldırılar aşağıda maddeler halinde verilmektedir. Bunlar:

- Yetkisiz şablon oluşturma ve modifikasyonu ve
- Veri tabanına erişim ve biyometrik özelliklerin çalınmasıdır.

Bu saldırılar için sunulan çözüm önerileri aşağıda maddeler halinde özetlenmektedir:

- Veri tabanına doğrudan erişimi engellemek adına güvenlik metodolojileri, prosedürleri ve standartları uygulanmalıdır.
- Veri tabanında şablon verilerini saklamadan önce şifreleme ve özetleme yaklaşımlarını kullanılmalıdır.

13.7. Biyometrik Sistemlerinde Güvenlik Standartları

Biyometrik tanıma işleminin etkin, doğru ve güvenli bir şekilde gerçekleştirilebilmesi için belirli kriterlerin olması gerekir. Bu kriterleri sağlayabilmek, biyometrik uygulamaların geliştirilmesi ve çalıştırılması sırasında ortaya çıkabilecek sorunları giderebilmek, sistemi daha kullanışlı ve güvenli hale getirmek için standartlar geliştirilmiştir. Standartlar ayrıca birlikte çalışabilirlik, esneklik, güvenilirlik, istikrar, verimlilik ve gizlilik sağlar. Standartları uygun bir şekilde oluşturmak ve bunları biyometrik sistem geliştirilmesi ve kullanılması aşamalarında kullanmak, kalite ve güvenliği büyük ölçüde iyileştirir.

Biyometrik standartların temel amacı yüksek güvenilirlikli ve performanslı, düşük maliyetli sistemlerin geliştirilmesini sağlamaktadır. Bu kapsamda ulusal ve uluslararası standartlar incelenmiştir. Uluslararası Standart Organizasyonu (ISO), Uluslararası Elektroteknik Komisyonu (IEC) gibi organizasyonlar uluslararası standartlar sunmaktadır. ISO ve IEC organizasyonları bilim komiteleri oluşturarak, ISO/IEC JTC1 adı altında bilgi teknolojileri alanında faaliyet göstermek üzere SC17, SC27 ve SC37 standartlarını geliştirmişlerdir. Özellikle SC37 biyometri ile ilgili olarak biyometrik uygulama arayüzü, biyometrik veri değişim formatları, biyometrik veri değerlendirme kriterleri ve performans testlerinin standart hale getirilmesini hedeflemektedir. ISO/IEC 30107-1:2016 standardı ise biyometrik sistemlerin sensör seviyesi ile ilgili olan bir standart olarak sensöre yönelik yapılabilecek saldırıları önlemeyi hedeflemektedir. Bu standartlara ek olarak; IETF, W3C ve OASIS gibi biyometrik sistemler için geliştirilmiş pek çok standart vardır [41].

Biyometrik sistemler için ulusal ve uluslararası organizasyonlar tarafından geliştirilen standartlar; düşük sistem maliyeti ve yüksek sistem kalitesi ile birlikte güvenilirliği yüksek biyometrik platformlar oluşturmayı hedeflemektedir. Bahsi geçen standartlar, bir biyometrik sistemin geliştirilmesi sürecindeki gereksinimler ve dikkat edilmesi gereken güvenlik açıklıkları konusunda yol gösterici niteliktedir. Bu standartlar sayesinde geliştirilen sistemleri test edebilecek senaryolar geliştirilebilmektedir. Sonuç olarak, biyometrik sistemler gerek tasarım esnasında, gerekse işletim ve bakım esnasında standartlara uygun olarak ürünleştirilmeli, kullanılmalı ve belirli politikalar kapsamında da test edilmelidir.

13.8. Yeni Trendler

Biyometrik sistemlerde meydana gelen güvenlik açıklıkları, yapılan saldırılar, oluşan tehditler, bu açıklıklara karşı dirençli sistemler veya savunma sistemlerinin geliştirilmesi gerekliliği, önceki başlıklarda yapılan açıklamalardan çok net olarak görülebilecektir. Bu durumun kritikliği göz önüne alındığında yeni trendlere ve çözümlere her zaman ihtiyaç vardır. Bunun gerekçeleri ise;

- biyometrik verilerin ömür boyu kişiyi temsil etmesi,
- herhangi bir saldırgan tarafından biyometrik verilerin ele geçirmesi veya değiştirmesi durumunun telafi edilememesi,
- biyometrik verilerin korunmasının anayasal bir hak olması,
- ülkemizde biyometrik verilerin KVKK ile kişinin açık rızası ile toplanması ve işlenmesi, aksi durumda cezai işlemlerle karşılaşılması,
- biyometrik verilerin analizleri ile sonucu iyi olabilecek sonuçlar kadar kişisel mahremiyeti ihlal eden sonuçlar doğurabilecek olması,
- artık kişilerin değil ülke vatandaşlarının ortak davranışlarının ve ulus, millet, grup veya toplum biyometrilerinin de bugün sahip olunan teknolojiler ve uygulamalarla çözümlenebilmesi

olarak sıralanabilir. Bu hassasiyetlerden dolayı hem yeni çözümler geliştirilmeli hem de meydana gelebilecek yeni tehdit ve tehlikelerin de farkında olunmalıdır. Alt başlıklarda bu konular ele alınacak ve biyometriye yeni bakış açılarının neler olabileceği sunulacaktır.

13.8.1. Davranışsal Biyometri

Söz konusu siber güvenlik olunca, bir yandan savunma yöntemleri geliştirilirken bir yandan da yeni saldırı senaryolarının ortaya çıktığı günümüz dünyasının kaçınılmaz gerçeği, kusursuz güvenlik mekanizmalarının ütopik olmasıdır. Mevcut güvenlik mekanizmaları ile birlikte biyometrik tabanlı güvenlik yaklaşımlarının bile yetersiz kaldığı durumlar sebebiyle; bireyi doğrudan bir özellikten anlık kontrol etmek yerine sürekli teyit etme fırsatı sunan, toplanması ve analiz edilmesi biyometrik sistemlere göre daha kolay olan veriler ile bireyi tanımlayabilecek yenilikçi yaklaşımlara ihtiyaç duyulmaktadır.

Davranışsal biyometri [42];

- kullanıcının bilişsel ayak izi olarak tanımlanmaktadır.
- kullanıcının davranışı ile ilgili olarak belirli bir işlemi nasıl gerçekleştirdiğiyle ilgili özelliklere odaklanmaktadır.

- kullanıcının eylemlerini temel alarak kimliğini doğrulamak için kullanılabilecek benzersiz bir kullanıcı profili oluşturmaktadır.
- parola ve fiziksel biyometri tabanlı geleneksel kimlik doğrulama yöntemleri statik modellerdir ve kullanıcıya bir kerelik doğrulama sonucunda uzun süreli yetkilendirme hizmeti sunar.
- risk puanına dayalı, sürekli ve dinamik kimlik doğrulama modeli önermektedir.
- çok faktörlü kimlik doğrulama stratejisine bir uygulama katmanı ekleyerek sürekli kimlik doğrulama hizmeti özelliğini kazandırmaktadır.
- kimlik doğrulanması, mevcut kimlik doğrulama yöntemlerinin güvenlik seviyesini arttırabilen bir yaklaşımdır.

Yukarıda yapılan açıklamalar konunun önemini bizlere göstermektedir. Bu sebeplerden dolayı son yıllarda konuya karşı yoğun bir ilgi vardır.

Siber güvenliğin gündeminde yer alan biyometri güvenliği ve mahremiyeti sağlayabilmek için parmak izi, yüz, iris gibi karakteristiklerin güvenlik mekanizmalarında kullanılması ile kurulan biyometri-güvenlik ilişkisi uzun zamandır devam ederken, alternatif bir yaklaşım olarak görülen davranışsal biyometri, siber güvenlik dünyasına da hızlı bir giriş yapmıştır. Davranışsal biyometrinin siber güvenlik ile iletişiminin bu kadar popüler olmasının altında aşağıdaki sebeplerin olduğu tespit edilmiştir. Bunlar [43-45]:

- Klasik biyometri tabanlı sistemlerin çalışma mekanizmaları statiktir. Kullanım açısından belirli bir prosedürü takip etme zorunluluğu biyometrik sistemlerin uygulanabilirliğini azaltmaktadır. Bu kapsamda davranışsal biyometri daha dinamik bir biyometrik form doğurarak uygulamanın entegrasyon sürecini kolaylaştırmıştır.
- Bireyi tanımlama için fiziksel özellikleri kullanan statik biyometrik sistemlerin veri toplama, özellik çıkarımı, depolama ve eşleştirme bileşenlerinde kullanılan teknolojiler ve donanım altyapıları yüksek maliyetlidir. Başka bir deyişle; geleneksel biyometride bireyin kim olduğu üzerine odaklanmak ve bunun tespitini

yapmak için kullanılan veriler, ortamlar ve analiz yöntemleri, davranışsal biyometride bireyin ne yaptığını tanımlayan veriler, ortamlar ve analiz yöntemlerine göre daha maliyetlidir.

- Siber güvenlik perspektifinden bakıldığında davranışsal biyometrinin yüksek güvenirlikli platformlar oluşturma konusunda çığır açan bir etkiye sahip olduğu görülmektedir. Bunun sebebi ise, davranışsal biyometrinin kullanıcıya sürekli kimlik doğrulama (continuous authentication) hizmeti sunmasıdır. Daha spesifik olarak ifade edilirse; geleneksel biyometrik sistemlerde erişim kontrolü için yapılan anlık taleplerin sonrasında oturumun güvenilirliğini değerlendirebilen herhangi bir mekanizmanın olmaması ve davranışsal biyometrinin bu kapsamda harici bir güvenlik katmanı kullanarak oturumun açık olduğu süre boyunca bireyi kontrol edebilme fırsatı sunması, davranışsal biyometrinin siber güvenlik ile olan ilişkisini güçlendirmiştir.

Sonuç olarak, davranışsal biyometrinin gelecekte yeni çözümlerin geliştirilmesine yüksek katkı sağlayacağı değerlendirilmektedir. Dolayısıyla, bu konularda daha çok çalışmalar yapılmalı, bu yaklaşımlar yeni çözümlere ve uygulamalara adapte edilmeli, karşılaşılabilecek olumsuzluklara karşı önlemler geliştirilmeli ve en önemlisi bu konuda bilgi birikimleri artırılmalıdır.

13.8.2. Sosyal Ağ Biyometrisi: Sosyometrik Biyometri

Sosyal ağ; bireylerin ağ unsurlarını kullanarak birbirleri ile etkileşimleri sonucu oluşturdukları bir dizi sosyal ilişkiyi tanımlayan sosyolojik bir kavramdır [46]. Bireylerin sosyal ağlara karşı artan ilgisi, bu mecralardan yeni çıkarımların, teknolojilerin, algoritmaların, yaklaşımların veya uygulamaların geliştirilmesinin önünü açmış, bazılarına göre de sonucu gelecekte olumsuz olabilecek pek çok çalışmasının da yapılmasına fırsat doğurmuştur. Küreselleşme ve gelişen teknolojilerin etkisiyle, sosyal ağlarda paylaşılan her türlü içeriğin analiz edilmesine imkân veren veri bilimi yaklaşımları ise artık gündemde olan önemli araştırma konuları arasındadır. Sosyal ağ terimi, ilk kez 1950 yılında, sosyal davranış hakkında veri elde etmek ve analiz etmek isteyen bilim olan sosyometride kullanılmıştır. Daha önceden hesaplanması imkânsız, karmaşık ve yetersiz mate-

matiksel modellemelerle analiz edilemeyen sosyal ağ verilerinden anlamlı sonuçlar elde edilmesi sosyal ağ analizini ve veri analitiği yöntemlerinin gelişimini tetiklemiştir [47].

Günümüzde, bireyler farklı sosyal medya platformlarında farklı içeriklere veriler paylaşmaktadır: bloglar (Blogger, LiveJournal), mikro bloglar (Twitter, FMyLife), sosyal ağlar (Facebook, LinkedIn), wiki siteleri (Wikipedia, Wetpaint), sosyal yer işareti (Delicious, CiteULike), sosyal haberler (Digg, Mixx), yorumlar (ePinions, Yelp) ve multimedya paylaşımı (Flickr, Youtube) [47]. Sosyal ağ platformlarında bireylerin günlük dilleri ile yaptıkları bu paylaşımlar belirli bir şablona sahiptir. Her bireyin kendine göre sosyal açıdan anlamlı ve önemli olduğunu düşündüğü bir içeriği paylaşması, zaman içerisinde bireyler arasındaki farklılıkların paylaşılan bu içeriklerden gözlemlenebildiğini ortaya koymuştur. Bireylerin paylaşımları onları tanımlayan bir modelin geliştirilmesinde kullanılabilmektedir. Bireyin kullandığı dil örneklenerek, insan kişilik özelliklerinin hiç olmadığı kadar ayrıntılı bir sınıflandırması yapılabilmektedir [48].

Bireylerin sanal dünyada yaptıkları paylaşımlardan; cinsiyetinin, inancının, tercihlerinin, düşüncelerinin, hastalıkların veya kişiliklerinin tahminlenmesi için kullanılan kişilik araştırmaları fikri çok eskiye dayanmaktadır. Parmak izinin bireyi ayırt edici özellikte olduğu ve bu özelliğin adli vakaları incelemede kullanılabileceği fikrini ortaya atan Francis Galton, aynı şekilde bireyin kullandığı dilin bireyi ayırt edici bir unsur olduğu belirtmiştir [49]. Sonrasında bireyi tanımlamak adına kullanılan Beş Faktörlü Model ile (diğer adı ile OCEAN model), bireyi tanımlamak için kullanılan beş temel kişilik özelliğinin bireyin dilsel örneklerinden çıkarılabildiği görülmüştür. Bu modelde bireylerin sözel ifadelerinde yer alan kişilik tanımlayıcı sözcükler kullanılarak kişilik özellikleri tespit edilmiştir [50].

Bireyi tanımlamak için geleneksel yöntemler kullanmak yerine bireyin kişilik özelliklerini betimleyen metin içerikli paylaşımlar, tıklamalar, beğeniler (like), beğenilmeyenler (dislike), yönlendirenler, kullanıcı etkinlikleri, açık ve gizli mesajlar, eklenen veya silinen arkadaşlar veya arkadaşlıklar, paylaşılanlar (hobiler, resimler, yazılar), ilgi alanları, erişim sıklıkları, favoriler, indirilen veya yüklenen veriler vb. kullanılarak, sanal sosyal mecra ile kurulan her etkile-

şimde bırakılan izler ile kullanıcıların kişiliğini ilişkilendirmek hatta doğrudan tespit etmek mümkündür [51].

Buna en çarpıcı örnekler, Prof. Dr. Michal Kosinski ve arkadaşlarının 2013'de PNAS'da yayımladıkları çalışmada bulunulabilir [59]. Bu çalışmada, sanal ortamda yapılan beğeniler dikkate alınarak yapılan analizlerde, kullanıcıların hristiyan ve müslüman ayrımının %82 oranında, demokrat ve cumhuriyetçi ayrımının %85, cinsel yönelimlerin tespitinde erkeklerde %88 kadınlarda ise %75 oranında başarı elde edilebildiği, madde kullanımının %73 oranında tespit edilebildiği, ebeveynlerin ayrı veya birlikte yaşadığının %60 oranında belirlenebildiği raporlanmıştır. Kosinski ve arkadaşlarının yaptığı çalışma aslında, elektronik ortamda kişisel veri işlemenin reklam gösteriminden çok daha farklı sonuçları olabileceğini bizlere göstermektedir. Buna verilebilecek diğer önemli örnek, Cambridge Analytica Skandalı'dır [60]. Milyonlarca kullanıcının sosyal ağ platformlarındaki paylaşımlarının toplanarak analiz edildiği ve elde edilen sonuçlar doğrultusunda ABD seçimlerinde destekledikleri partiyi değiştirmek için kişilerin etki altına alındığı bu olay göstermektedir ki; toplumların yönelimlerini ve reaksiyon gösterdikleri veya etkilendikleri unsurları anlayabilmek için sosyal medya paylaşımlarını analiz etmek yeterli olabilmektedir. Bugün için sosyal medyadan elde edilen verilerden, parmak izi gibi kişileri belirleyebilecek 50.000'in üzerinde özelliğin bulunduğu belirtilmektedir [60].

Gelecekte bu konuda pek çok çalışmanın karşımıza çıkabileceği muhakkaktır. Özellikle, toplumsal biyometrik veri analizleri ile elde edilen sonuçların ulusal kazanç sağlamasının yanında aslında ulusal güvenliği tehdit edeceği ortadadır. Bu konuda çalışmalar artıkça farklı sonuçların elde edilebileceği, konuya daha çok önem verileceği değerlendirilmektedir.

13.8.3. Siber Antropolojinin Gerçeği: Toplumsal Biyometri

Antropoloji; biyolojik bir varlık olarak kabul edilen insanın morfolojik, anatomik ve fizyolojik özellikleri ve bu özelliklerin oluşumuna etki eden faktörleri inceleyen bilim dalıdır. İnsanı bahsi geçen özellikleri üzerinden değerlendirebilmek için birçok farklı disiplin

ile birlikte çalışır [52]. Biyometrik sistemlerin dünya tarihindeki gelişim süreci değerlendirildiğinde, biyometri ile antropoloji arasındaki derin bağlantıları görmemek imkânsızdır. Antropolojide bireyi tanımlamak için kullanılan özelliklerin bazıları her birey için eşsiz olarak görülmüştür ve bu özellikler biyometri başlığı altında incelenmiştir. Bu sebeple antropoloji bilimi, yeni bir biyometrik teknolojinin geliştirilmesinde ve değerlendirilmesinde eşsiz bir rol oynamakta, bireyin fiziksel açıdan incelendiği biyolojik antropoloji ve bireyi sosyal/ kültürel açıdan inceleyen antropoloji olarak ikiye ayrılmaktadır [52]. Günümüzde; siber dünyanın toplumsal bir alana dönüştüğü ve sanal toplulukların tıpkı geleneksel topluluklar gibi kurallar ve normlar geliştirmesi sebebiyle, siber dünyanın araştırılması için antropolojik bir bilincin gerekliliği ortaya çıkmıştır [53].

Gelişen teknoloji ve buna bağlı olarak internetin hızla yayılması ile birlikte iletişim yöntemleri de değişiklik göstermiştir. İnternetin kullanıldığı teknolojilerin yaygınlaşması ile birlikte, gerçek hayatta içinde bulunduğumuz toplulukların sanal versiyonları ortaya çıkmıştır. Bu sanal topluluklarda bireylerin birbirleri ile etkileşimleri, yapılan bilgi/veri alış verişi, kurulan ilişkiler sosyal medyayı oluşturmaktadır [54,55]. "We Are Social 2017" yayınladığı rapora göre dünyada 2,8 milyar aktif sosyal medya kullanıcısı bulunmaktadır [56]. Bu kadar kullanıcının bulunduğu bir mecrada; her saniye, her an, milyonlarca içerik paylaşılması ise kaçınılmazdır. Bu kadar çok veri üreten kullanıcının olduğu internet dünyasında, araştırmacılar için artık internet yeni bir veri kaynağıdır [54]. Sosyal medya platformlarından toplanan bu veriler üzerinde siber antropolojik yöntemler kullanılarak toplumların;

- ekonomik, politik, siyasal, dini görüşleri ve ilişkileri,
- tutum ve davranış kalıpları,
- hassas noktaları ve problemleri ile
- durumlara ve olaylara verdikleri reaksiyonları vb.

artık tespit edilebilmektedir.

Bugün büyük veri analitiği ve güvenliği konusunda geliştirilen teknik ve teknolojilerle yapılan uygulamalar değerlendirildiğinde;

siber antropolojinin geldiği nokta daha iyi anlaşılabilir. Sosyal ortamlardan elde edilen kullanıcı bilgileri temel alınarak, toplumun tutum ve davranış kalıplarının öğrenilebileceği görülmektedir. 2009 yılında Nature dergisinde yayımlanan makalede, büyük veriden gerçekten büyük değer elde edilebileceği göstermektedir [61]. Bu örnekte, Google'ın Domuz Gribi Modeli toplumsal alanda en iyi uygulama olarak kabul edilmektedir. Burada, ABD'nin belirli bir bölgesinde yapılan Google aramasında kullanılan 42 arama kelimesi temel alınarak yapılan analizde o bölgedeki domuz gribinin yayılma modelinin belirlendiği görülmüştür [62]. Bunun farklı alanlara uygulandığı düşünülürse konunun önemi ve geleceğimize olan etkisi daha iyi anlaşılacaktır.

İnsan ve siber dünya ilişkisi üzerine yapılan siber antropolojik çalışmalar ile çok farklı sonuçların elde edilebileceği görülmektedir. Aslında sanal izlerimizin toplumsal olarak analiz edildiğinde, toplumsal çözümlerin geliştirilmesinde önemli ilerlemeler ve çözümler geliştirilebileceğini gösterse de oluşabilecek olumsuzluklarında farkında olunması gereklidir.

13.8.4. Kuantum Biyometrisi

Gerçek dünyada ve siber uzayda bireyleri birbirlerinden ayırt edebilmek adına kullanılabilecek karakteristik özelliklerin keşfi için birçok farklı disiplin eş zamanlı olarak çalışmaktadır. Bu disiplinlerden biri olan kuantum fiziği, sezgisel özelliklerinden gelen potansiyeli faydalı teknolojiye dönüştürecek yöntemler sayesinde, bireyi ayırt edebilmek için şimdiye kadar kullanılan karakteristik özelliklere alternatif bir özellik kullanarak çok daha yüksek güvenlik seviyesi imkânı sunabilen bir yaklaşım sunmuştur: kuantum biyometrisi. Bu yöntem güvenli bir biyometrik tanımlama sistemi sunabilmek için; göz retinasında yer alan çubuk hücrelerindeki rodopsin moleküllerine ile etkileşime girecek özel bir ışık algılama ekipmanı kullanarak insan gözünün tek bir fotonu algılamasını ölçmektedir. Kuantum biyometrisinde; tek bir fotonun algılanmasına etki eden kornea, ön oda, göz bebeği, mercek gibi noktalarda yer alan kan damarları, sinir hücreleri, ışığa duyarlı hücreler vb. üzerinden fotonun geçmesi için harcanan sürenin bireyi tanımlamak için kullanılabileceği ifade

edilmiştir. Bu süre alfa olarak adlandırılmıştır. Bir kişinin alfa haritası çıkartılarak, bu bilginin kişiyi tanımlamak için kullanılabileceği düşünülmektedir [57].

Biyometrik sistemlerin en büyük zafiyeti, saldırganlar tarafından çeşitli saldırılar ile sisteme sızılarak bireye ait karakteristik özelliklerin çalınması durumudur. Konu kuantum olduğunda bilinmesi gereken en temel özellik sistemlere yapılan her türlü erişimin sistemde iz bırakacağı ve sistemin çalışmasına etki edeceğidir. Bu kapsamda biyometrik sistemlere yapılan saldırılar düşünüldüğünde, kuantum fiziğinin yasalarının bu kadar kullanışlı olduğu farklı bir uygulama ortamı akla gelmemektedir. Çünkü kuantum fiziği kullanılarak önerilen bu yaklaşım sayesinde, bir dinleyicinin sisteme ne kadar müdahil olduğu konusunda iyi tanımlanmış sınırlar koyulmuş olunur [57,58].

Elektronik ortamlardaki tehditler değerlendirildiğinde, kuantum biyometrinin gelecekte pek çok sıkıntının giderilmesine katkı sağlayacak trendlerden birisi olduğu ortadadır. Bu konuya önem verilmeli ve bu konuda uzmanlaşacak laboratuvarlar kurulmalıdır.

13.9. Değerlendirmeler

Bir biyometrik sistemin temel bileşenleri, çalışma mekanizması, geliştirme ve uygulanma sürecinde oluşabilecek riskler ve problemler genel hatları ile açıklanmış, bu sistemleri geliştirecek, araştıracak ve güvenlik politikaları önerecek kitlelere yönelik olarak öneriler yapılmıştır. Biyometrik sistemler, bu sistemler için tehdit unsurları ve sistem güvenliği üzerine genel bir değerlendirme yapılmak istenirse:

- Biyometrik özelliklerin kullanıldığı tüm doğrulama/tanıma/kanıtlama sistemleri bireyleri birbirlerinden ayırt edebilmek için, sürecin doğası gereği olasılıksal bir çaba göstermektedir. İçerdiği teknoloji ve sistem tasarlandığı gibi davranıyor olsa bile, sistem tarafından ölçülen özelliklerin farklılığı ve kararlılığı hakkında zayıf veya eksik bir anlayışın var olabilme ihtimali sebebiyle tüm biyometrik sistemlerde kaçınılmaz bir belirsizlik ve hata riski olduğu unutulmadan önlem alınmalıdır.

- Biyometrik sistemler diğer doğrulama teknolojileri içinde iyi seviyede bir güvenlik hizmeti sunmakta olsa da yüzde yüz başarıyı garantileyemez. Dolayısıyla, her sistemde olduğu gibi biyometrik sistemlerde de %100 güvenlikten bahsetmenin mümkün olamayacağı göz ardı edilmemeli ve gereken önlemler alınmalıdır.
- Öte yandan, diğer yöntemlerle biyometrik yaklaşımların birleştirilmesi, doğrulama/onaylama işlemi gerektiren tüm uygulama alanları için güvenliği artırıcı özelliğe sahiptir. Bu husus unutulmamalı ve bu özelliklerden faydalanılmalıdır.
- Güvenlik hizmetinin uygulanacağı alan ve bu alan için biyometrik sistem kullanımının gerekliliği iyi değerlendirilmelidir. Biyometrik sistemlerin bilgi sistemlerini veya diğer kaynakları korumak adına bir güvenlik mekanizması olarak kullanılması için, uygulama alanın iyi kritik edilmesi gerekmektedir. Biyometrik sistem tarafından çözülecek problem, uygulama alanının modellenilebilirliği, uygulanabilirliği, korunabilirliği veya yönetilebilirliği iyi değerlendirilmediği takdirde, güvenliği arttırmak için kullanılan biyometrik verinin ele geçirilmesiyle güvenlik zafiyeti oluşturacağı göz ardı edilmemelidir.
- Biyometrik sistemlere yönelik tehditler, uygulama alanı ve çalışma sahasına göre değişkenlik gösterebileceğinden, geliştirilen bir sistemin güvenilirliği değerlendirilirken, sistem tasarımı ve performans testlerinin uygulama alanı ve çalışma sahasına uygun bir şekilde yapılması gerektiği unutulmamalıdır.
- Geliştirilen her biyometrik sistem bileşeni, yeni gelişmelere adapte olabilmek adına standartlara uygun bir şekilde tasarlanmalıdır. Sistem bileşenleri yeniliklere açık bir şekilde tasarlanmadığı takdirde, teknoloji değişikliklere ve dönüşümlere adapte olamamadan kaynaklı veri kalitesi kaybı, yanlış eşleştirme sonuçları vb. sonuçlar ortaya çıkabilmektedir. Sistemin bileşenleri ve bu bileşenleri geliştirirken kullanılan yaşam döngüsü yeni yaklaşımları destekleyebilecek şekilde tasarlanmalıdır.
- Biyometrik sistemler; bireylerin ayırt edilmesi hususunda önemli kolaylıklar sunmakla birlikte ömür boyu değişmezlik özelliği

sebebiyle, bir yandan sunduğu konfordan bahsedilirken bir yandan da biyometrik verilerin ihlalinden bireyin olumsuz etkileneceği unutulmamalıdır. Buna göre önlem alınmalı ve sistemler kurulmalı ve yönetilmelidir.

- Hem kamu hem de özel sektörün biyometrik veri toplamasını ve kullanımını düzenleyen, biyometrik verilerinin kim tarafından ve hangi amaçla toplanıldığı üzerine tüketicilerin bilgilendirilmesini zorunlu kılan yaptırımlar, 6698 sayılı Kişisel Verileri Koruma Kanunu ile işleme konulmuştur. Dolayısıyla, yapılan izinsiz işlemlerin veya ihlallerin hukuki sonuçlarının olacağı ortadadır. Bunun bir koruma sağlaması beklenilse de kullanıcılar kişisel verilerini koruma için üstün çaba göstermesi de gereklidir.
- Bu kitap bölümünde ele alınan; toplumsal biyometri, davranışsal biyometri, siber antropoloji, sosyometrik biyometri ve kuantum biyometri gibi konulara ağırlık verilmeli, bu konularda da kapsamlı çalışmalar yapılmalıdır.

Kaynaklar

1. Jain, A. K., Ross, A., Pankanti, S. (2006). Biometrics: a tool for information security. IEEE transactions on information forensics and security, 1(2), 125-143.
2. Wayman, J. L., Jain, A. K., Maltoni, D., Maio, D. (2005). Biometric systems: Technology, design and performance evaluation. Springer Science & Business Media.
3. Shrestha, A. (2014). Multi-biometric systems, Bachelor's Thesis, Turku University Of Applied Sciences, Finland, 9-14.
4. Cassandra M. Carrillo, C. (2003). Continuous Biometric Authentication For Authorized Aircraft Personnel: A Proposed Design, Master Thesis, Naval Postgraduate School Monterey, California, 14–20.
5. Yalçın, N., Gürbüz, F. (2015). Biyometrik Güvenlik Sistemlerinin İncelenmesi. Düzce Üniversitesi Bilim ve Teknoloji Dergisi, 3(2).
6. Unar, J. A., Seng, W. C., Abbasi, A. (2014). A review of Biometric Technology along with trends and prospect. Pattern Recognition, 47(8), 2673–2688.
7. Maltoni, D., Maio, D., Jain, A. K., Prabhakar, S. (2009). Handbook of fingerprint recognition. Springer Science & Business Media.

8. Jain, A. K., Ross, A., Prabhakar, S. (2004). An introduction to biometric recognition. IEEE Transactions on circuits and systems for video technology, 14(1).

9. Jain, R., Kant, C. (2015). Attacks on biometric systems: an overview. International Journal of Advances in Scientific Research, 1(7), 283-288.

10. Mansfield, A. (2006). Information technology--Biometric performance testing and reporting--Part 1: Principles and framework. ISO/IEC, 19795-1.

11. Understanding Biometrics (2018). URL: https://www.biometricsinstitute.org/wp-content/uploads/Understanding-Biometrics-Guide-WIP-Sept-2018.pdf

12. Mansfield, A. J., Wayman, J. L. (2002). Best practices in testing and reporting performance of biometric devices.

13. Clarke, R. (1994). Human identification in information systems: Management challenges and public policy issues. Information Technology & People, 7(4), 6-37.

14. Yadav, A. K., Grewal, K. S. (2014). A Comparative Study of Different Biometric Technologies, International Journal of Computer Science & Communication, 5(1).

15. El-Abed, M., Christophe, C., Christophe. R. (2012). Evaluation of Biometric Systems. New Trends and Developments in Biometrics, 149-169.

16. Biometric Identification: Are We Ethically Ready? Renaud, K., Hoskins, A., Von Solms, R. (2015). Biometric identification: Are we ethically ready?, IEEE Information Security for South Africa (ISSA), 1-8.

17. Cukic, B., Bartlow, N. (2005). Biomentric system threats and countermeasures: A risk-based approach. In Biometric Consortium Conference.

18. Singh, Y. N., Singh, S. K. (2013). A taxonomy of biometric system vulnerabilities and defences. International journal of biometrics, 5(2), 137-159.

19. Prabhakar, S., Pankanti, S., & Jain, A. K. (2003). Biometric recognition: Security and privacy concerns. IEEE security & privacy, (2), 33-42.

20. Kumar, M., Vaisla, K. S. To study of various security attacks against Biometric template in a generic Biometric Recognition System. In Proceedings of the Second International Conference on Research in Intelligent and Computing in Engineering (RICE), 235-240.

21. Speicher, D. (2006). Vulnerability analysis of biometric systems using attack trees. West Virginia University Libraries.

22. BEAT (Biometrics Evaluation and Testing). URL: https://www.beat-eu.org/project/deliver ables-public/d4.6-description-of-metrics-for-the-evaluation-of-vulnerabilities-to-indirect-a ttacks.

23. Galbally, J., Cappelli, R., Lumini, A., Gonzalez-de-Rivera, G., Maltoni, D., Fierrez, J., Ortega-Garcia, J., Maio, D. (2010). An evaluation of direct attacks using fake fingers generated from ISO templates. Pattern Recognition Letters, 31(8), 725-732.

24. Martinez-Diaz, M., Fierrez, J., Galbally, J., Ortega-Garcia, J. (2011). An evaluation of indirect attacks and countermeasures in fingerprint verification systems. Pattern Recognition Letters, 32(12), 1643-1651.

25. Ghouzali, S., Lafkih, M., Abdul, W., Mikram, M., El Haziti, M., Aboutajdine, D. (2016). Trace attack against biometric mobile applications. Mobile Information Systems.

26. Fierrez, J. (2015). Indirect Attacks on Biometric Systems. URL: http:// gigantes.ii.uam.es/ fierrez/files/2015_NISLab_Attacks_Fierrez.pdf.

27. Du, Y. E. (2013). Biometrics: from fiction to practice. CRC Press.

28. Adler, A., & Schuckers, S. A. (2015). Biometric vulnerabilities, overview. Encyclopedia of Biometrics, 271-279.

29. National Research Council, & Whither Biometrics Committee. (2010). Biometric recognition: challenges and opportunities. National Academies Press.

30. Ratha, N. K., Connell, J. H., & Bolle, R. M. (2001). Enhancing security and privacy in biometrics-based authentication systems. IBM systems Journal, 40(3), 614-634.

31. Nabil, D. H., Karima, B., Mouloud, K., Ahmed, B. (2012). Threats models on biometric systems: A comparative study. Fourth International Conference on Computational Aspects of Social Networks, 186-191.

32. J.L. Wayman, J. L. (2009). Technical Testing and Evaluation of Biometric Devices. Biometrics, Springer, 345-368.

33. Cukic, B., Bartlow, N. (2005). The vulnerabilities of biometric systems-An integrated look and old and new ideas. West Virginia University, Tech. Rep.

34. Nagar Jain, A. K., Nandakumar, K., & Nagar, A. (2008). Biometric template security. EURASIP Journal on advances in signal processing, 2008, 113.

35. Canbek, G., Sagıroğlu, Ş. (2006). Bilgi, bilgi güvenliği ve süreçleri üzerine bir inceleme. Politeknik Dergisi, 9(3), 165-174.

36. (2004). Cybersecurity for Critical Infrastructure Protection. URL: https://www.gao.gov/ne w.items/d04321.pdf

37. Singla, S. K., & Kumar, S. (2013). A review of data acquisition and difficulties in sensor module of biometric systems. Songklanakarin Journal of Science & Technology, 35(5).

38. Roberts, C. (2007). Biometric attack vectors and defences. Computers & Security, 26(1), 14-25.

39. Galbally, J. (2009). Vulnerabilities and attack protection in security systems based on biometric recognition.

40. Alaswad, A. O., Montaser, A. H., & Mohamad, F. E. (2014). Vulnerabilities of biometric authentication threats and countermeasures. International Journal of Information & Computation Technology, 4(10), 947-58.

41. Tilton, C. T. Planet Biometrics-Standards-Getting Started. URL: https://www.planetbiom etrics.com/creo_files/upload/article-files/getting_started_-_biometric_standards_-_v2_(se p2011).pdf.

42. Lingathoti, V. (2018). BehavioSec Fires Up Next-Gen Cybersecurity Solutions with Behavioral Biometrics. URL: https://blogs.cisco.com/innovation/behaviosec-fires-up-next-gen-cybersecurity-solutions-with-behavioral-biometrics

43. Behavioral Biometrics Improve Security and the Customer Experience. URL: https://www.vasco.com/images/Behavioral-Biometrics_tcm42-67183.pdf

44. Todd Rebner, T. (2019). Behavioral Biometrics Is The Future Of User Authentication Forbes Technology Council. URL: https://www.forbes.com/sites/forbestechcouncil/2019/05/13/behavioral-biometrics-is-the-future-of-user-authentication/#48f83ccb40d7.

45. (2018). Behavioral Biometrics: A Primer on the Future of Cybersecurity, URL: https://www.biocatch.com/blog/behavioral-biometrics-primer-future-cybersecurity.

46. Marti, J., Zenou, Y. (2009). Social Networks. URL: http://www.ifn.se/wfiles/wp/wp816.pdf

47. Elena Pupazan, E. (2011). Social Networking Analytics. URL: https://www.math.vu .nl/~sbhulai/papers/paper-pupazan.pdf.

48. Uher, J. (2013). Personality psychology: Lexical approaches, assessment methods, and trait concepts reveal only half of the story-Why it is time for a paradigm shift. Integrative Psychological and Behavioral Science, 47(1), 1-55.

49. Francis Galton and Fingerprints. URL: http://galton.org/fingerprinter.html

50. Goldberg, L. R. (1993). The structure of phenotypic personality traits. American psychologist, 48(1), 26.

51. Olshannikova, E., Olsson, T., Huhtamäki, J., & Kärkkäinen, H. (2017). Conceptualizing big social data. Journal of Big Data, 4(1), 3.

52. Choudhary, V, Kapoor, A.K. (2013). Role of Biometrics in Anthropological Settings. International Research Journal of Social Sciences, 2(8), 55-57.

53. Bearls, R. L., Hoijer, H., Erginer, G. (2018). Antropolojinin Konusu ve Alanı. Ankara Üniversitesi Dil ve Tarih-Coğrafya Fakültesi Dergisi, 35(2).

54. Malkoç, N. Ş. (2012). "Oturduğu Yerden Antropoloji": Doryo'larda Siberetnografiyi Düşünmek. Folklor/Edebiyat, 18(72), 153-162.

55. Özkaynar, K., Altunışık, R., Yolcu, T. (2019). Siyasal Pazarlama İçin Etnografi Ve Netnografi Temelli Araştırmaların Kullanımına Yönelik Bir Araştırma: Twıtter Üzerinden Yapılan Anketler İle 2017 Referandumu Resmi Sonuçlarının Karşılaştırılması. Journal of World of Turks/Zeitschrift für die Welt der Türken, 11(2).

56. We are Social (WAS). (2017). Digital in 2017 Global Overview. URL: https://wearesocial.com/uk/special-reports/digital-in-2017-global-overview.

57. Loulakis, M., Blatsios, G., Vrettou, C. S., Kominis, I. K. (2017). Quantum Biometrics with Retinal Photon Counting. Physical Review Applied, 8(4), 044012.

58. Mathew Dirjish, M. (2017). Quantum Biometrics Technique Holds Promise Of Personal Security. URL: https://www.fierceelectronics.com/embedded/quantum-biometrics-technique-holds-promise-personal-security.

59. Kosinski, M., Stillwell, D., Graepel, T. (2013). Private traits and attributes are predictable from digital records of human behavior. Proceedings of the National Academy of Sciences, 110(15), 5802-5805.

60. Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. URL: https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-face book-influence-us-election.

61. Ginsberg J, Mohebbi M.H., Patel R.S., Brammer L, Smolinski M.S., Brilliant, L. (2009) Detecting influenza epidemics using search engine query data. Nature 457: 1012–1014.

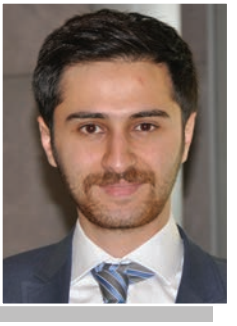
62. (2009) Google Flu Trends. URL: https://www.google.org/flutrends/about/

Yazarların Özgeçmişleri

Onur AKTAŞ

BTK bünyesinde siber güvenlik alanında çalışmalar yapan Onur Aktaş, çeşitli projelerde yöneticilik yapmaktadır.

Siber güvenlikte büyük veri, olay müdahale, güvenli yazılım geliştirme, zafiyet tespiti ve sömürü geliştirme konularında uzmanlığı vardır. Gazi Üniversitesi Bilgi Güvenliği Mühendisliği ile Hacettepe Üniversitesi Bilişim Hukuku bölümlerinde yüksek lisans yapmıştır. Siber Güvenlik - Hacking - Atölyesi adlı bir adet kitabı bulunan Aktaş, Hacettepe Üniversitesi'nde Mühendislik doktorasına devam etmektedir.



A. Oğuzhan ALKAN

1992 Kayseri doğumludur. Bilkent Üniversitesi Bilgisayar Mühendisliği'nden 2016 yılında mezun olmuştur. Başkent Üniversitesi'nde Teknoloji ve Bilgi Yönetimi Bölümünde yüksek lisans yapmaktadır.

Bilgi Güvenliği Derneği Gençlik Platformu Başkanı ve CyberMag Dergisi'nin genel yayın yönetmenliği görevini sürdürmektedir.

Siber güvenlik alanında teknik danışmanlık hizmetleri ve eğitimleri veren Ulusal Siber Güvenlik Akademisi şirketinin yönetim kurulu başkanıdır. Kamu kurum ve kuruluşlarına ve özel şirketlere siber güvenlik alanında danışmanlık ve eğitim hizmetleri vermektedir. Bilgi Güvenliği Derneği'nde Denetim Kurulu Üyesi olarak da görev almaktadır.

Bilgehan ARSLAN

- Gazi Üniversitesi Mühendislik Fakültesi Bilgisayar Mühendisliği Bölümü Öğretim Görevlisi, Ankara.

2015 yılından beri Gazi Üniversitesi'nde doktora çalışmalarına devam etmektedir. 2013 yılında Gazi Üniversitesi Fen Bilimleri Enstitüsü'nde Araştırma Görevlisi olarak çalışmıştır. Halen, Gazi Üniversitesi Bilgisayar Mühendisliği bölümünde Öğretim Görevlisi olarak çalışmaktadır. Biyometri, Görüntü İşleme, Makine Öğrenmesi, Derin Öğrenme ve Bilgi Güvenliği gibi konular üzerinde akademik çalışmalarını sürdürmektedir.

Dr. Öğr. Üyesi Atila BOSTAN

- Türk Hava Kurumu Üniversitesi, Bilgisayar Mühendisliği Bölümü, Öğretim Üyesi, Ankara

Bilgisayar güvenliği, sayısal ağlar ve görüntü işleme konularında araştırmalar yapmakta olan Atila Bostan, Türk Silahlı Kuvvetlerinin çeşitli kademelerinde yirmı yıl otomatik bilgi işlem subaylığı yapmıştır. Emekliliğini müteakiben, 2008-2019 yılları arasında Atılım Üniversitesi, Bilgisayar Mühensilği Bölümünde öğretim üyesi olarak görev yapmıştır. Halen THK Üniversitesi, Bilgisayar Mühendisliği bölümünde öğretim üyesi olarak görev yapmaktadır. Dr. Bostan'ın "Experiments on Computer Networks" isminde bir yayınlanmış kitabı bulunmaktadır. Ayrıca, gerçek hava boşluğu ile ağlar arasında bilgi aktarma ve temassız kart okuma kontrolü konularında iki adet patent sahibi olan Bostan'ın 15 uluslararası dergi makalesi ve 40 uluslararası konferans bildirisi bulunmaktadır.

TSK ve NATO bilgi sisemleri ve harekat birlikleri bilgisayar ağ desteği konularında birçok proje yöneten Dr. Bostan, NATO ve TSK Üstün Hizmet madalyalarının sahibidir. Ayrıca, Atılım Üniversitesi Bilgisayar Mühendisliği Bölünmünde bilgisayar güvenliği konusunda yürüttüğü projelerle IBM firması tarafından 2009 ve 2011 yıllarında iki kez "IBM Shared University Research Award" ödülünü kazanmıştır. Dr. Atila Bostan, bilgisayar güvenliği, bilgisayar ağları ve görüntü işleme alanlarında uluslarası dergilerde editörlük, makale hakemliği, konferanslarda teknik komite ve bildiri hakemliği yapmaktadır.

Dr. Öğr. Üyesi Eyüp Burak CEYHAN

- Bartın Üniversitesi Mühendislik Mimarlık ve Tasarım Fakültesi Bilgisayar Mühendisliği Bölüm Başkanı.

Biyometrik Sistemler, Bilgi ve Bilgisayar Güvenliği, Kurumsal Bilgi Güvenliği, Adli Bilişim, Sosyal Ağ Güvenliği, Büyük Veri, Kripto Para, Yapay Zekâ gibi alanlarda çalışmalar yapmaktadır.

Gazi Üniversitesi Bilgisayar Mühendisliği Bölümü'nde danışmanı Prof. Dr. Şeref Sağıroğlu ile tamamladığı yüksek lisans ve doktora tezlerinden ürettiği zeki sistemler ile Türkiye, Amerika ve Avrupa'ya yaptığı patent başvuruları sonucunda bu sistemlerin patentini alarak güvenlik alanında önemli olan sistemleri Türkiye'ye kazandırmıştır.

Dr. Ceyhan, lisans, yüksek lisans ve doktora derecelerini Bilgisayar Mühendisliği alanlarında almıştır. 2011-2016 yılları arasında Gazi Üniversitesi Bilgisayar Mühendisliği Bölümü'nde araştırma görevlisi olarak görev yapmış, 2016 yılından itibaren halen çalışmakta olduğu Bartın Üniversitesi Bilgisayar Mühendisliği Bölümü'nde bölüm başkanı olarak görev yapmaktadır. Bartın Üniversitesi'nde Akıllı Lojistik Sistemler Laboratuvarı ve Siber Güvenlik ve Biyometri Laboratuvarlarında yönetici olarak çalışmaktadır. Yine Bartın Üniversitesi Proje Teknoloji Ofisi'nde Patent Koordinatörü olarak görev yapmaktadır. Bartın Kamu-Üniversite-Sanayi İşbirliği (KÜSİ) Temsilcisi olarak Sanayi ve Teknoloji Bakanlığı'nda görev almıştır.

Doktora eğitiminden sonra 12 ay boyunca Amerika'da, TÜBİTAK 2219 Yurt Dışı Doktora Sonrası Araştırma Burs Programı desteği ile University of Miami'de biyometrik güvenlik sistemleri alanında çalışmalarına devam etmiştir.

Çoğu biyometrik sistemler, bilgi güvenliği, yapay zekâ, veri madenciliği konularında olmak üzere 30'un üzerinde ulusal ve uluslararası indeksli dergilerde yayınlanan makaleleri ve uluslararası konferanslarda sunduğu bildirileri bulunmaktadır. Ayrıca TÜBİTAK, Ankara Kalkınma Ajansı, Gazi Üniversitesi ve Bartın Üniversitesi destekli ulusal projelerde de proje yürütücüsü ve araştırmacı olarak çok sayıda projede yer almıştır. Uluslararası düzenlenen 18 konferansta düzenleme kurulu üyesi olarak görev almıştır. 30'un üzerinde uluslararası konferansta bilim kurulu üyeliği ve çeşitli SCI dergilerde hakemlik de yapmıştır.

DERGİPARK'a kayıtlı 1 dergide editörlük, 2 dergide Editör Kurulu Üyeliği ve çok sayıda dergide de hakemlik yapmaktadır.

Yıldız Teknik Üniversitesi'nde IEEE destekli düzenlenen İş Fikri Yarışması'na sunduğu proje 1.lik ödülü almış ve 7.000TL para ödülü kazanmıştır. Ayrıca Gazi Üniversitesi Bilim Şenliği Proje Yarışması'nda 1.lik, 2. İş Fikri Yarışması'nda mansiyon, 3. Endüstri ve Teknoloji Tezleri Yarışması'nda Teşvik Ödülleri elde etmiş ve sırasıyla 10.000TL, 5.000TL ve 1.000TL para ödülleri kazanmıştır.

Çeşitli kamu kurumları ve firmalara biyometrik sistemler, siber güvenlik, mobil güvenlik, bilgi güvenliği eğitimleri ve danışmanlık hizmeti de vermektedir.

Dr. Öğr. Üyesi İsmail Fatih CEYHAN

- Bartın Üniversitesi İktisadi ve İdari Bilimler Fakültesi İşletme Bölümü, ismailc@bartin.edu.tr

Dr. Öğr. Üyesi İsmail Fatih Ceyhan, 1996 yılında İstanbul Üniversitesi Siyasal Bilgiler Fakültesi İşletme Bölümünü kazanmış ve 2001 yılında mezun olmuştur. 2002-2005 yılları arasında Kırıkkale Üniversitesi İktisadi ve İdari Bilimler Fakültesi'nde araştırma görevliliği yapmıştır. 2006-2008 yılları arasında İstanbul'da özel bir bağımsız denetim firmasında denetçi yardımcısı olarak çalışmış ve bu dönemde serbest muhasebeci ve mali müşavir stajını tamamlayıp yeterlilik sınavlarından başarılı olarak mali müşavir olmaya hak kazanmıştır. 2009 yılında Bartın Üniversitesi İktisadi ve İdari Bilimler Fakültesi İşletme Bölümü'nde araştırma görevliliğine geri dönmüştür. 2010 yılında Kırıkkale Üniversitesi Sosyal Bilimler Enstitüsü İşletme Ana Bilim Dalı'nda yüksek lisansını "İç Denetim ve Kurumsallaşma" başlıklı tezi ile tamamlamış ve aynı yıl Sakarya Üniversitesi Sosyal Bilimler Enstitüsü İşletme Ana Bilim Dalı, Muhasebe ve Finansman Bilim Dalı'nda doktora eğitimine başlamıştır. 2014 yılında "Denetim Kalitesini Artırıcı Bir Yöntem Olarak Veri Madenciliği" başlıklı doktora tezi ile doktorasını tamamlamıştır. 2015 yılında Bartın Üniversitesi İktisadi ve İdari Bilimler Fakültesi İşletme Bölümü Muhasebe ve Finansman Ana Bilim Dalı'na öğretim üyesi olarak atanmıştır ve halen burada göreve devam etmektedir. Muhasebe ve finans alanında çeşitli akademik yayınları bulunmaktadır.

Dr. Öğr. Üyesi Onur ÇAKIRGÖZ

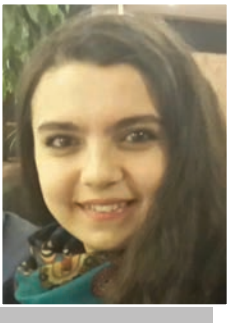
- Bartın Üniversitesi Mühendislik Mimarlık ve Tasarım Fakültesi Bilgisayar Mühendisliği Bölümü.

24/11/1985 tarihinde Manisa'da doğmuştur. Lisans eğitimini Selçuk Üniversitesi Bilgisayar Mühendisliği Bölümü'nde aldıktan sonra, yüksek lisans ve doktora eğitimlerini Dokuz Eylül Üniversitesi Bilgisayar Mühendisliği Bölümü'nde tamamlamıştır ve bu süreçte aynı üniversitede araştırma görevlisi olarak görev yapmıştır. Yüksek Lisansta şifrelerin güvenli ve gizli bir şekilde kullanılması üzerine çalışmıştır. Doktorada ise kişisel genetik verilerin klinik kullanımda organizasyonu ve depolanması üzerine çalışmalar gerçekleştirmiştir. Yazarın ilgi alanları bilgisayar güvenliği, şifreleme, kimlik doğrulama, blok-zincir, biyoinformatik ve yapay zekâdır. 2019-2020 Eğitim Öğretim yılı itibariyle Bartın Üniversitesi'nde Dr. Öğr. Üyesi olarak görev yapmaktadır. Yazar evli ve bir çocuk babasıdır.

Dr. Öğr. Üyesi Mehmet DEMİRCİ

Gazi Üniversitesi Mühendislik Fakültesi Bilgisayar Mühendisliği Bölümü, Ankara.

Bilgisayar bilimi alanında lisans derecesini Purdue Üniversitesinden, yüksek lisans ve doktora derecelerini ise Georgia Teknoloji Enstitüsünden almıştır. Gazi Üniversitesi Mühendislik Fakültesi Bilgisayar Mühendisliği Bölümünde öğretim üyesi ve bölüm başkan yardımcısı olarak görev yapmaktadır. Çalışma alanları arasında yazılım tanımlı ağlar (SDN), ağ fonksiyonlarını sanallaştırma (NFV), bilgi güvenliği ve 5G ağları bulunmaktadır. Yazılım tanımlı ağlar ve ağ güvenliği konularında 2015'ten bu yana lisansüstü dersler vermektedir. IEEE destekli ISNCC konferansında SDN ve NFV konulu oturum düzenlemektedir. Ayrıca ISCTurkey ve ISDFS konferanslarında düzenleme kurulu üyesi olarak görev yapmıştır.



Arş. Gör. Sedef DEMİRCİ

- Gazi Üniversitesi Mühendislik Fakültesi Bilgisayar Mühendisliği Bölümü, Ankara.

Gazi Üniversitesi Mühendislik Fakültesi Bilgisayar Mühendisliği bölümünde araştırma görevlisi olarak çalışmakta olan Sedef Demirci, 2014 yılından beri aynı bölümde doktora çalışmalarına devam etmektedir. Çalışma alanları arasında siber güvenlik yazılım tanımlı ağlar (SDN) ve ağ fonksiyonlarını sanallaştırma (NFV) bulunmaktadır. Ayrıca ISCTurkey, ISDFS ve UBMK konferanslarında düzenleme kurulu üyesi olarak görev yapmıştır.

Doç. Dr. Gülüstan DOĞAN

- University of North Carolina Wilmington'da öğretim üyesi olarak görev yapmaktadır. Aynı zamanda Yıldız Teknik Üniversitesi'nde öğretim üyesidir.

Araştırma alanları bilgisayar ağları, güven ve veri bilimidir. Lisans derecesini Orta Doğu Teknik Üniversitesi Bilgisayar Mühendisliği bölümünden aldı. Kaliforniya, Silikon Vadisinde NetApp ve Intel şirketlerinde yazılım mühendisi olarak çalıştı. Doktora derecesini City University of New York Üniversitesi'nden Bilgisayar Bilimleri alanında aldı. Birçok ulusal ve uluslararası konferansda bilim kurulu üyeliği yapmıştır ve birçok bilimsel dergide yayın kurulu üyesidir. Aynı zamanda kadınların bilgisayar muhendisliğine yönlendirilmesi konusunda çalışmaları vardır. Uluslararası Türk Kadın Bilgisayar Mühendisleri Topluluğunun kurucusudur.

Dr. Öğr. Üyesi Muharrem Tuncay GENÇOĞLU

- Fırat Üniversitesi Teknik Bilimler MYO Müdür Yardımcısı.

Elazığ doğumlu olan Gençoğlu, 1992 yılında Fırat üniversitesi Matematik bölümünde lisans eğitimini tamamlamış, 1993 yılında aynı bölüme araştırma görevlisi olarak atanmıştır. 1995 yılında Zaman Serileri Analizi üzerine yaptığı çalışmayla yüksek lisansını bitirmiştir. 1996-2010 yılları arasında özel sektörde çeşitli kademelerde yönetici olarak çalışmış bu arada İ.T.Ü. Matematik Mühendisliğinden ve Fırat Üniversitesi Uygulamalı Matematik Bilim dalı Doktora programından da mezun olmuştur. 2010-2015 yılları arası Tunceli Üniversitesi Bilgisayar Mühendisliğinde öğretim üyesi olarak çalışırken 2014 yılında Berlin Teknik Üniversitesi Dağıtık Yapay Zekâ Laboratuvarında kısa süreli olarak bulunmuştur.

2015 yılında Fırat Üniversitesi Teknik Bilimler MYO'na öğretim üyesi olarak atanan Gençoğlu, Bilgisayar teknolojileri bölümünde Kriptolojinin Temelleri, Bilgi Güvenliği ve Siber Güvenlik derslerini, Yazılım Mühendisliğinde Bilgisayar Sistemleri ve Güvenliği dersini, Milli Savunma Üniversitesi Kara Harp Okulu Savunma Yönetimi Bölümünde Siber Savaş ve Bilişim Sistemleri Güvenliği dersini ve Alparslan Savunma Bilimleri Enstitüsünde (OBİ) Ayrık Matematik dersini, Ahmet Yesevi Üniversitesi (TÜRTEP) Siber Güvenlik Ve Savunma Politikaları, Stratejileri ve Hukuku dersini vermektedir.

TEB Eğt. Hiz. Ltd. Şti. Yönetim Kurulu Başkanlığı, Aydınlar Ocağı Kurucu Başkanlığı, MÜSİAD Yönetim Kurulu Üyeliği, Elazığ Valiliği tarafından yürütülen birçok Sosyal ve Araştırma projelerinde yürütücü, Fırat Üniversitesi Bilgisayar Teknolojileri Bölüm Başkanlığı, Fırat Üniversitesi Siber Savunma Komisyonu Üyeliği, Fırat Üniversitesi Teknik Bilimler MYO Kalite Komisyonu Başkanlığı, Fırat Üniversitesi YÖS Yürütme Kurulu Üyeliği görevlerinde bulunmuştur.

ISO 27001 Bilgi Güvenliği Standardı Temel Eğitimi, Quality Management Systems, Auditor/Lead Auditor Course, IRCA-IPC, TSE, İç Kalite Tetkik Eğitimi, Kalite Yönetimi Temel Eğitimi, Proseslerin Yönetimi Etkileşimi ve İyileştirme Teknikleri, Müşteri Memnuniyeti, FMEA Liderlik, Toplam Kalite Yönetimi, Problem Çözme Teknikleri, Performans

Değerlendirmesi, Kuruluş İçi Kalite Tetkiki (2000) gibi birçok sertifikaya sahiptir.

Kriptografi, Kriptonaliz, Siber Güvenlik ve Diferansiyel Denklemler alanında çalışmalarını sürdüren ve yayınlanmış 3 kitap, 30'un üzerinde bildiri ve makalesi bulunan Gençoğlu, Yüksek Öğretim Kurulu Siber Güvenlik Çalışma Grubu, Bilgi Güvenliği Derneği, International Association for Cryptologic Research, American Association for Artificial Intelligent (AAAI), VECTOR Türk Dünyası Araştırmaları Uluslararası İlimler Akademisi, Türk İstatistik Deneği üyesidir.

Doç. Dr. Ali Hakan IŞIK

- Lisans ve lisansüstü çalışmalarını Gazi Üniversitesinde tamamlamıştır. Yüksek lisans çalışmasında bulanık mantık algoritmasının telekomünikasyon alanındaki uygulaması üzerine, doktorada ise yapay zekâ tabanlı mobil uygulamanın evde bakıma ihtiyaç duyan KOAH hastaları üzerine çalışmıştır. Halen Burdur Mehmet Akif Ersoy Üniversitesi, Mühendislik Mimarlık Fakültesi Bilgisayar Mühendisliği bölümünde öğretim üyesi olarak çalışmaktadır. Ondan fazla SCI kapsamında yayınlanan makalesi ve çeşitli ulusal ve uluslararası dergilerde akademik yayınları bulunmaktadır. Halen yapay zekâ, bilgi güvenliği, yazılım geliştirme ve optimizasyon alanlarında proje ve akademik çalışmalarına devam etmektedir.

Burak ÖZÇAKMAK

- Redeye Firması Teknik Genel Müdürü (CTO),

Gazi Üniversitesi Mühendislik Fakültesi Bilgisayar Mühendisliği Bölümünden bölüm ikinciliği derecesiyle mezun olan Burak Özçakmak, aynı fakültenin Endüstri Mühendisliği (Çift Anadal) bölümünü 2 yılda tamamlayarak mezun olmuş, Bilgi Güvenliği Mühendisliği Anabilim Dalından Yüksek Lisans derecesini almıştır.

İş hayatına TÜBİTAK'da araştırmacı olarak başlamış, kısa sürede sırasıyla uzman araştırmacı, proje yöneticisi olarak görev yapmıştır. TÜBİTAK'dan ayrılarak Devletin farklı kurumlarında teknik yöneticilik ve Şube müdürlüğü görevlerini üstlenen Özçakmak, 2019 yılında özel sektöre geçiş yapmıştır. Redeye firmasının Teknik Genel Müdürlük görevini üstlenen Özçakmak aynı zamanda İstanbul Aydın Üniversitesi Bilgisayar mühendisliği bölümünde Lisans öğrencilerine ders vermektedir. RF teknolojileri, GSM teknolojileri, Siber teknolojiler, IT audit, Drone üretimi (UAV), Yapay Zekâ, Big data & Veri madenciliği alanlarında birçok farklı proje yöneten Özçakmak, uzmanlık alanlarına ilişkin akademik çalışmalarda da yer almaktadır.

Prof. Dr. Şeref SAĞIROĞLU

- Gazi Üniversitesi Mühendislik Fakültesi Bilgisayar Mühendisliği Bölüm Başkanı, Ankara.

Doçentliğini Yazılım Mühendisliğinde alan Prof. Sağıroğlu, ülkemizde bilgi güvenliği, siber güvenlik ve büyük veri bilimi, analitiği, güvenliği ve mahremiyeti konularında çalışmalar yapmaktadır. Bilgi Güvenliği, Siber Güvenlik, Yapay Zekâ, Makine Öğrenme, Casus Yazılımlar ve Korunma Yöntemleri, Büyük Veri, Etkin Bilişim Teknolojileri Kullanımı, Ulusal Atıf İndeksi gibi konular ile uluslarası konferans bildiri kitabı editörlükleri olmak üzere 20'nin üzerinde yayınlanmış kitabı bulunmaktadır. Bu kitaplardan sonuncusu "Büyük Veri Analitiği, Güvenliği ve Mahremiyeti" olup ülkemizde bu alanda yayımlanan ilk akademik kitap olup, açık kaynak olarak okuyuculara sunulmaktadır. Biri amerikan patenti olmak üzere 5 patenti, değerlendirme sürecinde olan 7 patenti, 100'ün üzerinde ulusal ve uluslararası indeksli dergilerde yayınlanmış makalesi ile 300'e yakın ulusal ve uluslararası

yayımlanmış bildirisi ve 4.000'e yakın atıfı bulunmaktadır. H-indeksi ise 35'dir.

Uluslararası Bilgi Güvenliği Mühendisliği Dergisi (www.dergipark.gov.tr/ubgmd) ile International Journal of Information Security Science (www.ijiss.org) dergilerinin baş editörlük görevini yürütmektedir. Ayrıca aylık yayımlanan CyberMag Dergisinin de editörüdür.

Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı (www.iscturkey.org), IEEE Uluslararası Bilgisayar Bilimleri ve Mühendisliği Konferansı (www. ubmk.org), IEEE Uluslararası Makine Öğrenmesi ve Uygulamaları Konferansı Büyük Veri ve Siber Güvenlik Oturumu (www.icmla-conferences.org/ icmla2017), Büyük Veri Analitiği, Güvenliği ve Mahremiyeti Ulusal Kamu Çalıştayı (bigdatacenter.gazi.edu.tr), Ulusal Siber Terör Konferansı (www.siberteror.org), Açık Veri Türkiye Konferansı (www.acikveriturkiye.org), Siber Güvenlik ve Savunma Çalıştayı (www.iscturkey.org) gibi konferansların başkanlığını veya eşbaşkanlığını yürütmektedir.

Bilgi Güvenliği Derneği (BGD), Türk Bilim Araştırma Vakfı (TÜBAV), Geleceği Önemseyenler Derneği (GÖNDER) Kurucu Üyesidir. İki dönem, BGD Yönetim Kurulu Başkanlığı ve TÜBAV Genel Başkanlığı Gazi Üniversitesi Fen Bilimleri Enstitüsü Müdürlüğü gibi görevleri yürütmüştür. Uluslararası IEEE, ISACA ve ACM üyeliğide bulunan Sağıroğlu, IEEE Biyometrik Görev Gücü üyeliği, IPvb Forum Türkiye Başkanlığı görevlerini de yürütmektedir. BTK, Havelsan ve Kişisel Verileri Korumu Kurumuna danışmanlık yapmıştır.

Gönüllü olarak pek çok sosyal projeyi de yürütmüş olan Sağıroğlu, TÜBİTAK, Avrupa Birliği, Gazi Teknopark, Cumhurbaşkanlığı dijital Ofis yapay Zekâ Birimi, BAP gibi Bilimsel Araştırma Projelerinde görev almıştır.

Pek çok alanda ödülü de bulunan Sağıroğlu, İnternetin gelişimine sağladığı katkılardan dolayı IPvb 2019 Hall of Fame ödülü almıştır.

Ulusal ve uluslararası konferanslarda, Bilgi Güvenliği, Büyük Veri, Siber Güvenlik ve Savunma, Yapay Zekâ, Akıllı Şebekeler, 5 G Biyometrik Uygulamalar, İnovasyon Kültürü Oluşturma gibi konularda davetli konuşmacı olarak seminer ve konferanslar vermektedir.

Halen; Gazi Üniversitesi Bilgisayar Mühendisliği Bölüm Başkanı , FutureTech Genel Müdürü, BIDISEC Merkez Laboratuvarı Sorumlusu, Yüksek Öğretim Kurulu Siber Güvenlik Çalışma Grubu Üyeliği, Bilim Sanayi ve Teknoloji Bakanlığı Yazılım Sektörü Çalışma Grubu Üyeliği, Bilgi Güvenliği Derneği Yönetim Kurulu Üyeliği ve II. Başkanı gibi görevleri yürütmektedir.

Dr. Öğr. Üyesi A. Nurdan SARAN

Lisans eğitimini Ankara Üniversitesi Fen Fakültesi Matematik bölümünde tamamlamıştır. Çankaya Üniversitesi Bilgisayar Mühendisliği bölümünde görüntü işleme konusunda yüksek lisans yapmıştır. Doktora eğitimini Orta Doğu Teknik Üniversitesinde Uygulamalı Matematik Enstitüsünde Kriptografi Ana Bilim dalında tamamlamıştır. 2011 yılından beri Çankaya Üniversitesi Bilgisayar Mühendisliği bölümünde doktoralı öğretim üyesi olarak görev yapmaktadır. Başlıca ilgili alanları Bilgi Güvenliği ve Kriptografi olmakla birlikte Hesaplamalı Bilimler ve Görüntü İşleme üzerine çalışmaları vardır.

Doç. Dr. Gökhan ŞENGÜL

- Atılım Üniversitesi Mühendislik Fakültesi Bilgisayar Mühendisliği Bölümü, Ankara.

Ankara-Nallıhan doğumlu olan Şengül; görüntü ve sinyal işleme, örüntü tanıma, makine öğrenmesi, biyomedikal mühendisliği, bilgi güvenliği ve siber güvenlik konularında çalışmalar yapmaktadır. Şengül'ün 3 adet patenti, farklı ulusal ve uluslararası indeksli dergilerde yayınlanmış çok sayıda makalesi ve ulusal ve uluslararası yayımlanmış bildirileri bulunmaktadır.

Birçok TÜBİTAK ve BAP projelerinde görev almış olan Şengül, halen Atılım Üniversitesi Bilgisayar Mühendisliği bölümünde öğretim üyesi ve bölüm başkanı olarak görev yapmaktadır.

Seda YILMAZ

2009 yılında Bilgisayar Mühendisi unvanı ile mezun olmuştur. Çeşitli yazılım firmalarında yazılım mühendisi ve proje yöneticisi görevlerini almasının ardından kamuda bilgisayar mühendisi olarak göreve başlamıştır. 2015 yılında Gazi Üniversitesi Bilişim Enstitüsü Bilgisayar Bilimleri bölümünde yüksek lisansını tamamlamıştır.

Siber güvenlik, güvenli yazılım geliştirme, yazılım kalite standartları ve yazılım kalite süreçleri üzerinde çeşitli ulusal mecralarda bildiri ve yayınları bulunmakta olup halen bu kapsamda akademik çalışmalarını sürdürmektedir. İngilizce ve İspanyolca bilmektedir.

Özgür YÜREKTEN

- TÜBİTAK-BİLGEM Siber Güvenlik Enstitüsü Birim Yöneticisi & Başuzman Araştırmacı.

2000 yılında TÜBİTAK-UEKAE bünyesinde yarı zamanlı olarak çalışmaya başlayan Yürekten, 2001 yılında Başkent Üniversitesi bilgisayar mühendisliği bölümünü burslu olarak tamamladı. 2001-2015 tarihleri arasında tam zamanlı araştırmacı olarak çeşitli askeri ve kamu projelerinde yazılım geliştirme mühendisi ve proje yöneticisi olarak görev yaptı. 2015-2016 yılları arasında TÜBİTAK-BİLGEM Yazılım Teknolojileri Araştırma Enstitüsü (YTE) e-Devlet Planlama Birim Yöneticiliği görevini yürüttü, kamu kurumları için gerçekleştirilen dijital dönüşüm çalışmalarında proje yöneticiliği ve danışmanlık yaptı. 2016 yılından itibaren kamu kurumlarının siber güvenlik kapasitesinin iyileştirilmesi ve siber güvenlik teknolojilerinin kazanımı konularında TÜBİTAK-BİLGEM Siber Güvenlik Enstitüsü (SGE) tarafından yürütülen projelerde görev yapmakta ve aynı zamanda Siber Güvenlik Enstitüsü (SGE) Uygulama Güvenliği Birim Yöneticiliğini yürütmektedir.

Bilgi Güvenliği Derneği, kuruluşundan bugüne kadar ülkemizin **"Siber Güvenlik ve Savunmasının"** gelişimine katkı sağlamakta, birikimini topluma aktarmakta, içerik üretilmesine, yeni çözümler geliştirilmesine ve bilginin yaygınlaştırılmasına destek vermekte, kamuoyunun farkındalığını artırmaya çalışmakta ve sonuçta siber ve bilgi güvenliğinin kişisel, kurumsal ve ulusal boyutta sağlanmasına katkılar sunmaktadır. Tehditlerin artması, boyut ve yön değiştirmesi, çeşitlerinin artması, siber tehdit ekosisteminin büyümesi, kritik altyapıların hedef haline gelmesi, bilgi hırsızlıklarının çoğalması, yeraltında çalışan korsanların etkinleşmesi, siber tehditlerin artık savaşa dönüşmesi, siber suçların ve suçluların çoğalması, siber terörün artması nedeniyle, siber saldırılarla, suçlarla, terörizmle, zafiyetlerle mücadeleye her zamankinden daha fazla ihtiyaç duyulmaktadır. Kapsamlı bir mücadele için; ulusal stratejileri ve eylem planlarının iyileştirilmesi, araştırma merkezlerinin etkinleştirilmesi, yeni altyapılar kurulması, yeni programların açılması ve son zamanlarda ise "siber ordular", "mükemmeliyet merkezleri", "ulusal siber olaylara müdahale", "siber savunma merkezleri" gibi yapıların kurulması, mevcutları iyileştirilmesi gibi ihtiyaçlar bizleri bu kitap serisini hazırlamaya yöneltmiştir. Tehditlerin boyutunu ve geleceğini anlamak ancak ve ancak bu alanın kapsamını iyi anlamak, gelecekte karşılaşılacak olan tehditleri öngörmek, buna hazır olmak için konunun etkileşim içerisinde olduğu tüm alanları iyi bilmek, etkileşim içerisinde olunan alanları iyi tanımak, yeni alanları öğrenmek, işbirliklerini artırmak, yetenek ve kabiliyetleri geliştirmek ve daha fazla ar-ge yapmak gerekmektedir. Siber güvenlik ve savunmaya kapsamlı bir bakış sunmayı amaçlayan bu eser serisinin, ülke siber güvenliğimiz ve savunmasına katkı sağlaması beklenmektedir.

ISBN : 978-605-2233-42-9

9 786052 233429

grafiker.com.tr • 0 312. 284 16 39