Güvenli VoIP Hizmetleri için Mevcut ve Yeni Yaklaşımlar

H.Hakan Kılınç, Uğur Cağal

Netaş, Siber Güvenlik Birimi, İstanbul

hakank@netas.com.tr, ucagal@netas.com.tr

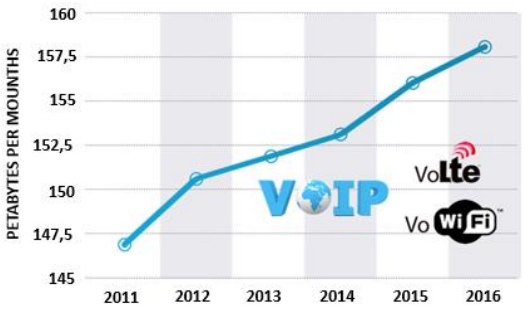
Özet: Telekom teknolojisinde, 4G günleri yaşanmakta ve 5G için hazırlıklar yapılmaktadır. Teknolojideki nesil değişimi ve IPv6'nın yaygınlaşması VoIP'in kullanımı arttırmıştır. Bu artışa paralel olarak birçok dolandırıcılık ve zafiyetlere maruz kalınmaktadır. Bu yüzden, VoIP sistemlerin açıklıklarını bulmak, bu sistemlere yönelik tehditleri tespit etmek ve onları korumak için uygulama katmanı seviyesinde derinlemesine paket analizi yapan güvenlik ürünlerine ihtiyaç vardır. Bununla birlikte, e-posta ve web gibi hizmetlerin aksine, VoIP hizmeti zaman duyarlıdır. Karmaşık ve zaman alıcı güvenlik mekanizmaları, VoIP için uygun değildir. Çalışmamızda, VoIP güvenlik problemlerine yönelik mevcut ve olması gereken yeni güvenlik yaklaşımlarını tartıştık.

Anahtar Sözcükler: VoIP, SIP, Güvenlik Tehditleri, Güvenlik Ürünleri, DoS/DDoS, VoIP IDS (Intrusion Detection System), VoIP IPS (Intrusion Prevention System), VoIP Firewall, VoIP Security Scanner.

Abstract: The current telecom technology uses 4G and preparations are being made for 5G. Technological generation change and the expansion of IPv6 have increased the use of VoIP. In parallel to this increase, many frauds and weaknesses are realized. There is a growing need for security products that have in-depth packet analysis capabilities in application layer in order to find the vulnerabilities of VoIP systems, to detect attacks against these systems and to protect them. However, unlike services such as e-mail and web, VoIP services are time-sensitive. Complex and time-consuming security mechanisms are not suitable for VoIP. In our study, we discuss existing and new security approaches for VoIP security issues.

1. Giriş

Düşük maliyet ve zengin servisler sunan IP (Internet Protocol) üzerinden ses ve multimedya iletişim teknolojisi VoIP (Voice over Internet Protocol), IP alt yapı teknolojilerin gelişmesiyle hızla yaygınlaşmaktadır. VoIP, geleneksel telekom teknolojisi olan PSTN (Public Switched Telephone Network)'e göre birçok avantaja sahiptir ve VoIP servisleri, PSTN networklerin önemli bir rakibi olmuştur. Şekil 1'de, veri boyutu, aya göre petabytes cinsinden verilen VoIP servis trafiği göstermektedir ki, günden güne VoIP trafiği artmaktadır. 4G LTE teknolojisi ile gelen, VoLTE (Voice over LTE) ve VoWIFI (Voice over WIFI) teknolojileri ile VoIP trafiği daha da artacaktır.



Şekil 1. VoIP Servis Trafiğinin Yıllara Göre Veri Boyutu [1]

IP üzerinden iletişimin güvenlik zafiyetlerini barındırması ve internetin tüm güvenlik problemlerini miras alması nedeniyle yeni nesil telekom teknolojilerin de güvenlik önem arz etmektedir. VoIP tarafındaki güvenlik zafiyetlerine örnek olarak, VoIP trafik hırsızlığı, altyapıların izinsiz kullanımı, ücretsiz servislere istem dışı aramalar, ses kalitesinin bozulması, servisleri işlev dışı bırakılması, sisteme sahte kayıt, servis hırsızlığı, dinleme, spam, virüs, bilgi çalma, VoIP trafiğini yönlendirme gibi problemler örnek olarak verilebilir. 2013 yılında Communications Fraud Control Association tarafından yayınlanan "Global Fraud Loss Survey" raporuna göre, VoIP ağlarına saldırı zararı 3,62 milyar $'dır[2]. Bununla birlikte, kayıtlara girmemiş dolandırıcılığın boyutu bu rakamların çok üzerindedir.

Bu zararlar, VoIP ve UC sistemlerine yönelik atakların sonucudur. Hacker ataklarının %25'i VoIP ve UC (Unified Communication) sistemlerine yönelik olup bu sistemlere karşı 20,000'den fazla exploit (açık) ve tehdit tanımlanmıştır [3]. Gerçekleştirmesi kolay ve oldukça karlı bir tehdit olan ücret sahtekârlığı (toll fraud), telekom dünyasındaki en yaygın suçlardan biridir.

VoIP altyapısına yönelik atakların çoğu, sinyalleşme teknolojileri üzerinden gerçekleşir. SIP (Session Initation Protocol), VoIP haberleşmesi için kullanılan, VoIP bileşenleri arasında oturumları kurmak, değiştirmek ve sonlandırmak amacıyla kullanılan metin tabanlı en yaygın sinyalleşme protokolüdür [4]. Kullanım esnekliği ve ölçeklenebilirliği sayesinde, IMS (IP Multimedia Subsystem) ve VoLTE teknolojilerinin sinyalleşme protokolü olarak SIP benimsenmiştir [5]. SIP, önemli avantajlar sunuyor olsa da, birçok farklı güvenlik tehditlerine maruz kalmaktadır [6] [7] [8] [9].

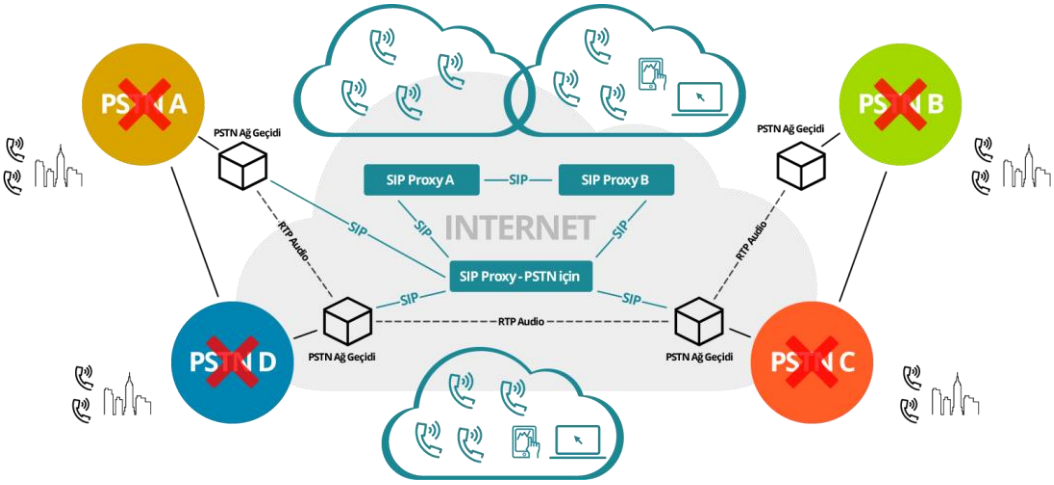
Bu makale de, Bölüm 2'de yeni telekom altyapılarının bir özetini verdikten sonra, Bölüm 3'de, VoIP güvenlik problemlerinden bahsederek mevcut ve yeni güvenlik çözümleri açıklanacaktır. Bölüm 4'de verilen öneriler ile sonuçlandırılacaktır.

2. Yeni Telekom Altyapısı ve VoIP

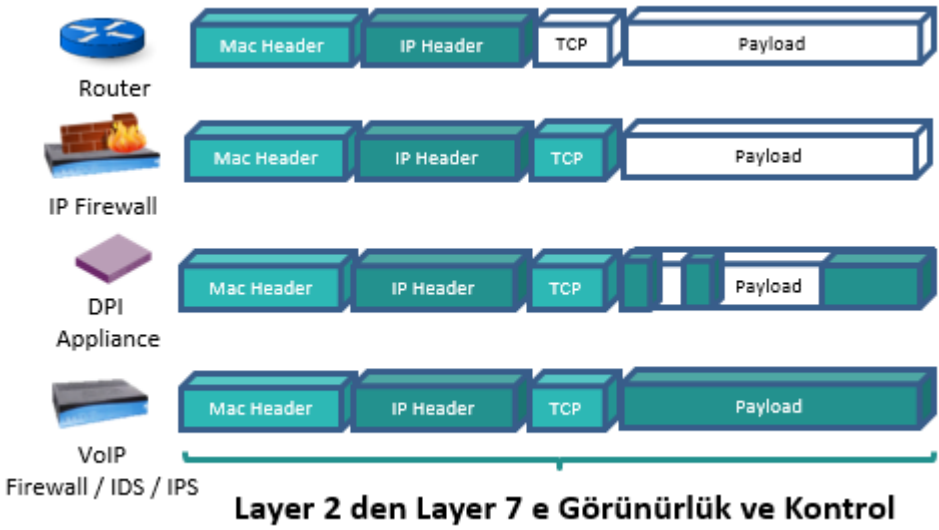
Geleneksel telekom altyapısı, PSTN adı verilen devre anahtarlama (circuit switching) yönteminin kullanıldığı sabit ses hizmeti sunan bir altyapıdan oluşmaktadır. Yeni telekom altyapısını oluşturan VoIP ise, ses iletişim altyapısı olarak internet ağını kullanmaktadır. Ses, internet üzerinde veri taşıma metodu olan paket anahtarlama (packet switching) yöntemi ile taşınmaktadır.

Şekil 2'de gösterildiği gibi yeni telekom altyapısında, PSTN ağlar yerini VoIP ağlara ve ağ bileşenlerine bırakmaktadır. Bu değişim, önce hibrit bir yapıya bürünmekte, sonra ise tamamen VoIP olacak şekilde gerçekleşmektedir. Hibrit yapı da, genelde kurum içerisinde VoIP altyapısı kullanılmakta iken kurum dışına çıkarken PSTN ağ kullanılmaktadır. Türkiye'deki yapı için hibrit yapı diyebiliriz. Telekom omurga yapısı tamamen IP'ye kaynakta ve PSTN yapıdan uzaklaşmaktadır. Gelecek teknolojilerden 4G LTE tamamen IP tabanlı olup IPv6 ile de daha da gelişecektir.

VoIP, veri, ses ve video gibi paket anahtarlamalı servisler için, tek bir geniş bant devresini kullanabilir. Birçok kurumda, VoIP hizmeti, var olan veri ağı içerisinde kullanılır. Bu kullanım, maliyetleri azaltırken, daha fazla performans ve güvenlik ihtiyaçları anlamına gelir. Bütünleşik bir sistem, çağrı kalitesini korumak için hizmet kalite (QoS) sürecini ve güvenlik sürecini önemli hale getirir [10].



Şekil 2. Yeni telekom altyapısı



Şekil 3. Güvenlik Ürünleri ve Paket Analiz Düzeyleri

3. VoIP Güvenlik Problemleri ve Çözüm Yaklaşımları

Telefon ağları, her zaman hackerların (bilgisayar korsanları) hedefi olmuş ve 1970/80'li yıllarda, telefon korsancılığı eylemi anlamına gelen "Phreaking" yaygınlaşmıştır. Genelde amaçları, ücret sahtekârlığı ve ücretsiz şehirlerarası hizmet almaktır. PSTN ağların güvenlik problemleri olan çağrı yönlendirme ve kanunsuz dinleme gibi eylemler gerçekleştirilmiştir. VoIP telefonculuğu da, bu tip problemlere ek olarak internetten miras olarak gelen güvenlik problemleriyle yüz yüzedir.[10]

Bazı VoIP güvenlik problemleri ve önlemlerini aşağıdaki gibi 5 sınıf altında açıklayabiliriz. Açıklamalar sırasında Şekil

3'ten faydalanacağız. Şekil 3, hem bazı problemleri hem de çözümleri tüm açıklığı ile göstermektedir. Yukarıda da bahsedildiği gibi, VoIP altyapısına yönelik atakların çoğu, sinyalleşme teknolojileri üzerinden gerçekleşir. Bunun içinde, paketlerdeki payload kısmının incelenmesi gerekmektedir.

I. Problem: VoIP Trafik Hırsızlığı ve Ücret Sahtekârlığı

VoIP servis sağlayıcı ve müşterilerinin geçmişten buyana maruz kaldıkları tehditlerin başında gelir.

Mevcut Çözüm Yaklaşımları: Birçok santral bu problemi adreslemek için sınıf sınırlandırma ve yetki kodları kullanma gibi özelliklere sahiptir. Sınıf sınırlandırma ile bazı telefon numaraları kısa mesafe veya uzun mesafe gibi özelliklere göre sınıflandırılır ve bu sınıflara arama sınırlandırmaları getirilir. Diğer yaklaşım ise yetkilendirme kodları kullanarak arama yapmadan önce kod girmesi beklenir. Her iki yaklaşımında yönetimi ve bakımı zordur. Yetki kodları kolayca elde edilip paylaşılabilmektedir.

Yeni Çözüm Yaklaşımları: Yeni yaklaşımda, sistemin her zaman takip edilmesinin, sistem kullanıcılarının tanımladığı politika ve kurallara göre belirlenen parametreleri (çağrı sayısı, çağrı süresi, birikimli çağrı süresi) temel alarak eşik değerini aşan çağrıların tespit edilmesi ve önlenmesinin sağlanmasıdır. VoIP IDS ve VoIP IPS adı verilen normal çağrı deseninin dışındaki çağrıları tespit eden ve önleyen ürünler kullanılmaktadır.

II. Problem: VoIP Trafiği ve Ağ Güvenliği

İkinci problem, VoIP trafiğinin, internet trafiği ile birlikte olması ve VoIP güvenliğinin temel ağ güvenliği kadar güvenilir olması olarak ifade edilebilir.

Mevcut Çözüm Yaklaşımları: İnternet üzerinden trafik yönlendirme, geleneksel devre anahtarlamalı ağlar üzerinden yapılan yönlendirmelere benzerdir. Paket dinleyiciler (packet sniffer), kolaylıkla şifresiz trafiği yakalayabilir. Bu problemin üstesinden gelmek için, sanal özel ağlar (VPN) kullanılır. Bu çözüm iyi çalışmakla birlikte, çağrı alırken ve yaparken ortam kurulumu biraz zaman alabilir ve trafik şifreleme/çözme işlemleri VoIP paket gecikmelerine sebep olur. VPN çözümlerinin genelde donanım tabanlı olması da ikinci bir sınırlamadır.

Var olan bir ağda bir güvenlik açığı var ise, bu açık, ağ üzerine kurulu VoIP altyapısı için de bir istismar kaynağıdır. Bu endişeleri gidermek için, bağımsız güvenlik denetlemeleri yaptırmak, güvenlik duvarı yapılandırmaları yapmak, yama prosedürleri uygulamak ve periyodik log kaydı kontrolleri yapmak tavsiye edilir.

Yeni Çözüm Yaklaşımları: Yeni yaklaşımlarda da, VPN kullanımı tavsiye edilmekle birlikte yeterli değildir. VPN üzerinde yeni açıkların keşfedilmesi ve VPN'nin kullanıldığı uç noktaların güvenliği konusunda bir garantinin sağlanmaması, VPN yanında VoIP'e özel güvenlik duvarı ihtiyacını zorunlu kılmaktadır. Niçin VoIP güvenlik duvarı sorusunun cevabı olarak, Ağ/IP güvenlik duvarları, Şekil 3'de de gösterildiği gibi paketin payload denilen kısmı incelememesi şeklinde verilebilir.

Bağımsız güvenlik denetimleri yaptırmak her zaman olması gerekmesinin yanında, VoIP'e özel tehditlerin de tespit edilebilmesi ve çözümler sunulması beklenmelidir. Yama prosedürlerini

uygulamak ve takip etmek zordur. Özellikle VoIP telefonların yamalarını tespit edebilecek araçlar kullanılmalıdır. Hem güvenlik denetimleri hem de yama problemlerinden kaynaklanabilecek zafiyetleri tespit eden VoIP Security Scanner adı verilen VoIP zafiyet analiz araçları kullanılmaktadır.

Periyodik log kayıt kontrolleri, güzel bir yaklaşım olmakla birlikte, genelde iş işten geçtikten sonra incelenir ve bu ise sonraki problem çözümleri için kullanılır. Yeni yaklaşımda, anlık veri analizi yapan ürünler öne çıkmaktadır. Bunun içinde, VoIP Firewall, VoIP IDS ve VoIP IPS ürünleri kullanılır.

III. Problem: Kötü niyetli çağrılar, DoS ve DDoS atakları

Üçüncü problem, hizmet engellemeye yönelik DoS ve DDoS (Distributed Denial of Service) atakları, telefon görüşmesine engel olurlar, Aynı şekilde, otomatik çağrı üreticilerle yapılan ataklarla VoIP sistemleri cevap veremez hale getirilebilir.

Mevcut Çözüm Yaklaşımları: Kutu olarak gelen birçok VoIP kurulumunda yeterince izlenemeyen ve gereksiz yere açık bırakılan TCP/UDP portları bulunabilir. Böyle bir ortam, DoS ve DDoS atakları için uygun bir ortamdır. Örneğin, bir VoIP altyapısında, sinyalleşme için 5060 ve 5061 portlarını açmak gerekirken ses paketleri için birçok portu açmak gerekmektedir. Bu saldırılarla mücadele etmek için gereksiz port ve hizmetlerin kapatıldığından emin olmak ve yeni keşfedilen güvenlik açıkları için hızlıca yama oluşturmak gerekir.

Önceden kaydedilmiş, istenmeyen mesajlar içeren aramalara, SPIT (Spam over IP Telephony) aramalar denir. SPIT aramalar, DoS atakları ve kaynakların (bant genişliği gibi) izinsiz kullanımı gibi tehditleri içerir. SPIT ile mücadele, SPAM ile mücadeleye benzer ve klasik güvenlik araçları ile durdurmak mümkün değildir.

Yeni Çözüm Yaklaşımları: VoIP sinyal ataklarını önlemenin anahtarı, güçlü bir kimlik tanıma protokolünü hayata geçirmektir. Bu yaklaşım, kurum içi özel kullanım şeklinde olabilir ama genele uygulamak mümkün olmayabilir. Normal trafik desenini gözlemleyerek medya ve sinyal limitlerinin belirlendiği ve konfigüre edildiği ürünler kullanılmalıdır. Bu şekilde, normal olmayan trafiğin adresleri bloklanabilir. Fakat bu bloklama, VoIP sistemlerinde farklı şekilde hayata geçirilmelidir. Bir IP adresini bloklamak, tüm bir kurumun devre dışı kalmasına sebep olabilir. Bu yüzden, bloklama işlemi "kullanıcı-IP adresi-port" üçgeni gözetilerek yapılmalıdır. Bu yaklaşımın yanında akıllı DDoS denilen, eşik değeri tespit edilmiş bir sisteme yapılan ve eşik değerinin hemen altında birçok defa yapılan saldırıların da tespit edilmesi gerekmektedir. Bu tespit için, istatistiki yaklaşımları kullanan ürünlere ihtiyaç vardır. Bu tür problemlere göre geliştirilmiş VoIP Firewall, VoIP IDS ve VoIP IPS ürünleri kullanılabilir.

IV. Problem: Çağrıların dinlenmesi

VoIP ve SIP ile ilgili çözülemeyen veya çözümü basit olmayan birçok problem vardır. İlgili teknoloji ve protokollerin kullanımı büyümeye devam ettikçe zayıflıkları ve açıklıkları da büyümeye devam edecektir. Çözümü basit olmayan problemlerden biri de çağrıların izinsiz dinlenmesidir.

Mevcut Çözüm Yaklaşımları: Ağ üzerinden akan trafik paketlerini yakalayan ve dinlemek için ses dosya formatına çeviren VoMIT, SIPtap,

Wireshark, Voipong, Cain&Abel gibi onlarca uygulama bulunmaktadır [11]. Bu tip uygulamalar, sadece ses paketlerini değil sinyalleşme sırasında kullanılan bilgileri de (çağrı ID, çağrı kaynağı, çağrı hedefi, süresi ve zamanı) elde ederler.

Çağrıları dinlemeyi önlemenin tek metodu, çağrı için güvenli bir kanal kurmak ve ses verisini şifrelemektir.

Yeni Çözüm Yaklaşımları: İki uç nokta arasında hem kimlik tanıma hem de ortak anahtar üzerinde anlaşma protokolleri geliştirilmelidir. Oluşturulan ortak anahtar ile ses paketleri de arada kimse olmaksızın şifrelenebilir ve çözümlenebilir. Tabii ki, şifreleme kurulum işlemleri ve metotları da, performans bakış açısından geçirildikten sonra uygulanmalıdır. [9]

Araya giren kişileri tespit etmek için trafik verisi üzerinde bir anormal durum kontrolü yapılabilir. Olması gerekenden fazla bir paket akışının tespit edilebilmesi gerekir. Örneğin, VoIP sistem üzerinde, o anda 10 adet çağrı var ise en kaliteli çağrı kodekslerinin kullanıldığı varsayıldığında yaklaşık 160 Kilobaytlık bir trafik anlamına gelir. Fakat sistem üzerinde 300 Kilobaytlık bir trafik var ise anormal durumlar var anlamına gelir. Bu anormal durumun tespit edilebilmesi gerekir. Bunun için de bu durum tespit özelliğine sahip VoIP IDS araçları kullanılabilir.

V. Problem: Kuruma özel politikaların uygulanamaması ve operasyon yönetimi

Bazı durumlarda, bazı telefon çağrılarının daha öncelikli olması gerekebilir veya bazı telefon numaralarının bazı telefon numaralarını aramaması istenebilir veya kurumun bir ofisinde bulunan telefon cihazının başka bir ofisinde kullanılmaması istenebilir. Benzer durumların ve telefon cihaz güncellemelerinin yönetilmesi gerekebilir. VoIP sistemlerinde istenebilecek bu gibi durumları gerçekleştirmek için klasik güvenlik ve operasyon uygulamaları kullanmak zordur veya imkânsızdır.

Mevcut Çözüm Yaklaşımları: İstenilen operasyonları gerçekleştirmek için kullanılan IP PBX santralın varsa özellikleri kullanılır. Telefon cihaz güncellemeleri için ise cihaz üzerinde bulunan TFTP gibi ilkel dosya transfer uygulamaları ile halledilemeye çalışılır. Bu yaklaşım, bilgisayar korsanları tarafından her türlü dosyanın cihaza yerleştirmesine izin verebilir.

Yeni Çözüm Yaklaşımları: Kuruma özel politika ve kuralların VoIP çağrılarına uygulanabilmesi gerekmektedir. Gerekirse sinyalleşme paketleri seviyesinde buna ihtiyaç olabilir. Bu ihtiyaçlar için politika ve kural tabanlı altyapıya sahip paket seviyesinde kural oluşturabilme yeteneğine ve raporlayabilme yeteneğine sahip VoIP firewall kullanılabilir. Yama durumlarını takip için VoIP Zafiyet Analiz araçları ve dosya güncellemeleri için de VoIP firewall kullanılabilir.

4. Öneriler ve Sonuç

Güvenli bir VoIP altyapısını oluşturmak, güvenlik açıklarının tespiti ve çözümlerinin raporlanması ile başlar. Bununla birlikte, sistemdeki güvenlik açıklarını bulmak ve bu açıkları kapatacak çözümler sunmak zordur. Bunun için, VoIP için özelleşmiş zafiyet analiz araçları kullanılabilir ve mantıksal hataları tespit edebilecek VoIP güvenlik uzmanlarından faydalanılabilir.

İkinci olarak, ses trafiğinde gecikmeye sebep olmadan, derinlemesine anlık veri analizi yaparak anomali ve atak tespiti yapan ve bu atakları önleyen, akıllı ve bilinmeyen ataklara karşı dinamik kural

oluşturma ve filtreleme özelliğine sahip VoIP Firewall ürünleri kullanılabilir. Uygulama katmanı seviyesi analizi ile hem bilinen atakların tespitini yapabilirler hem de mesaj silsileleri ile durum analizi yaparak bilinmeyen atakların oluşturacağı anormal durumları tespit ederek önlemini alırlar. Ağ güvenliğinin yanında, kötü niyetli servis kullanımı ve çağrıları önlemesi, anlık vereceği alarmlar ile daha büyük zararlardan koruyacaktır.

Üçüncü olarak, VoIP trafik yönlendirme ve ücret sahtekârlığının önüne geçecek, sosyal mühendisliği tespit edecek ve operasyonel yönetime katkı sağlayacak VoIP IDS ve VoIP IPS ürünlerinden faydalanılabilir.

Son olarak, geleneksel veri ağlarındaki güvenlik önlemleri, VoIP dünyasına uygulanamaz. Performans problemine sebep olmadan, zaman kritik veri üzerinde çalışan uygulamaların olması gerekmektedir.

Kaynaklar

[1] Data volume of global VoIP service traffic from 2011 to 2016 (in petabytes per month), http://www.statista.com/statistics/267183/forecast-for-the-worldwide-voip-traffic/ (Erişim Tarihi: 17.10.2015)

[2] Global Fraud Loss Survey, http://cfca.org/pdf/survey/Global%20Fraud_Loss_Survey2013.pdf, (Erişim Tarihi: 17.10.2015)

[3] Securing UC: There are Ways, but Where's the Will? http://www.nojitter.com/blog/230600035/securing-uc-there-are-ways-but-wheres-the-will (Erişim Tarihi: 17.10.2015)

[4] Rosenberg J., Schulzrinne H., Camarillo G., Johnston A., Peterson J., Sparks R., Handley M., Schooler E., "SIP: Session Initiation Protocol," Internet Engineering Task Force, RFC 3261, 2002.

[5] Camarillo G., Garca-Martn M.-A., "The 3G IP Multimedia Subsystem (IMS): Merging the Internet and the Cellular Worlds", Second Edition. WILEY, 2006.

[6] Geneiatakis D., Dagiouklas A., Kambourakis G., Lambrinoudakis C., Gritzalis S., Ehlert S., Sisalem D., "Survey of Security Vulnerabilities in Session Initiation Protocol," IEEE Commun. Surveys Tutorials, vol. 8, no. 3, pp. 68–81, 2006.

[7] Geneiatakis D., Lambrinoudakis C., Kambourakis G., "An Ontology Based-Policy for Deploying Secure SIP-based VoIP Services," Elsevier Computer and Security, vol. 27, no. 7-8, pp. 285–297, 2008.

[8] S. Salsano, L. Veltri, and D. Papalilo, "SIP Security Issues: The SIP Authentication Procedure and its Processing Load," IEEE Network, vol. 16, no. 6, pp. 38–44, 2002.

[9] Kilinc, H.H., Yanik, T., "A Survey of SIP Authentication and Key Agreement Schemes," in Communications Surveys & Tutorials, IEEE , vol.16, no.2, pp.1005-1023, 2014.

[10] Ruck, M., "Top Ten Security Issues with Voice over IP (VoIP)", http://www.designdata.com/wp-content/uploads/sites/321/whitepaper/top_ten_voip_security_issue.pdf, (Erişim Tarihi: 29.10.2015)

[11] VoIP Security Tool List, http://www.voipsa.org/Resources/tools.php#VoIP%20Sniffing%20Tools, (Erişim Tarihi: 31.10.2015)