VoIP Teknolojilerinde Opnet Tabanlı Güvenlik Uygulaması

Ceyhun ÇAKIR[1] Hakan KAPTAN[2]

Marmara Üniversitesi Teknik Eğitim Fakültesi Elektronik Bilgisayar Eğitimi Bölümü[1,2]
ceyhuncakir@yahoo.com[1] hkaptan@marmara.edu.tr[2]

Özet— Internet ve uygulamalarının hızlı bir şekilde artması yüksek seviyeli güvenlik servislerine olan ihtiyacı attırmaktadır. İnternet uygulamalarından VoIP teknolojilerinin en büyük problemi band genişliği ve güvenlik tehditleridir. Güvenlik açıkları kullanılarak, VoIP sistemlerine saldırılar düzenlenebilir. Bu saldırılar sonucunda VoIP trafiği saldırganlar tarafından kesilebilir, kopyalanabilir, engellenebilir, yavaşlatılabilir veya değiştirilebilir. Bir VoIP sistemindeki güvenlik açıkları, kullanılan cihazlardan, yazılımlardan ve protokollerden kaynaklanabilir. Bu çalışmada, VoIP mimarisine yönelik tehditler, saldırılar incelenmiş, bu tehditlere karşı geliştirilen önlemlere ve teknolojilere değinilmiştir. OPNET modelleme programı kullanılarak, güvenlik simülasyonları gerçekleştirilmiş, VoIP teknolojisinde güvenli iletişim için gereken unsurlar ortaya konmuştur.

Anahtar kelimeler— VoIP güvenlik, Opnet

Opnet Based Security Application in VoIP Technologies

Abstract— With the dramatic increase of the use of the Internet and its applications increase necessity of high level of security services. VoIP is one of the Internet applications and biggest problems with VoIP technology are bandwidth and security threats. The attacks with the use of vulnerability on VoIP systems can be arranged, as a result of this attack, VoIP traffic can be interrupted, can be copied, can be prevented, can be slowed or changed by an attacker. Vulnerability in a VoIP system can arise from equipment, software and protocols. This paper investigates common threats and attacks that used on VoIP technology and different precautions and security technologies. Security simulations are realized by using OPNET modeler and secure VoIP technology components required for secure communication have been identified.

Keywords— VoIP security, Opnet

1. GİRİŞ

Voice over IP (VoIP) bir ses iletim tekniğidir. Bu teknoloji sayesinde ses, veri paketleri halinde IP üzerinden gönderilebilmektedir. IP üzerinden sesi iletmek, internete ulaşılabilen her yerde, birkaç cihaz ve hatta yalnız yazılımlar ile sesli görüşme yapabilmek anlamına gelmektedir. Bu kullanıcıya daha ucuz, erişilebilir, kullanışlı bir sistem sağlamaktadır. Haberleşme teknolojisindeki bu gelişmeler yalnız bireysel kullanıcıların değil, kurumsal abonelerin de VoIP teknolojisine geçişini sağlamaktadır[1].

VoIP bu yönleriyle diğer sesli görüşme sistemlerine karşı avantaj sağlamaktadır. Ancak iletim IP üzerinden, yani internetten sağlandığı için internette oluşan sorunlardan etkilenmektedir. IP protokolünden dolayı VoIP bazı güvenlik problemleri taşımaktadır. VoIP trafiği, diğer veri akışlarında olduğu gibi bir yönlendiriciden (router) diğerine giden trafik olarak değerlendirilebilir. Bu da diğer Internet trafikleri gibi saldırılara ve engellemelere açık olması demektir[2].
Sistemi tehdit eden unsurlar; kullanılan protokoller, VoIP cihazları, yazılımlar gibi farklı parametrelerden oluşur. Bununla birlikte sisteme farklı saldırı yöntemleri mevcuttur. Bunların sonucunda VoIP trafiği kötü niyetli kişiler tarafından kesilebilir, kopyalanabilir, engellenebilir, yavaşlatılabilir veya değiştirilebilir. Bu sorunlar karşısında geliştirilen sistemler, VoIP görüşmelerini daha güvenilir hale getirmeyi hedeflemektedir.

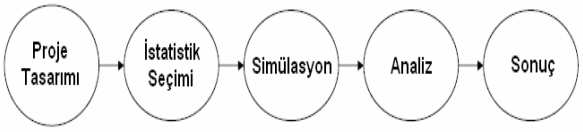
İletişim altyapısında yer alan VoIP cihazları, noktalar arası ses iletiminde kullanılmaktadır. Kullanıcının iletişimde kalabilmesi için bir ağa bağlanması, internete erişebilmesi gerekir. Bununla birlikte bir arayüz kullanmalı, bazı durumlarda şifreleme işlemleri yapılmalı, duruma uygun protokol seçilmelidir. Tüm bu değişkenlerdeki hatalar sistemin güvenliğini tehdit eden unsurlardır.

İnternet güvenliği kesin olarak sağlanamamış bir konu olarak önümüzde durmaktadır. Bir VoIP sisteminde yukarıda sayılan parametreler de dahil olunca daha çok etkenin sağlıklı çalışması, VoIP güvenliği açısından son derece önemlidir. Kullanılacak protokolün zayıf noktalarından, şifreleme yapılmamasından veya kullanılan şifreleme siteminden kaynaklanan güvenlik açıkları, kullanılacak programdan kaynaklanan hatalar sistemi olumsuz yönde etkilemektedir.

2. OPNET

Opnet, IT teknolojilerini modelleme yoluyla analiz eden bir simülasyon programıdır. Opnet, ağ teknolojileri, uygulamalar, çeşitli bileşenlerle oluşturulmuş bir sanal ortamdır. Dünya üzerinde binlerce ticari ve ulusal kuruluş ve beş yüzü aşkın üniversite Opnet yazılımını kullanmaktadır. [3] Türkiye'de Boğaziçi Üniversitesi Netlab Laboratuarı, Anadolu Üniversitesi Elektrik Elektronik Mühendisliği Bilgisayar Laboratuarı, Sabancı Üniversitesi ve Sakarya Üniversitesi Teknik Eğitim Fakültesi'nde kullanılmaktadır. [4-6] Opnet modelleme programı kullanılarak birçok akademik çalışma gerçekleştirilmiştir. Bilimsel makalelerde ve tez çalışmalarında sıkça kullanılmaktadır.

Opnet, yazılımı istenilen boyuttaki alanlarda simülasyon yapmaya olanak sağlar. Opnet yazılımı ile ofis boyutunda bir proje oluşturmak mümkün olduğu gibi, kıtalararası bir proje gerçekleştirmek de mümkündür. Ayrıca projenin simülasyon süresi, birkaç saniye ile birkaç hafta arası değiştirilebilir. Bu durum, Opnet modelleme programının gerçeğe uygun simülasyonlar gerçekleştirdiğinin bir göstergesidir. Şekil 1 de Opnet modelleme programının işlem akışı görülmektedir.



Şekil 1 Opnet İşlem Akışı

Opnet modelleme programı kullanılarak, birçok akademik çalışma yapılmıştır. Özellikle yurtdışı birçok makale yayınında opnet simülasyonları kullanılmıştır. Bunun yanında birçok tez çalışması Opnet temeline dayandırılarak gerçekleştirilmiştir [7-11].

Bu çalışmada da Opnet modelleme program kullanılarak VoIp teknolojisine etki eden tehditler ve bunlara karşı oluşturulan güvenlik önlemleri analiz edilmiştir.

3. TEHDİTLER ve SALDIRILAR

VoIP teknolojisinde güvenli protokoller, destekleyici servisler ve cihazlar kullanılması durumunda bile, her saldırıya karşı korunmak zordur. VoIP mimarisinde güvenlik zaafları oluşabilir ve bu durum tam bir koruma sağlanmasını önler. Alt katmanlarda sağlanacak güvenlik, sistem güvenliği için çok önemlidir. Uygulama katmanında yapılacak analizler ve uygulamalar ise, güvenli bir ağ oluşturmak için daha pratik bir çözümdür. Aşağıda VoIP mimarisinde karşılaşılan saldırıların sınıflandırması mevcuttur[12,13].

- Hizmet Karıştırma (Service disruption): VoIP servislerini, yönetimi, erişimi bozmaya yönelik saldırı türüdür. Bu kategoride bulunan saldırılar, routerlar, DNS sunucuları, proxy sunucuları gibi ağ bileşenlerini etkileyebilir. Bu tür saldırılar hedef alınan bileşenlere doğrudan erişim olmadan, uzaktan saldırı gerçekleştirebilir ve yönetebilirler. Saldırgan VoIP telefon gibi bir terminali, bir ağ bileşenini veya bir grubu hedef alabilir. SPIT (Spam Through Internet Telephony) gibi büyük sorun oluşturan saldırılar bu kategoride yer alırlar.

- Telekulak (Eavesdropping, Annoyance): Aktarılan bilgiye erişmek amacıyla yapılan saldırı türüdür. Bu durum kullanıcılar arasında yapılan korumasız sinyalleşmenin ve veri paketlerinin görüntülenmesi anlamına gelmektedir. Trafik analizleri bu kategoride incelenmektedir. Veri paketlerine erişmek, saklamak, analiz etmek mümkündür. Saldırının amacı konuşmadaki sözlü veya yazılı bilgileri elde etmektir. Bu sayede kart numaraları ve pin numaralarına ulaşılabilir. Bağlantının analizi yapılarak, sistemin zayıf yanları tespit edilir.

- Gizlenme (Masquerading and impersonation): Bir kullanıcı veya sistem bileşeni gibi davranılarak, ağa erişimin sağlandığı saldırı türüdür. Bu şekilde bir başka kullanıcıya, servise veya bileşene erişilmesi amaçlanır. Bu önemli bir saldırı türüdür. Çünkü, çağrı dolandırıcılığı (fraud), yetkisiz sisteme girme (unauthorized access) ve hizmet engelleme (service disruption) saldırıları, bu yöntem kullanılarak gerçekleştirilebilir. Bu saldırının özelliği, sistem bileşenlerinin kimliğini taklit edebilmesidir. Saldırının hedefi bir kullanıcı, aygıt ya da ağ bileşeni olabilir. VoIP bileşenlerine izinsiz erişerek veya uzaktan bağlantı kurarak sinyalleşmeyi veya veri paketlerini kendi isteği doğrultusunda kullanabilir. Örneğin, yetkilendirme için yalnız kullanıcı adının kullanıldığı bir sistemde bilgilere kolaylıkla erişilebilir. Bu uygulama katmanında bir saldırıdır. Aynı zamanda VoIP mimarisinde yer alan, yardımcı protokollere (ARP, IP, DNS) de saldırı düzenlenebilir.

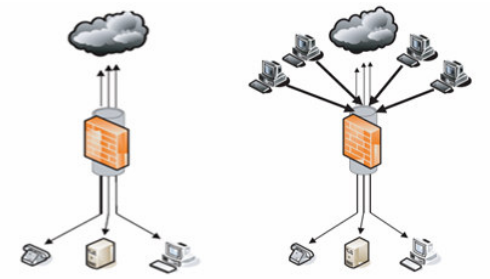
- Yetkisiz Erişim (Unauthorized Access): Bir ağ bileşenine, servise ya da özelliğe, doğru yetkilendirme olmadan erişmektir. Bu saldırı, diğer saldırı türleriyle birlikte gerçekleştirilebilir, diğer saldırılara destek sağlar. Bu saldırı türü, bileşenlerin, kaynakların ve ağ erişiminin kontrolüne imkan tanır. Yanıltma saldırılarından farkı, başka bir kullanıcının ya da bileşenin yerine geçmek zorunda olmamasıdır. Saldırı, sistemin yoğunluğundan, kullanılan ayarlardan, zayıf sinyalleşme güvenliğinden ve ağ erişimindeki zayıflıklardan yararlanılarak gerçekleştirilir. Örneğin, Proxy sunucusu aracılığıyla, yönetici niteliğine sahip bir saldırgan, sistem bilgilerini silerek, VoIP sinyalleşmesini engelleyebilir. Bu durum sunucu ve servisi devre dışı bırakır. Yine bir kullanıcı

gatewaye erişerek, zararlı bir yazılım yükleyebilir. Bu yazılımla veri paketlerini kaydedebilir.

- Dolandırıcılık (Fraud): VoIP hizmetini kötüye kullanarak kişisel ya da maddi kazanç sağlamaya yönelik saldırı türüdür. Bu saldırı türü telekom taşıyıcıları ve sağlayıcıları için en tehlikeli saldırılardandır. Bu saldırı türü, sinyalleşme mesajlarının veya VoIP aygıtlarının ayarlarının değiştirilmesiyle gerçekleştirilir. Faturalandırma sistemleri, saldırının hedefleri arasındadır. Bir bağlantıdaki çağrı akışına etki ederek, VoIP uygulamalarında çeşitli dolandırıcılık senaryoları gerçekleştirilebilir. Bunun için daha karmaşık yöntemler kullanmak gerekir. [14]

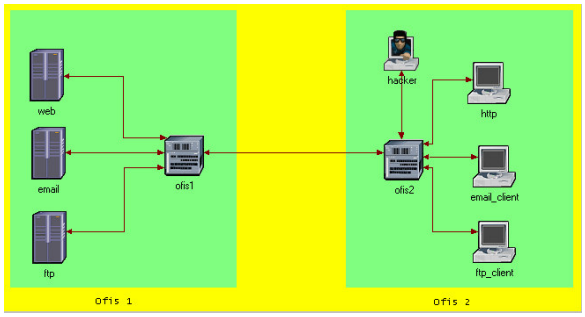
- Servis Yanıltma (Denial of Service): Servis yanıltma saldırısı (Denial of Service, DoS), IP temelli ağları hedef alır. DoS saldırıları, sistemin çalışmasına küçük etkiler oluşturabileceği gibi, sistemi tamamen kullanılamaz hale de getirebilir. Bu saldırıların bir türü, farklı harici kaynaklardan çok sayıda veri paketi göndererek, sistemin tüm çağrıları karşılayamaması esasına dayanır. [15] Şekil 2'de DoS saldırısına maruz kalan bir sistem görülmektedir. Şeklin ilk bölümünde olağan trafik akışı görülürken, ikinci bölümde ise, saldırganlar tarafından oluşturulan trafiğin kullanıcıları etkilediği görülmektedir.

DoS saldırıları, ağ içerisindeki kullanıcıların etkisiz hale getirilmesini amaçlar. Bu saldırı da benzer şekilde çok sayıda paket göndererek, kullanıcıların hizmet almasını zorlaştırır. DoS saldırılarında, servisi etkisiz hale getirmek için bant genişliği ve CPU hedef alınır.



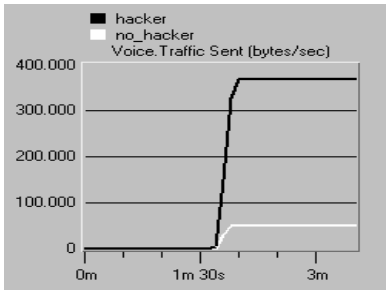
Şekil 2 DoS Saldırısı [14]

Şekil 3 de Opnet modelleme programı kullanılarak oluşturulmuş bir DoS saldırı senaryosu görülmektedir. Bu senaryoda saldırgan sistem kaynaklarına erişerek, diğer kullanıcıların hizmet kalitesini etkilemektedir.



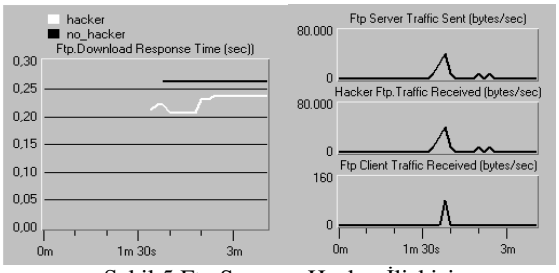
Şekil 3 DoS Senaryosu

Senaryoda sunucuların bulunduğu bir ofis ile, kullanıcıların bulunduğu diğer bir ofis arasında bağlantı kurulmuş ve bir saldırgan sisteme dahil olarak, sistem kaynaklarını kullanacak şekilde tasarlanmıştır.



Şekil 4 Ses Trafiği

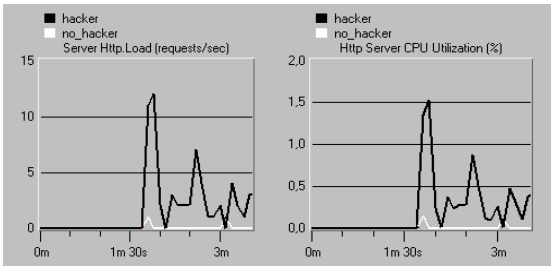
Şekil 4'de ses uygulaması için trafik değişimi görülmektedir. Grafikte, senaryolardaki ses trafiği saniyede gönderilen byte cinsinden ifade edilmiştir. Bu grafikten, sisteme bir hacker dahil olmasıyla, ses trafiğinin arttığı anlaşılmaktadır. Bunun sebebi, hacker'ın profil tanımlamasını gerçekleştirirken, VoIp hizmetinden yararlanabileceğini belirtmiş olmamızdır. Bu durum, voice trafiğinin yüksek değerlere ulaşmasına neden olmuştur. Hacker sistemdeki diğer uygulamalardan da yararlanabildiği için, tüm uygulamalarda trafik artışı görülecektir.



Şekil 5 Ftp Sunucu. Hacker İlişkisi

Şekil 5'de ftp uygulamasında download işlemi için yanıt süresinin arttığı görülmektedir. Bu durum, kullanıcılar tarafından sistemin yavaşladığı şeklinde algılanır. Bu durumun sebebi, sisteme bir hacker'ın bağlanmış olması ve DoS saldırısı düzenlenmiş olmasıdır. Ayrıca sunucudan alınan trafiğin büyük bölümü hacker tarafından kullanılmaktadır. Sisteme etki eden hacker

sayısı artması durumunda, yanıt süresi daha yüksek değerlere ulaşacaktır.



Şekil 6 Web sunucusu hizmet değişimi

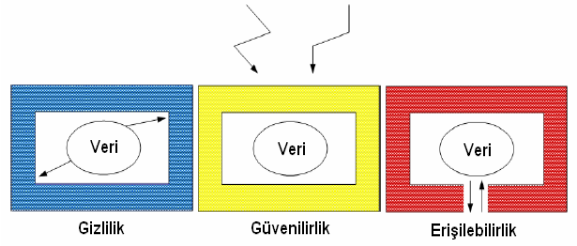
Şekil 6'de web sunucunun farklı senaryolardaki hizmet değişimi görülmektedir. İlk grafikte sisteme hacker dahil olmasıyla, sunucuya iletilen hizmet talebindeki artış görülmektedir. İkinci grafikte ise, sunucunun kullanım oranı artmıştır. DoS saldırılarının, sistem üzerindeki olumsuz etkilerinden biri işlemci hızını yükseltmesidir. İkinci grafikte bu durum ortaya konmuştur. Hacker'ın sisteme gönderdiği paket sayısındaki artışa göre, bu oran artabilir ve %100'ü geçmesi durumunda, bazı kullanıcılar hizmet alamayacaktır.

4. GÜVENLİK ÖNLEMLERİ

VoIP teknolojisi, iletişim sırasında İnternet altyapısını kullanır. Veriler, IP paketleri olarak terminaller arasında iletilir. Bu nedenle, VoIP güvenliği ile İnternet güvenliği doğru orantılı olarak etkilenir. Önceki bölümde anlatılan saldırı yöntemlerine karşı geliştirilmiş, birçok güvenlik mekanizması bulunmaktadır. Bu bölümde VoIP güvenliğinde kullanılan güvenlik önlemleri incelenecektir. Bu güvenlik önlemleri, iletim katmanından uygulama katmanına kadar, her katmanda güvenliği sağlamayı amaçlar.

Bir sistemin güvenli olabilmesi için, üç niteliği barındırması gerekir. Bunlar;

- Gizlilik (Confidentially): İletilen veriye yalnız yetkili kullanıcıların erişebilmesi anlamına gelir.
- Güvenilirlik (Integrity): Verinin dış etkenlere karşı korunması, veri bütünlüğünün sağlanması, veriyi yalnız yetkili kullanıcıların değiştirmesi anlamına gelmektedir.
- Erişilebilirlik (Availability): Sistemde tanımlı kullanıcıların, servis isteğinde bulundukları zaman, hizmet alabilmeleri olarak tanımlanmaktadır.



Şekil 7 Güvenlik Kriterleri [14]

Bir sistemde iletilen verilere, istenmeyen kişiler tarafından erişilmesinin engellenmesi, güvenliğin temellerindendir. Bu amaç için birçok yöntem geliştirilmiştir. Ancak bu yöntemler, sistem kaynaklarına erişimi zorlaştırmamalıdır. Güvenlik önlemleri üst düzeyde olan, ancak hizmet kalitesi düşük bir sistem, güvenlik kriterlerini yerine getirmiş sayılmamaktadır. [16]

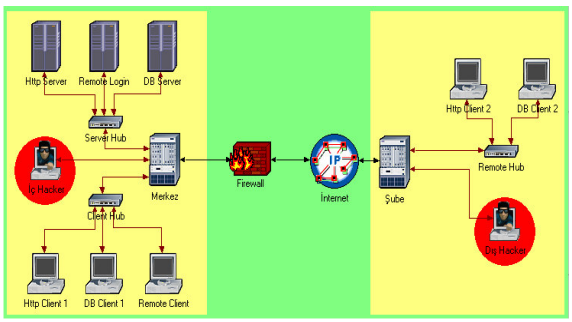
VoIP teknolojisinde güvenliği sağlamak için, çeşitli yöntemler geliştirilmiştir. Bu yöntemler farklı katmanlarda görev yapan teknolojilerden oluşmaktadır. Firewall ve VLAN VoIP teknolojisinde kullanılan güvenlik önlemlerindendir.
Bu bölümde bahsedilen güvenlik önlemleri için Opnet modelleme program kullanılarak değişik senaryolar tasarlanmış ve güvenlik önlemlerinin etkileri incelenmiştir.

4.1 Firewall

Güvenlik duvarı (Firewall), yerel ağlar üzerindeki kaynakları diğer ağlar üzerinden gelecek saldırılara karsı koruyan, iç ve dış ağlar arası ağ trafiğini tanımlanan kurallara göre denetleyen bir ağ geçidi çözümüdür. Güvenlik duvarları ağın içinden veya dışından gelen yetkisiz erişimleri engelleyen, süzen ve izin denetimi sağlayan yazılımlar veya donanımlardır. Kullanıcılarına internet erişim hakkı vermiş olan bir kurum, yerel ağındaki kaynakları korumak ve dış ağlardaki kaynaklara kullanıcılarının erişim hakkını belirlemek için yazılım veya donanım tabanlı güvenlik duvarları kullanırlar.

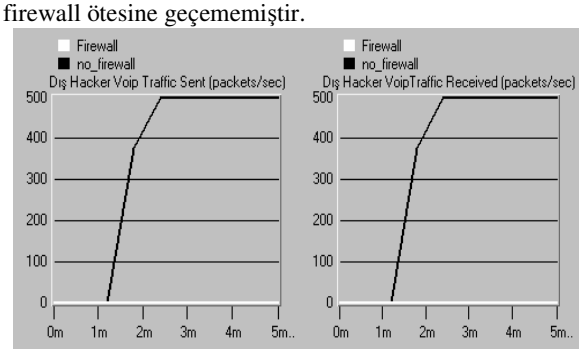
Temel olarak bir firewall, network üzerinde kendisine gelen paketleri, tanımlanan kurallar doğrultusunda geçirip geçirmeyeceğine karar verir. Güvenlik duvarları, genel olarak ağdaki diğer makinelerden farklı bir makinenin üstüne kurulurlar. Bunun sebebi, dışarıdan gelen isteklerin direkt olarak yerel ağ kaynaklarına ulaşmasını engellemektir.

Şekil 8'de Opnet modelleme programı kullanılarak bir firewall senaryosu oluşturulmuştur. Senaryoda bir iç, bir de dış saldırgan bulunmaktadır. Dış saldırgan ile sunucular arasına bir firewall yerleştirilmiştir. Güvenlik duvarının Voice trafiğine açık ve kapalı olması durumlarına göre, sistem tepkisi incelenmiştir.



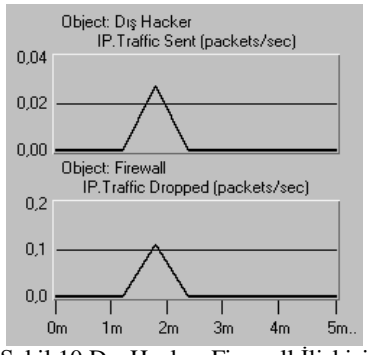
Şekil 8 Firewall Senaryosu

Şekil 9'da, Dış Hacker'ın iki senaryodaki veri trafiği görülmektedir. Buna göre; 'no firewall' isimli senaryoda Dış Hacker'ın diğer kullanıcılarla VoIP uygulaması gerçekleştirdiği görülür. Bu kullanıcılar merkez ofiste bulunmaktadırlar. Yani 'Dış Hacker' veri paketlerini, firewall üzerinden gönderebilmiştir. İkinci senaryoda ise, firewall ayarlarından voice uygulamaları engellendiği için, saldırılar engellenmiş, 'Dış Hacker'dan gelen veriler, firewall ötesine geçememiştir.



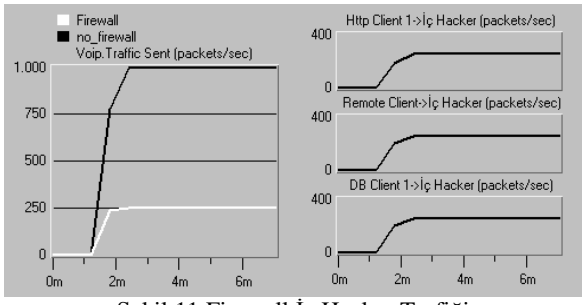
Şekil 9 Dış Hacker Trafiği

Şekil 10'da görüldüğü üzere, dış hacker tarafından gönderilen IP paketleri, firewall tarafından düşürülmüştür. Böylece, 'Dış Hacker'ın sisteme saldırı düzenlemesi engellenmiş olur.



Şekil 10 Dış Hacker-Firewall İlişkisi

Şekil 11'de, ilk grafikte, 'İç Hacker'ın her iki senaryoda da veri alışverişi yapabildiği görülmektedir. Bu durum, ikinci grafikte saniyede iletilen paket cinsinden belirtilmiştir. Bunun sebebi 'İç Hacker' ve diğer VoIP kullanıcılarının aynı bölüm içinde bulunmasıdır. Bu iki bileşen arasında iletilen veriler firewall üzerinden geçmediği için, firewall 'İç Hacker' sinyallerin engelleyemez. Bu durum, firewall güvenliğinin, iç saldırganlara karşı etkisiz olduğu, koruma sağlamadığının bir göstergesidir.

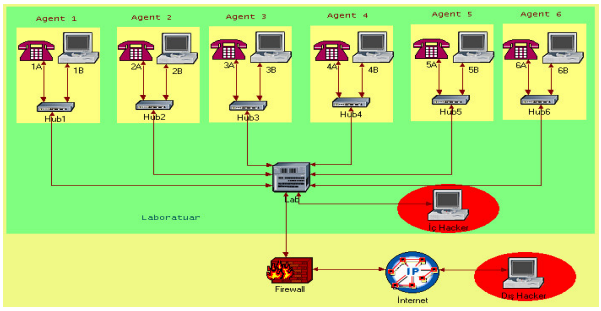


Şekil 11 Firewall İç Hacker Trafiği

4.2 VLAN

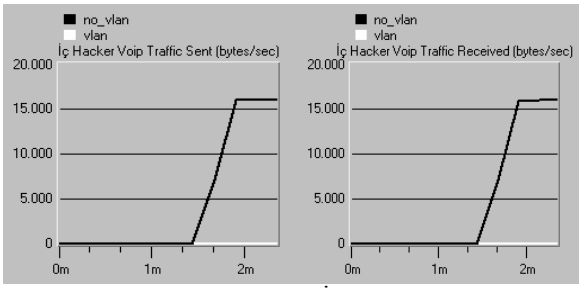
VLAN (Virtual Local Area Network), sanal yerel ağ anlamına gelmektedir. VLAN teknolojisi kullanılarak, bu teknolojiyi destekleyen cihazlar üzerinde mantıksal ağlar oluşturulur.

Sanal yerel alan ağı (VLAN), bir yerel alan ağı (LAN) üzerindeki ağ kullanıcılarının ve kaynakların mantıksal olarak gruplandırılması ve switch (Anahtarlama cihazları) üzerinde portlara atanmasıyla oluşturulur. Sanal ağ kullanılmasıyla, her sanal ağ sadece kendisine ait yayınları (broadcast) alabilir. Bu sayede yayın trafiği azaltılarak bant genişliği artırılmış olur. VLAN tanımlamaları, bulunulan yere, bölüme, kişilere ya da hatta kullanılan uygulamaya ya da protokole göre tanımlanabilir. Sanal ağlar sistem üzerinde uygulanarak, anahtarlama cihazlarından kaynaklanan birçok problem ortadan kaldırılır.



Şekil 12 VLAN Senaryosu

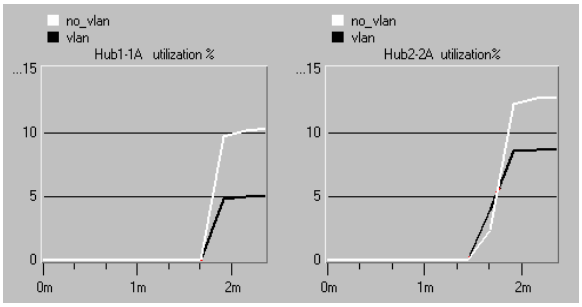
Şekil 12'de Opnet smodelleme programı kullanılarak tasarlanmış bir VLAN senaryosu görülmektedir. VLAN senaryosunda 6 kullanıcı bulunmaktadır. Her kullanıcı bir hub vasıtasıyla merkezi switch'e bağlanır. Switch bir firewall aracılığıyla internete açılır. Merkezi switch'e bir hacker (iç hacker) bağlanmış olup, sistem kaynaklarını kullanmaya yönelik saldırılar düzenlemektedir. Ayrıca başka bir hacker (dış hacker) internet üzerinden laboratuara erişmeye çalışmaktadır. Bu projede, switch üzerinde VLAN kurulu olması ve olmaması durumları ayrı ayrı incelenmiş ve sonuçlar analiz edilmiştir.



Şekil 13 VLAN İç Hacker Trafiği

Şekil 13'de 'İç Hacker'ın her iki senaryodaki veri alışverişi görülmektedir. Buna göre, 'no vlan' adlı senaryoda 'İç Hacker' diğer bileşenlerle veri alışverişinde bulunurken, 'vlan' adlı senaryoda veri iletişimi yapılamadığı görülmektedir. Bunun sebebi, 'İç Hacker'ın bağlı olduğu 14 numaralı portun veri trafiğine kapatılmış olmasıdır. Böylece, sistemin dahili saldırganlara karşı da korunmuş olduğu görülmektedir.

Sanal ağların bir avantajı da, sistemin daha verimli kullanılmasını sağlamasıdır. Bileşenlerin gönderdiği sinyaller, tüm ağa değil, yalnız VLAN tarafından belirlenen portlara iletilir. Şekil 14'de, Vlan ile birlikte, sistemin kullanım oranının düştüğü görülmektedir.



Şekil 14 Veri Hattı Kullanım Oranı

4. SONUÇ

VoIP teknolojisinde bulunan güvenlik açıklarına karşı, birçok güvenlik önlemi bulunmaktadır. Bunlardan bir kısmı sinyalleşmeyi, bir kısmı veriyi korumaya yönelik önlemlerdir. Bu önlemler çeşitli kuruluşlar tarafından tanımlanmakta ve geliştirilmektedir. Bu önlemlerin kullanıcıya yansıyan kısmı, güvenlik teknolojileri olarak karşımıza çıkmaktadır. Güvenlik teknolojilerinden olan firewall ve VLAN teknolojilerinin, uygulama bölümünde Opnet modelleme programı ile benzetimi gerçekleştirilmiştir.

DoS saldırıları sistem kaynaklarını kullanmaya yönelik bir saldırı olduğu gösterilmiştir. Bir saldırı sırasında, veri trafiğinin arttığı belirlenmiştir. Saldırı sırasında veri trafiğinin artmasıyla birlikte, sunucuların yanıt süreleri artmaktadır. Bu durum, DoS saldırılarının sistemi yavaşlattığını göstermektedir. Saldırganın, sisteme etkisi gönderdiği sinyal boyutu ile doğru orantılı olarak değişmektedir. Büyük çapta saldırılar, sistem kaynaklarının büyük kısmını saldırganın kullanmasına neden olabilir. Saldırganlar, sistemin fazla çalışması sonucunu doğuracağından, işlem kapasitesi artar. Bu durum işlemcilerin çalışma oranını artırır. DoS saldırılarının işlemci kullanım oranlarını olumsuz yönde etkilediği görülmektedir.

DoS saldırısı sonucu sistem olumsuz yönde etkilenmiş, sistem kaynakları saldırgan tarafından kullanılmış, sistem yavaşlamış, ancak kullanıcılar hizmet almaya devam edebilmişlerdir. Bu durum güvenlik kriterlerinde belirtilen 'erişilebilirlik' ilkesine uygundur. Yani, sisteme bir saldırı olması durumunda dahi, kullanıcılar hizmet almaya devam edebilmektedirler.

Bir firewall, üzerinden geçen trafiği engelleyebilir. Saldırganların erişmesinin istenilmediği bir uygulama, firewall kullanılarak güvenli hale getirilebilir. Saldırgan tarafından gönderilen sinyaller, firewall tarafından etkisiz hale getirilir. Bu nedenle dış saldırganlara karşı firewall kullanılmalıdır.

Firewall yalnızca üzerinden geçen trafiği kontrol edebildiği için, sistem içerisindeki yerel ağlarda bulunan saldırganlara karşı, koruma sağlayamaz. Güvenlik duvarları, dahili saldırganlara karşı etkisizdir.

VLAN tanımlamaları sırasında erişime engellenen portlardan veri transferi yapılamamaktadır. Bu nedenle sistemde tanımlı olan kullanıcılar haricindeki portlar veri trafiğine kapanarak, saldırganların sisteme erişmeleri engellenir. Sanal ağlar, sistemde daha az yayın (broadcast) yapıldığı için, iletim hatlarının kullanım oranı düşer. Bu durum sistemin daha verimli çalışmasını sağlamaktadır.

KAYNAKLAR

[1] Z. Baharlooei, M. Hashemi, "A Low Cost Voip Architecture For Private Network" International Conference on Future Networks 2009.

[2] P. Hung, M. Martin "Security Issues In VoIP Applications" Electrical and Computer Engineering,. CCECE '06. Canadian Conference, 2006.

[3] İnternet: http://www.opnet.com/university_ program /participant_spotlight/universities. html, 2009.

[4] İnternet: http://www.mm.anadolu.edu.tr/eee/Pc %20Lab.html 2009.

[5] İnternet: http://netlab.boun.edu.tr/projects/ projects.htm, 2009.

[6] İnternet: http://fens.sabanciuniv.edu/telecom/eng/software/OPNETatSabanciUniversity/OPNET_TE404.htm , 2009.

[7] S. Pandey, "Secure Localization and Node Placement Strategies for Wireless Networks" Doctor of Philosophy Thesis, Auburn University,2007.

[8] H. Qu, "Integrated Wireless-Based Information Processing And Communications For E-Healthcare System: Design, Analysis, Optimization And Resource Protection" Doctor Of Philosophy Thesis, Wayne State University, 2007.

[9] M. A. Almashari, "An Analytical Simulator for Deploying IP Telephony" Master of Science Thesis, King Fahd University 2006

[10] R. R. Sakhardande "The Use Of Modelling And Simulation to Examine Network Performance Under Denial Of Service Attacs" Master of Science Thesis, State University NY 2008.

[11] S. Basavanatha, "Simulationof Voice Over Internet Protocol Service Performance when Overlaid with Background Traffic Over a Local Area Network, Master of Science Thesis, California State University 2008

[12] M. Garuba, J. Li, Z Yi "Security in the New Era of Telecommunication: Threats, Risks and Controls of VoIP" IEEE Fifth International Conference on Information Technology: New Generations 2008.
[13] P.C. K. Hung, M.V Martin "Security Issues In VoIP Applications" Electrical and Computer Engineering, 2006. CCECE '06. Canadian Conference on May 2006
[14] P. Thermos, A. Takanen, **"**Securing Voip Networks"**,** Pearson Education, Inc., Massachusetts, USA, 2008.
[15] T. Porter, B. Baskin, L. Chaffin, M. Cross Jr.J. Kanclirz, A. Rosela, C. Shim, A. Zmolek, "Pratical VoIP Security", Syngress Publishing, Inc., Canada, 2006.
[16] A. Luthra, W. Ashraf, "Security in VoIP Systems", Master's Thesis, Technical University of Denmark, 2005.