Araştırma Makalesi

ISO 27001 BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ KAPSAMINDA TEK KULLANIMLIK ŞİFRE ÜRETME

İsmail Sinan TATLIGİL[†], Erkan BOLAT[††], Asst. Prof. Dr. Ali BOYACI [‡]

[†] Volfram Bilgi Teknolojileri, İstanbul, Türkiye

[††] Siber Suçlar Analiz Merkezi, İstanbul, Türkiye

[‡] İstanbul Ticaret Üniversitesi, Bilgisayar Mühendisliği, İstanbul, Türkiye

https://orcid.org/0000-0002-8495-5618, https://orcid.org/0000-0002-7342-4547, https://orcid.org/0000-0002-2553-1911

Sinan.tatligil@volfram.com.tr, erkan.bolat@sisamer.com , aboyaci@ticaret.edu.tr

ÖZET

Günümüzde en önemli bilgi kaynağı siber uzaydır. Siber uzay içerisinde yapılacak olan bilgi toplama çalışmaları ile kullanıcı hesapları ve bunlarla bağlantılı birçok hesap bilgisi elde edilecektir. Elde edilen bu bilgiler, ciddi bir istihbarat kaynağı sağlayacağından siber savaş hazırlıkları için temel kaynak olacaktır.

Siber istihbaratı engellemek için ise "Bilgi Güvenliği, Siber Güvenlik ve Mahremiyetin Korunması" alanlarını içeren ISO (International Organization for Standardization) içerisinde bir alt komite olan ISO/IEC 1/SC 27 komitesi tarafından yönetilmektedir. Tüm dünyada kullanılabilmesi için hazırlanmış olan temel standart, ISO 27001 Bilgi Güvenliği Yönetim Sistemi'dir. Kullanıcı hesaplarının yönetilmesi ve güvenliği ile ilgili olarak ISO 27001 standardının "EK-A 9.2 Kullanıcı Erişim Yönetimi" , "EK-A 9.3 Kullanıcı Sorumlulukları" ve "EK-A 9.4 Sistem ve Uygulama Erişim Kontrolü" maddelerinde derinlemesine ele alınmaktadır.

Kullanıcı hesaplarının korunmasında iki faktörlü doğrulama için akıllı kart, kısa mesaj ile tek kullanımlık şifre gönderimi , e-posta mesajı ile tek kullanımlık şifre gönderimi yada mobil uygulama üzerinden tek kullanımlık şifre gönderimi kullanılmaktadır.

Tek kullanımlık şifre üretilmesinde kişiye özel olarak şifre üretilebilmesi için kişiye ait cihaz ve içerisinde kullanılan komponentlerinin tekil özellikleri AES (Advanced Encryption Standard) algoritması kullanılarak, tek kullanımlık şifre güvenliğinin arttırılması amaçlanmıştır.

Anahtar Kelimeler: ISO 27001, Tek Kullanımlık Şifre, Dijital Hesap Güvenliği, Şifre Güvenliği, Tek Kullanımlık Şifre, Siber Uzay, IMEI, SIM Seri Numarası, ICCID

GENERATING ONE-TIME PASSWORD WITHIN THE SCOPE OF ISO 27001 INFORMATION SECURITY MANAGEMENT SYSTEM

ABSTRACT

Cyber space is the most important source of information today. User accounts and their related information will be obtained through information gathering activities in cyber space. This information will be the main source for cyber war preparations as it will provide a serious source of intelligence.

To prevent cyber intelligence, it is managed by the ISO / IEC 1 / SC 27 Committee within the ISO (The International Organization for Standardization), which includes the areas of "Information Security, Cyber Security and Protection of Privacy". The basic standard prepared for use all over the world is ISO 27001 Information Security Management System. With regard to user accounts, it can be discussed in depth within the "ANNEX-A 9.2 User Access Management", "ANNEX-A 9.3 User Responsibilities" and "ANNEX-A 9.4 System and Application Access Control" articles of ISO 27001 standard.

For the protection of user accounts, two-factor authentication is used for smart card, sending one-time password via text message, sending one-time password via e-mail message or sending single-use password via mobile application.

Geliş/Received	**:**	**27.05.2020**
Gözden Geçirme/Revised	**:**	**28.05.2020**
Kabul/Accepted	**:**	**04.06.2020**

In order to generate a personalized password for single-use password generation, it is aimed to increase the single-use password security by using the AES (Advanced Encryption Standard) algorithm for the individual features of the device and its components.

Keywords: ISO 27001, One Time Password, Digital Account Security, Password Security, One Time Password, Cyber Space, IMEI, SIM Number, SIM Serial Number, ICCID

1. GİRİŞ

Teknolojinin bir çok alanda yaygınlaşmasıyla birlikte bilgiye ulaşım her geçen gün kolaylaşmaktadır. Bilgiye ulaşımda internet yaygınlaşmaktadır. Bilgi çağı olarak kabul edilen günümüzde, bilgiye nasıl erişim sağlanacağı (Ortaş, 2018)'e göre içinde bulunduğumuz Bilgi ve İletişim Teknolojileri çağının en hareketli alanını bilgiye ve üretime erişim ve bilginin paylaşımı oluşturmaktadır. Bilim ve teknoloji yapan toplumların önemli bir özeliği bilgiye kolay erişmeleridir. BİT çağında bilgi hızla üretildiği gibi hızla da tüketilmektedir. Bu bağlamda bilgi ve iletişim teknolojileri ulusal ve uluslararası alanda ciddi bir rekabet alanı konumunda olup, ülkeler bu konuda bilgi ve iletişim politikaları oluşturmuşlardır. Bilim ve teknoloji üreten ülkeler yeni gelişmeleri takip etmek ve hatta güncel gelişmelerden kopmamak ve elindeki veri ve/veya bilgiyi üretime dönüştürmek için bilgiye zamanında erişim için yeni mekanizmalar devreye sokmaktadırlar. Bilgiye erişim için kullanılan BİT günümüzde siber uzay olarak adlandılıyor. Siber uzay içerisinde ise ülkelerin bilgi savaş modellerine bir yenisi daha eklenerek siber savaş kavramı da hayatımızın içerisinde yer almaktadır. (Bayraktar, 2018)'a göre Önümüzdeki dönemde savaşların kaderini klasik cephelerin yerine, asimetrik bir etki oluşturan ve harbin beşinci boyutu olarak kabul edilen siber uzayda yaşanan savaşlar belirleyecektir. Siber uzayda gerçekleşecek olan savaşlarda tıpkı klasik cephe savaşlarında olduğu gibi istihbarat yani bilgi toplamak önem arz edecektir. Kullanıcı bilgileri ve hesapları ise istihbaratta önemli bir yer tutacaktır. Bu nedenle siber uzayda güvenliğin sağlanması ve kullanıcı hesaplarının korunması günümüzde Siber Güvenlik olarak ifade edilmektedir.

Siber güvenliğin sağlanması için bir çok ülkenin üye olduğu ISO (International Organization for Standardization) içerisinde bir alt komite olan ISO/IEC 1/SC 27 komitesi tarafından ISO 27001:2013 Bilgi Güvenliği Yönetim Sistemi standardı yayınlanmıştır. Aynı zamanda bu standart ihtiyaçlar ve gelişmelere göre güncellenmektedir. (International Organization for Standardization, 2020) Yayınlanmış olan standart içerisinde kullanıcı hesaplarının yönetilmesi ve güvenliğinin sağlanması için kullanıcı hesaplarıyla ilgili olarak ISO 27001 standardının "EK-A 9.2 Kullanıcı Erişim Yönetimi" , "EK-A 9.3 Kullanıcı Sorumlulukları" ve "EK-A 9.4 Sistem ve Uygulama Erişim Kontrolü" maddeleri içerisinde derinlemesine ele alınmaktadır.

Kullanıcı hesaplarının korunması için klasik yöntem olan kullanıcı adı ve şifre kullanımı günümüz siber uzayında artık yeterli olmadığının değerlendirilmesinin en önemli nedenlerinden biri siber saldırılar sonucunda elde edilen kullanıcı bilgileridir. Kullanıcı bilgilerini yani dijital kullanıcı hesaplarını korumak için iki faktörlü doğrulama yöntemleri gibi sistemlerin geliştirilmesi üzerine çalışılmaktadır.

Bu çalışmaları destekleyen ISO 27001 Bilgi Güvenliği Yönetim Sistemi'nde, dijital hesapların şifre güvenliği ve tek kullanımlık şifre üretimi önem arz etmektedir. Tek kullanımlık şifrelerin üretimi (One Time Password – OTP) ise kişiselleştirildiği takdirde siber saldırı ile ele geçirilmesini zorlaşacaktır. Tek kullanımlık şifre ile yapılan çalışmalarda mobil kullanıcılar için bulundukları konumu temel alan raslantısal olarak tek kullanımlık şifre üretimi önermişlerdir. (Özsoy & Burunkaya, 2013), Tek kullanımlık şifreler ve yakın alan iletişimi (NFC- Near Field Communication) teknolojileri ile birlikte şifre kullanımının tarihe mi karışacağı değerlendirilmiştir. (Watts, 2015) İnternet bankacılığı için çoklu doğrulama ile ilgili olarak QR kod öncesi üretilen OTP ile QR kod oluşturarak, son doğrulama adımında IMEI (International Mobile station Equipment Identities) karşılaştırması ile ödeme işlemi gerçekleştirilmesinin güvenliği arttırdığı değerlendirilmektedir. (Neenu ve Soman, 2017) Mikro kaos ve kaotik uygulamalar ile rastgele sayı üretici kullanarak donanımsal olarak şifre üretici tasarlanmıştır. (Akkaya ve ark., 2018) Donanımsal olarak kullanılan şifre üreticiler her hangi bir kötü niyetli kişinin eline geçtiği takdirde bu donanım ters mühendislik yöntemleriyle çözümlenebilir ve çalışma mantığı tespit edilerek tekrar kullanılabilir olacaktır.

2. ISO 27001 BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ

ISO tarafından yayınlanan Bilgi Güvenliği Yönetim Sistemi her tip kuruluş tarafından uygulanabilir olması için tasarlanmıştır. (International Organization for Standardization, 2020). Standart uygulanırken 7 ana madde yani madde 4'ten Madde 10'a kadar ve EK-A 14 madde, EK-A.5'ten EK-A.18'e kadar ele alınarak uygulanmaktadır.

Kullanıcı hesaplarının yönetimi ve güvenliği için EK-A.9 ncu maddesi temel alınarak uygulanılması beklenmektedir. Bu maddeler içerisinde özetle "Kullanıcı Erişim Yönetimi", "Kullanıcı Sorumlulukları" ve "Sistem ve Uygulama Erişim Kontrol" leri yardımıyla dijital hesapların güvenliğinin sağlanması öngörülmektedir.

Kullanıcı Erişim Yönetimi : Kullanıcı kaydetme ve silme, erişmine izin verme, ayrıcalıklı erişim haklarının yönetimi, kullanıcılara ait gizli kimlik doğrulama bilgilerinin yönetimi, kullanıcı erişim haklarının gözden geçirilmesi ve erişim haklarının kaldırılması ve düzenlenmesi konularını ele almaktadır. (International Organization for Standardization, 2013)

Kullanıcı Sorumlulukları : Gizli kimlik doğrulama bilgisinin kullanımı'nı ele almaktadır. (International Organization for Standardization, 2013)

Sistem ve Uygulama Erişimi Kontrolü : Bilgiye erişimin kısıtlanması, güvenli oturum açma prosedürleri, parola yönetim sistemi, ayrıcalıklı destek programlarının kullanımı ve program kaynak koduna erişim kontrolü'nü ele almaktadır. (International Organization for Standardization, 2013)

Tüm bunları ele aldığımız takdirde, bir dijital kullanıcı hesabının nasıl açılacağına, nasıl yetki verileceğine, nasıl doğrulanacağına, kullanıcıların şifrelerini nasıl korumaları gerektiğine, sistemlerde ve uygulamalarda güvenli oturum açma ve şifre/parola yönetim sistemlerinin nasıl yönetileceğine dair kuralların belirlenmesi siber güvenlik için ne kadar önemli olduğu anlaşılmaktadır.

3. DİJİTAL HESAPLARIN ŞİFRE GÜVENLİĞİ

Dijital hesaplar geleneksel olarak kullanıcı adı ve şifre ile korunmaktadır. Dijital hesapların içerisinde sadece bu iki bilgi değil aynı zamanda kullanıcı ile ilgili bir çok farklı bilgi de bulunabilmektedir. Bu bilgiler genel olarak değerlendirildiğinde karşımıza ortalama olarak Tablo 1'de ki bilgiler çıkmaktadır.

Tablo 1. Kullanıcı Hesaplarında Bulunduğu Değerlendirilen Bilgiler

Kısaltma (İngilizce)	Tanım (İngilizce)	(Tanım Türkçe)
CCN	Credit Card Number	Kredi Kartı Numarası
SSN	Social Security Number	Sosyal Güvenlik Numarası
NAA	Names	İsimler
EMA	Email Adresses	E-Posta Adresleri
MICS	Miscellaneous	Diğer
MED	Medical	Sağlık
ACC	Account Information	Hesap Bilgileri
DOB	Date of Birth	Doğum Tarihi
FIN	Financial Information	Finansal Bilgiler
UNK	Unknown	Bilinmeyen
PWD	Passwords	Şifreler
ADD	Addresses	Adresler
USR	User Name	Kullanıcı Adı
NUM	Phone Number	Telefon Numarası
IP	Intellectual Property	Fikri Mülkiyet

Tablo 1' de bulunan bilgiler dijital hesapları çalındığı takdirde kullanıcıların hangi bilgisinin çalındığı hakkında bize fikir ve bilgiler vermektedir. Tablo 2'de ise Cyber Risk Analytics tarafından yayınlanan 2019 yılı raporunda en yüksek miktarda veri kaybı yaşayan kurumlardan ilk 5'i örnek olarak alınmış. (Cyber Risk Analytics, 2020)

Tablo 2. 2019 yılında yılı raporunda en yüksek miktarda veri kaybı yaşayan kurumlardan ilk 5

KURUM BİLGİSİ	RAPORLAMA TARİHİ	ÇALINAN VERİ MİKTARI ADET	KAYIT TİPLERİ
Verifications.io	7.3.2019	982.864.972	ADD / DOB / EMA / FIN / MISC / NAA / NUM / PWD
982.864.972 adet isim, adres, e-posta adresi, doğum tarihi, telefon numarası, faks numarası, cinsiyet, IP adresi, kişisel mortgage tutarları ve yanlış yapılandırılmış bir veritabanı nedeniyle İnternet'te ifşa edilen FTP sunucusu kimlik bilgileri			
First American Financial Corporation	24.5.2019	885.000.000	ADD / EMA / FIN / MISC / NAA / NUM / SSN
İsimleri, Sosyal Güvenlik numaralarını, telefon numaralarını içeren yaklaşık 885.000.000 adet gayrimenkul kapanış işlem kaydı, e-posta ve fiziksel adresler, ehliyet görüntüleri, bankacılık bilgileri ve ipotek borç veren adları ve kredi numaraları IDOR kusuru nedeniyle internette ifşa edilen			
Cultura Colectiva	3.4.2019	540.000.000	ACC / MISC
Yanlış yapılandırılmış bir veritabanı nedeniyle İnternet'te maruz kalan Facebook kullanıcı kimlikleri, hesap adları, yorumlar ve beğeniler			
Unknown Organization	1.5.2019	275.265.298	DOB / EMA / FIN / MISC / NAA / NUM
Unistellar hacking group isimli bir grup tarafından 275.265.298 adet Hint vatandaşının adları, e-posta adresleri, cinsiyetleri, doğum tarihleri, telefon numaraları, eğitim bilgileri ve halka açık endeksli MongoDB örneğinde tutulan maaşlar, mesleki beceriler ve işveren geçmişi gibi istihdam ayrıntıları alındı			
Unknown Organization	10.1.2019	202.730.434	ADD / DOB / EMA / MISC / NAA / NUM
Yanlış yapılandırılmış bir veritabanı nedeniyle 202.730.434 adet iş başvurusunda bulunanların isimleri, adresleri, doğum tarihleri, telefon numaraları, e-posta adresleri, evlilik durumları, sürücü belgesi bilgileri			

Milyonlarca dijital hesap ve bilgilerin çalındığı günümüzde dijital hesapların güvenliği için bir çok yöntem öne sürülmektedir. Bunlar şifrelerin karmaşık olması, belli sürelerde değiştirilmesi, şifrelerin uzun (6-8 karakter) olması ve son dönemlerde de çok aşamalı doğrulama (MFA-Multi-Factor Authentication) güvenlik için kullanılmaya başlanmıştır.

4. TEK KULLANIMLIK ŞİFRE

Tek kullanımlık şifre RFC2289 (Internet Engineering Task Force, 1998) ve tek kullanımlık zaman tabanlı şifre (Internet Engineering Task Force, 2011) üretilmesi RFC6238 koduyla IETF tarafından standartlaştırılmıştır.

Tek kullanımlık şifreler ve zaman tabanlı şifreler günümüzde MFA olarak bir çok global şirket tarafından kullanılmaktadır. Bunlardan başlıcaları; Facebook, Microsoft, Google, Instagram ve benzeri şirketlerdir.

5. KİŞİSELLEŞTİRİLMİŞ TEK KULLANIMLIK ŞİFRE GELİŞTİRME

Tek kullanımlık şifrelerin farklı algortimalar ve yöntemler ile geliştirilmesi her geçen gün gelişen atak tipleri için bir zorunluluk haline gelmektedir. Nitekim (Florencio ve ark., 2007) dijital hesaplarda güçlü şifrelerin kullanımının bir öneminin olmadığını değerlendirmektedir.

Ayrıca tek kullanımlık şifreler ve yakın alan iletişimi (NFC- Near Field Communication) teknolojileri ile birlikte şifre kullanımının tarihe karışabileceği ihtimali değerlendirilmiştir. (Watts, 2015)

Tek kullanımlık şifrelerin üretilmesiyle ilgili olarak mobil kullanıcılar için bulundukları konumu temel alan raslantısal olarak tek kullanımlık şifre üretimi önermişlerdir. (Özsoy ve Burunkaya, 2013) Burada kullanıcıların konumları bulundukları yerler tahmin edilebilecektir. Kişiler tek kullanımlık şifreleri ile ilgili işlemleri ağırlıklı sabit noktalardan gerçekleştirmektedirler. Bu sabit noktalar ev, iş yada konakladıkları oteller gibi değerlendirilebileceğinden konumlarının tahmin edilmesi kolaylaşacaktır.

Tek kullanımlık şifre üretimi için mobil cihazlar üzerinden tek kullanımlık şifre üretimi ve konum tabanlı tek kullanımlık şifre üretimi yöntemleriyle bir çok çalışma bulunmaktadır. Daha güvenli hale getirmek için kullanıcı ve mobil cihaz özelinde tek kullanımlık şifre üretilmesi gerekmektedir. Bu sayede ele geçirilmesi ve elde edilmesi çok daha zor olacaktır. Aynı zamanda GPS, internet gibi bağlantı ihtiyacı da gerekmeyecektir.

Tek kullanımlık şifre üretimi için donanım kullanılmasıyla ilgili olarak Mikro kaos ve kaotik uygulamalar ile rastgele sayı üretici kullanarak donanımsal şifre üretici tasarlanmıştır. (Akkaya ve ark., 2018) Donanımsal olarak kullanılan şifre üreticiler her hangi bir kötü niyetli kişinin eline geçtiği takdirde bu donanım kullanılabilir olacaktır. Hatta donanım ele geçirilmesi sebebiyle tersine mühendislikle tamamen geçersiz kılınması mümkün olabilecektir.

İnternet bankacılığı için çoklu doğrulama ile ilgili olarak QR kod öncesi üretilen OTP ile QR kod oluşturarak son adımında IMEI karşılaştırması ile ödeme işlemi gerçekleştirilmesi güvenliği artırdığı değerlendirilmektedir. (Neenu ve Soman, 2017) Üretilen tek kullanımlık şifre elde edildiği takdirde burada da QR kod üretilebilmesi mümkün olacaktır. Ancak buradaki önemli olan nokta bir den fazla üreteç kullanılarak doğrulama yapılması sebebiyle güvenlik seviyesi yükseltilmiş olduğu değerlendirilebilecektir.

Mobil kullanıcının tek kullanımlık şifre ihtiyacı kullanmış olduğu cihazın IMEI numarası ve SIM kartının seri numarası kullanılarak kişiselleştirilmiş tekil bir şifre üretilmesinin mümkün olacağı değerlendirilmektedir.

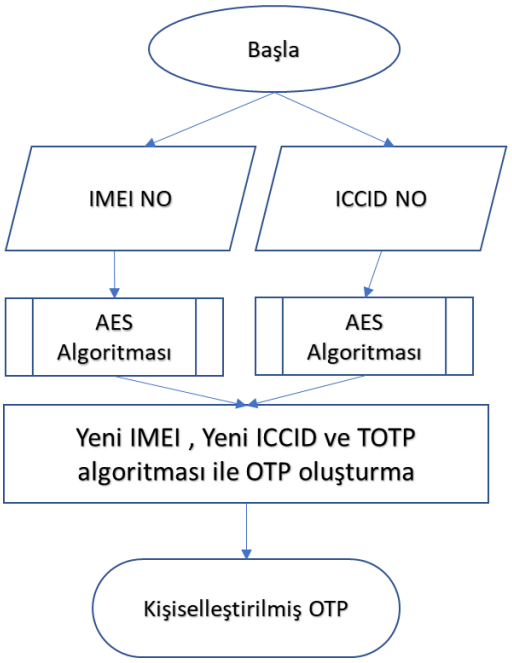
IMEI numaralarının kullanımı cihaz kaybolduğu yada acil durum çağrılarında kullanılabildiği için (3GPP, 2009) IMEI numaralarının kullanımı etkin bir yöntem olacağı değerlendirilmektedir.

2004 itibariyle, IMEI'nin formatı AA-BBBBBB-CCCCCC-D'dir, ancak her zaman bu şekilde görüntülenmeyebilir. IMEISV, Luhn kontrol basamağına sahip değildir, bunun yerine Yazılım Sürüm Numarası (SVN) için iki basamağa sahiptir, bu da AA-BBBBBB-CCCCCC-EE formatını oluşturur.

ICCID (Internationally Identified by Its Integrated Circuit Card Identifier) SIM kart kullanımı aynı şekilde IMEI numarası gibi tekil bir şifrede kullanılması güçlü ve etkin bir yöntem olarka değerlendirilmektedir.

Her SIM, entegre devre kartı tanımlayıcısı (ICCID) tarafından uluslararası olarak tanımlanır. ICCID, gerçek SIM kartın kendisinin tanımlayıcısıdır - yani SIM yongası için bir tanımlayıcıdır. Günümüzde ICCID numaraları, yalnızca fiziksel SIM kartları değil, eSIM profillerini tanımlamak için de kullanılmaktadır. ICCID'ler SIM kartlarda saklanır ve ayrıca kişiselleştirme adı verilen bir işlem sırasında SIM kart gövdesine işlenir veya yazdırılır.

IMEI numarası ve SIM Kart Seri Nosu bilinen bir algoritma içerisine alınarak (AES Algoritması) zaman bazlı tek kullanımlık şifre (Time Based One Time Password – TOTP) algoritması ile birlikte Şekil 1.'de Kişiselleştirilmiş OTP üretmekteyiz.



Şekil 1. Kişiselleştirilmiş OTP

Algoritmalar AES ve TOTP ispatlı olduklarından dolayı bizim yöntemimiz dijital hesapları güvenli tutmak adına kişielleştirilmiş tekil şifre üreterek güvenliği arttırmaktadır.

Bu sayede mobil cihaz çalınsa bile mobil cihazın içerisindeki IMEI numarasından ve SIM kart seri numarasından üretilien bilgilerin TOTP ye girdi olarak kullanılarak tek seferlik şifrenin tekrar üretilmesi gerçekleşemeyecektir.

Tablo 3'de önerilen yöntem ve diğer yöntemlerin karşılaştırılması gösterilmiştir.

Tablo.3 Önerilen yöntem ve diğer yöntemlerin karşılaştırılması

	ÖNERİLEN YÖNTEM	**S. WATTS**	**S.YAKUT-A.B.ÖZER**	**M.BURUNKAYA-M.ÖZSOY**
	KİŞİSELLEŞTİRİLMİŞ OTP	NFC	OTP	LOKASYON BAZLI OTP
TAHMİN EDİLEMEMEZLİK	✓	✓	✓	✓
ÇOKLU DOĞRULAMA	✓	✗	✓	✓
LOKASYON	✗	✗	✗	✓
IMEI NO	✓	✗	✗	✗
SIM KART SERİ NO	✓	✗	✗	✗

6. SONUÇ

Dijital hesapların güvenliği artık vazgeçilmez bir hal almaktadır. Bu hesaplara erişim güvenliği ise bir çok farklı yöntem ile sağlanmaya çalışılıyor. Dünya'da uluslararası standartlar ile dijital hesapların güvenliği bir temele oturtulmaya çalışılırken çoklu doğrulama yöntemleri ve tek kullanımlı şifreler vaz geçilmez hale geliyor.

Tek kullanımlık şifreler ise zaman bazlı, lokasyon bazlı ve farklı algoritmalar ile üretilebiliyor. Çalışmamızda kullanılan mevcut tüm çözümlerin kolaylıkla suistimal ve tahmin edilebileceği değerlendirilmiştir. Kişiselleştirilmiş tek kullanımlık şifrenin üretilebilmesi için kişinin mobil cihaz bilgileri kullanılarak IMEI ve SIM kart seri numarası AES ve TOTP algoritmalarından geçirilerek üretilen OTP şifreleri ile dijital hesaplar çok daha güvenli hale getirilmektedir.

KAYNAKLAR

3GPP. (2009, 9). International Mobile station Equipment Identities. *3rd Generation Partnership Project;Technical Specification Group Services and System Aspects*. 3GPP TS 22.016 V9.0.0.

Akkaya, S., Pehlivan, İ., Akgül, A., & Varan, M. (2018, 3). The design and application of bank authenticator device with a novel chaos based random. *Journal of the Faculty of Engineering and Architecture of Gazi University*, s. 1171-1182.

Bayraktar, G. (10). Harbin Beşinci Boyutunun Yeni Gereksinimi: Siber İstihbarat. *Güvenlik Stratejileri*(20), 12.

Cyber Risk Analytics. (2020, 4 23). *riskbasedsecurity.com.* https://pages.riskbasedsecurity.com/hubfs/Reports/2019/2019%20MidYear%20Data%20Breach%20QuickView%20Report.pdf adresinden alındı

Florencio, D., Herley, C., & Coskun, B. (2007). *Do Strong Web Passwords Accomplish Anything?* USA: Microsoft Research.

International Organization for Standardization. (2013). Bilgi teknolojisi - Güvenlik teknikleri - Bilgi güvenliği yönetim sistemleri - Gereksinimler.

International Organization for Standardization. (2020, 4 23). *ISO.ORG*. https://www.iso.org/isoiec-27001-information-security.html adresinden alındı

Internet Engineering Task Force. (1998, February). *A One-Time Password System*. Internet Engineering Task Force: https://tools.ietf.org/html/rfc2289 adresinden alındı

Internet Engineering Task Force. (2011, May). *TOTP: Time-Based One-Time Password Algorithm*. Internet Engineering Task Force: https://tools.ietf.org/html/rfc6238 adresinden alındı

Neenu , A. S., & Soman, S. (2017). Multi-Factor Authentication for Net Banking. *International Journal of System and Software Engineering*, Volume 5 Issue 1.

Ortaş, İ. (2018). Bilgi ve İletişim Çağında Bilimsel Bilgiye Erişimin Önemi ve Türkiye'nin Bilgiye Erişim Potansiyeli. *Türk Kütüphaneciliği*, 4.

Özsoy, M., & Burunkaya, M. (2013). Mobil Kullanıcılar için Konum Tabanlı Rastlantısal Tek Kullanımlık Şifreler . *BİLİŞİM TEKNOLOJİLERİ DERGİSİ*.

Watts, S. (2015, July). *NFC and 2FA: the death of the password.* Network Security Newsletter: https://www.sciencedirect.com/science/article/abs/pii/S1353485815300611 adresinden alındı