SIP Kayıt Silme Saldırısı Anatomisi ve Savunma Stratejileri

Anatomy of SIP Registration Removal Attack and Defense Strategies

İsmail Melih Taş, Onur Özbirecikli, Uğur Çağal, Erhan Taşkın
Güvenlik ARGE Departmanı
NETAŞ Telekomünikasyon A.Ş.
İstanbul, Türkiye
{meliht,onuroz,ucagal,etaskin}@netas.com.tr

Hüseyin Taş
Bilgisayar Programcılığı Bölümü
İstanbul Gelişim Üniversitesi M.Y.O.
İstanbul, Türkiye
htas@gelisim.edu.tr

***Özetçe*—VoIP ve SIP teknolojileri, son yıllarda oldukça popüler olmaya başlamıştır. Gelecek iletişim teknolojisi öngörülerinde SIP uygulamalarının, önemli bir yere sahip olacağı şüphesizdir. Bu popülerliğin artması ile VoIP/SIP dünyasında güvenlik teknolojileri henüz TCP/IP dünyasındaki kadar olgunlaşmamış ve bilinmemektedir. Bu nedenlerden dolayı hem ticari hem de akademik anlamda mevcut VoIP/SIP güvenlik teknolojilerinin araştırma geliştirme çalışmalarına ağırlık verilmesi oldukça önem taşımaktadır.**

Bu çalışmada yeni nesil haberleşme ortamı olarak bilinen Tümleşik Haberleşme (UC) sistemlerinde kullanılan Oturum Başlatma Protokolü'nün (SIP) SIP kayıt (register) mekanizmasına yönelik sinyalleşme zafiyetleri hakkında bilgiler verilmiştir. VoIP güvenlik laboratuvar ortamında gerçekleştirilen kayıt (registration) silme saldırısı ile ilgili saldırı sonuçlar paylaşılıp, saldırı anatomisi ve bu saldırı tipine yönelik savunma stratejilerinden bahsedilmiştir.

Anahtar Kelimeler — SIP; kayıt silme saldırısı; tümleşik haberleşme; sinyalleşme manipülasyonu

***Abstract*—This Popularity of VoIP and SIP technologies has been started at last years. SIP applications will have an important place in the future. VoIP/SIP security technologies are not known as much as TCP/IP's security world. Hence, VoIP/SIP security technologies, developments and researches are very important for academic and commercial.**

In this study, signaling vulnerabilities of registration mechanism in Session Initiation Protocol (SIP) which is used in next generation communication environment known as Unified Communications (UC) systems has been mentioned. The results of registration removal attack which has been carried out at VoIP security laboratory environment are shared, anatomy of attack and the defense strategies for that attack type are mentioned.

Keywords — SIP; registration removal attack; unified communication; signaling manipulation.

978-1-4799-4874-1/14/$31.00 ©2014 IEEE

I. GİRİŞ

Oturum Başlatma Protokolü (SIP Initiation Protocol), IETF tarafından IP üzerinden çoklu ortam görüşmesi yapabilmek için bir standart olarak oluşturulmuştur. SIP, iki veya daha fazla katılımcı arasındaki çoklu ortam (multimedia) oturumlarının kurulması, yürütülmesi ve sonlandırılması işlemlerini gerçekleştiren bir sinyalleşme kontrol protokolüdür [1].

VoIP ve SIP teknolojileri, son yıllarda oldukça popüler olmaya başlamıştır. Gelecek iletişim teknolojisi öngörülerinde SIP uygulamalarının, önemli bir yere sahip olacağı şüphesizdir. Bu popülerliğin artması ile VoIP/SIP dünyasında güvenlik teknolojileri henüz TCP/IP dünyasındaki kadar olgunlaşmamış ve bilinmemektedir. Bu nedenlerden dolayı hem ticari hem de akademik anlamda mevcut VoIP/SIP güvenlik teknolojilerinin araştırma geliştirme çalışmalarına önem verilmesi oldukça önemli değer taşımaktadır. SIP protokolünün sinyalleşme

manipülasyonu saldırılarına karşı zafiyeti bulunmaktadır [1].

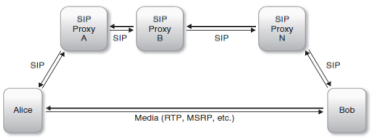
VoIP güvenlik laboratuvar ortamındaki VoIP ağı üzerinde temel SIP sinyalleşmesi ile kayıt olma, temel oturum başlatma ve sonlandırma işlemleri gerçekleştirilmiş ve daha sonra hazırladığımız zararlı bir kod parçası kullanılarak kayıt olan bir kullanıcının isteği dışında habersizce kaydı silinerek bu kullanıcının olağan çağrıları alması engellenmiştir. Buradaki zararlı kod parçası, SIP kayıt mekanizmasındaki manipülasyon zafiyetini kullanacak şekilde hazırlanmıştır. Bu çalışma yapılırken test ortamında SIP PBX olarak Linux tabanlı Trixbox PBX, istemci (client) olarak Zoiper yazılımsal istemci ve Polycom IP telefon kullanılmıştır. Zararlı kod, güvenlik testleri amaçlı kullanılan Linux tabanlı Kali işletim sistemi üzerinden çalıştırılıp Trixbox PBX' e hileli paket yollayacak şekilde tasarlanmıştır.

Bu çalışmada, SIP kayıt mekanizmasının zafiyetlerine yönelik olarak kayıt silme saldırısının anatomisi ele alınmış ve bu saldırıya özel savunma stratejilerinden bahsedilmiştir.

II. SALDIRININ ANATOMİSİ

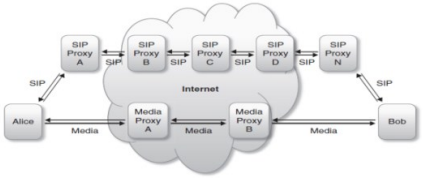
A. *SIP Tabanlı Tümleşik Haberleşme Sistemlerinin Yapısı*

Şekil 1'de görüldüğü gibi sinyalleşme mesajları birkaç Proxy (vekil sunucu) üzerinden iletilirken medya iletimi direk olarak uçtan uca gerçekleşebilmektedir.



Şekil 1. Sinyalleşmenin ve medya akışının farklı yollardan gerçekleşmesi[3].

Bir kurumda bulunan UC sistemde SIP sinyalleşmesi tek bir sunucu üzerinden olacağı gibi çok daha karmaşık bir şekilde, birçok sunucu üzerinden de iletilebilir. Bu durum Şekil 2'de gösterilmiştir.



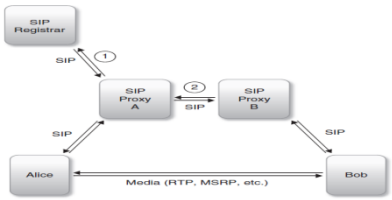
Şekil 2. Çok sayıda proxy sunucusu içeren UC sistemi[3].

B. *SIP Kayıt Mekanizması*

Bir SIP kullanıcısı çağrı başlatmadan önce sistem sunucusuna bir REGISTER mesajı yollamaktadır. Bu mesaj ile sunucu kullanıcının ID, IP adresi, alan adı gibi bilgilerini kaydetmektedir. Bu kayıt bilgileri belli bir süre sonra silinmektedir.

Saldırgan hileli REGISTER mesajı yollayarak aşağıdaki kötü niyetli işlemleri yapma girişiminde bulunabilmektedir:

- Kayıt girişi silinmesi
- Farklı bir hedefin kaydedilmesi

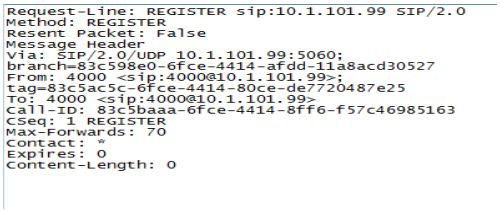


Şekil 3. SIP kayıt (register) işlemi[3].

C. *Kayıt Silme ve Manipülasyonu*

Tipik bir kurumsal ses haberleşme sistemi konuşlandırmasında da, SIP telefonlar kendilerini SIP proxy üzerinden kayıt ederler ve böylece SIP proxy gelen çağrıları nereye yönlendireceğini bilir. SIP telefonlar, yeniden başlatıldıklarında veya varsayılan olarak belirlenmiş ya da sonradan ayarlanmış belirli süre aralıklarında kendilerini kayıt ederler. Bu çalışma boyunca test ettiğimiz SIP telefonların hepsinde varsayılan olarak kayıt yenileme süre aralığı (registration interval) 3600 saniye (60 dakika) olarak görülmüştür, ancak bu zorunluluk değildir. Farklı üreticilerin SIP telefonları varsayılan olarak farklı değerlerde ayarlanmış olabilmektedirler. Ek olarak SIP proxy'ler talep edilen kayıt yenileme süre aralığı değerini 200 OK mesajı içinde değiştirebilmektedirler. SIP telefonlar SIP proxy'den gelen talimat ile bu değeri kayıt yenileme süre aralığı olarak kullanmalıdır.

Eğer kayıt silinmiş ya da gasp edilmiş ise, SIP telefon çağrıları alamaz. Kaydı silmek, SIP telefonun çağrı yapma yetkinliğini etkilemez. Aşağıdaki gibi bir REGISTER isteği gönderilerek, bir SIP telefon için tüm kayıtlar silinebilir (Şekil 4).



Şekil 4. Kayıt silmek için gönderilen SIP mesaj içeriği [2].

Buradaki kilit değerler; Contact: * ve Expires: 0 değerleridir. Bu değerler, SIP proxy'deki SIP telefon için tüm kayıtları siler. Bu işlem yapıldığında, SIP telefon hiçbir gelen çağrıyı alamaz.

D. Kayıt Silme Saldırısının Olma Olasılığı ve Etkisi

Bu saldırılar, bir ya da birçok kullanıcının çağrı almasını engelleyebilir. Yönetici hatları, müşteri ilişkileri hatları, müşteri destek hatları gibi daha birçok kritik haberleşme kanallarını olumsuz etkileyebilir. Bu saldırıların iş dünyasında ciddi bir etkiye sahip olduğu açıktır. Özellikle, çoğu kurumsal şirket için sadece birkaç çağrının alınamaması ile yaşanan sorunlarda bile kabul edilemez tavırlar ile karşılaşılırken, bu saldırıların dikkate alınmasının önemini dile getirmeye bile gerek yoktur [2,3].

Bu saldırıların gerçekleşmesi için, saldırganın iç ağa dâhil olması gerekmektedir. Bir kullanıcının, kayıtları silebilme yetkinliğine sahip bir zararlı yazılımı bilgisayarına indirmesi ile bu saldırı gerçekleşebilir. Bu yöntem ile saldırgan, aynı zamanda iç ağa erişim de kazanabilmektedir. Kayıt silme saldırısı, servis sağlayıcıya erişmek için kullanılan SIP trunk'ların kullanıldığı durumlarda internet üzerinden de gerçekleşebilmektedir.

III. ÖNLEMLER

Bir saldırganın SIP kayıtlarını silmesini engellemek için alınabilecek birkaç önlem vardır. Aynı önlemler, kayıt gasp etme saldırılarını tespit etmek için de kullanılabilmektedir. Buradaki amaç, kayıt işlemini korumak ve SIP proxy'nin geçersiz/sahte kayıtları kabul ederken aldatılmasını engellemektir. Alınabilecek önlemler aşağıda detaylandırılmıştır.

A. SIP Bağlantıları İçin TCP Kullanmak

RFC 3261 uyumlu SIP proxy'ler ve SIP telefonlar hem TCP'yi hem de UDP'yi desteklemelidirler. TCP kullanıldığında, SIP uç-noktaları birbirleri ile kalıcı bağlantılar kurar. Örneğin; SIP telefon, SIP proxy'ye kalıcı bağlantı kuracaktır. Gidiş-sıra (sequence) numaralarının kullanımı gibi, TCP'nin doğasında olan sebeplerden dolayı, bir saldırganın SIP proxy'yi hileli kayıtları kabul etmesi için yanıltması daha zorlaşacaktır [2,4]

TCP'nin kayıt saldırılarına karşı etkili bir önlem olabilmesi için, tüm SIP telefonların SIP proxy ile iletişiminde kullanılıyor olması şarttır. TCP kullanmayan herhangi bir SIP telefon, kayıt manipülasyon saldırılarına zafiyetlidir. TCP'ye yönelik bazı saldırılar da hala mevcuttur.

TCP kullanıldığında, aynı zamanda TLS (İletim Katman Güvenliği) kullanımı da mümkündür. TLS, gizlilik ve güçlü doğrulama (authentication) sağlamak ve saldırganların sinyalleşme üzerinde telekulak yapmasını engellemek için şifreleme kullanır. TLS, aynı zamanda saldırganın SIP proxy'yi hileli kayıtları kabul etmesi için yanıltmasını daha çok zorlaştıran güçlü doğrulama sağlar [5].

TLS, uçtan-uca çalışan bir protokol değildir. TLS, SIP proxy'ler ve SIP telefonlar arasındaki tekli bağlantıları güvenli tutmak için kullanılır. Bir çağrının güvenli olması için, çağrıya dâhil olan tüm SIP uç-noktaları arasındaki bağlantıların hepsi için TLS kullanılmalıdır. TLS, aynı zamanda TCP ile bir dezavantaja sahiptir, eğer bazı SIP telefonlar TLS kullanır ve diğerleri kullanmaz ise, sistemin bütünsel güvenlik modeli çöker. TLS kullanan SIP telefonları güvenli tutulabilirken, kullanmayanlar hala kayıt saldırılarına zafiyetli kalır. Ne yazık ki, Asterisk tabanlı SIP proxy'ler genellikle TCP'yi desteklemezler ve mevcut hiçbir Asterisk ve SER SIP proxy'ler TLS'i desteklemiyorlar. SIP telefonların çoğu TCP'yi destekler, ama çoğu da TLS'i desteklemezler [2,4].

B. Ses ve Veriyi Ayırmak İçin VLAN (Sanal Yerel Alan Ağı) Kullanmak

Kurumsal-seviyedeki SIP sistemlerinin çoğu, ses ve veriyi ayırmak için VLAN'ları kullanırlar. VLAN'lar ve doğru bir şekilde yapılandırılmış LAN (Yerel Alan Ağı) switch'leri (anahtarları) ile gizliliği ihlal edilmiş PC üzerinden kayıtların manipüle edilmesi için yapılan girişimler engellenebilir. Ek önlemler olarak, MAC adres filtrelemesi ve 802.1x port doğrulaması da kullanılabilir [2,7].

Eğer hileli PC, bir LAN switch portu üzerinde ses VLAN'ı için yapılandırılmışsa, ses VLAN'ı üzerinden paketleri elde etmek mümkündür.

PC'ler üzerindeki yazılımsal telefonların kullanımı, VLAN'ların güvenlik amaçlı kullanılmasını bozar. Yazılımsal telefonlar kullanıldığında, paketler (tahminen yazılımsal telefon üzerinden gelen paketler), SIP proxy tarafından kabul edilmek zorundadır. Bu durum da hileli bir uygulamanın yazılımsal telefon taklidi yapıp ve kayıtları manipüle edebilmesine imkân verebilmektedir. Eğer hileli PC, bir LAN switch portu üzerinde ses VLAN'i için yapılandırılmışsa, ses VLAN'ı üzerinde hileli kayıt paketlerini ele geçirmesi mümkündür [6,9,10].

C. *Doğrulamayı Aktif Etmek*

SIP isteklerinin tamamı için, REGISTER isteklerinin doğrulanmasını desteklemek çok hassas bir konudur. REGISTER istekleri sık sık değiştirilmez ve böylece doğrulama için sistem üzerinden geçen yük minimaldir. Sadece iç ya da kurumsal SIP telefonlar kayıt olmalıdır, böylece doğrulama aktif edilebilir ve her bir SIP telefon için güçlü şifre ayarlanabilir. Bu durum, harici ağdan gelen INVITE gibi istekler için (burada SIP trunk'ların (dış hatların) internete açık olduğu varsayılıyor) zıtlık oluşturur. INVITE istekleri daha sık oluşur ve sistem üzerinden geçen ek iş yükü potansiyeli taşır [2,7].

Doğrulamanın kullanışlı olması için, güçlü şifrelerin kullanılması temeldir. Eğer şifreler zayıf ya da telefon dâhili numarasının tersini kullanmak gibi mekanik olarak oluşturulmuşlarsa, saldırgan kolaylıkla tahmin edebilir ve doğrulamayı kırabilir.

D. *Kayıt Süre Aralığını Azaltmak*

SIP telefonlarının kendilerini daha sık kayıt etmelerini sağlamak için kayıt süre aralığı azaltılabilir. Örneğin; kayıt süre aralığı 60 saniye olarak ayarlanmışsa, kayıt silinmiş ya da gasp edilmiş olsa bile, SIP telefon bir dakika sonra kendini kurtaracaktır ve çağrıları almaya devam edecektir [2,7].

E. *İyi Bilinen Portları Değiştirmek*

SIP proxy'ler, varsayılan olarak kullanılan SIP port 5060'in değiştirilmesine izin verirler. Bu "belirsizlik üzerinden güvenlik sağlamak" olsa da, sınırlı bir açıdan koruma sağlayabilmektedir [2,7].

F. *SIP Firewall Kullanmak*

SIP proxy'ye gönderilen tüm sinyalleşmeyi denetlemek/gözden geçirmek için SIP firewall konuşlandırılabilir. SIP firewall, kayıt manipülasyon saldırıları dahil olmak üzere, çeşitli saldırı tiplerini tespit edebilir. SIP firewall kullanmak, internete çıkarken bir temel teşkil eder [6,8].

IV. SONUÇLAR

Açıkça, SIP protokolü doğası gereği sinyalleşme manipülasyon saldırılarına zafiyetlidir. SIP kayıt mekanizması günümüzde aktif olarak kullanılan birçok iş ortamında saldırılara açık olarak kullanılmaktadır. Bu çalışmada, hileli bir REGISTER mesajı üretip SIP sistemine ileten zararlı bir kod parçası yazılarak, VoIP güvenlik laboratuvar ortamında test edilmiş ve bulgular paylaşılmıştır. Bulgulara yönelik olarak bu saldırının anatomisi ile saldırıya yönelik savunma stratejileri önerilmiştir.

Bu test aşamasında öncelikle saldırı gerçekleştirilmeden önce sistem normal çalışır haldeyken Trixbox PBX web ara yüzünde kayıtlı olan kullanıcılar gözlemlenmiştir, zararlı kod çalıştırıldıktan sonra ise tekrar aynı şekilde sunucunun ara yüzü gözlemlendiğinde hedef kullanıcı Polycom IP telefonun kaydının silindiği gözlemlenmiş ancak Polycom telefon konsolunda hiçbir anormallik gözlemlenmemiştir. Saldırı sonrasında Polycom istemcisine çağrı yapmak istendiğinde "503 Service Unavailable (Servis Erişilemiyor)" mesajı alınmıştır.

Güvenlik uzmanları ve haberleşme profesyonelleri SIP konuşlandırmalarını yaparken SIP kayıt mekanizmasına yönelik zafiyetler hakkında bilgi sahibi olmalıdırlar ve bu zafiyetlere yönelik spesifik savunma stratejilerini dikkate almalıdırlar.

V. BİLGİLENDİRME

Bu çalışma TEYDEB 3130514 numaralı proje ile desteklenmiştir.

KAYNAKÇA

[1] Özbirecikli O., VoIP, *"SIP Sinyalleşmeye Yönelik Saldırı Uygulamaları, Zafiyet Analizleri ve Güvenlik Önlemleri"*, Kocaeli Üniversitesi Lisans Tezi, Mühendislik Fakültesi, Kocaeli 2013.

[2] Endler D., Collier M., "*Hacking Exposed VoIP:Voice Over IP Security Secrets & Solutions"*, McGRAW-Hill/Osborne,2007

[3] York D., *"Seven Deadlist Unified Communications Attacks"*, Elsevier Inc., 2010.

[4] Thermos P., Takanen A., *"Securing VoIP Networks"*, Pearson Education, Inc Massachusetts, USA, 2008.

[5] RFC5246, *"The Transport Layer Security (TLS) Protocol"*, Version 1.2, January 2008

[6] Taş İ.M., Taş H., *"VoIP Ağ Güvenliği Perspektifinden Firewall, VoIP IPS ve SBC Karşılaştırması"*, 29. Ulusal Bilişim Kurultayı, Ankara, Türkiye, 2012

[7] VoIP Secuirty Alliance Report, *"VoIP Security and Privacy Threat Taxonomy"*, October 2005.

[8] Taş İ. M., *"VoIP/UC'nin Ağ Güvenlik Planlamasına Dahil Edilmesi"*, 5. Uluslar arası Kriptoloji ve Bilgi Güvenliği Konferansı, ODTU, Ankara, Türkiye, Mayıs 18, 2012

[9] Taş İ. M., *"Tümleşik Haberleşme Güvenlik Riskleri ve Savunma Stratejileri"*, NopCon Uluslararası Hacker Konferansı, Bilgi Üniversitesi, Istanbul, Türkiye, Mayıs 21 2012.

[10] Taş İ. M., *"VoIP Hacking ve SIP Güvenliği"*, Siber Güvenlik Konferansı, ODTU, Ankara, Türkiye, Aralık 22, 2011