SIP Saldırıları ve Güvenlik Yöntemleri

Merve YÜKSEL[1], Nihat ÖZTÜRK[2]*

[1]Bilişim Enstitüsü Bilişim Sistemleri A.B.D., Gazi Üniversitesi, Ankara, Türkiye
[2]Elektrik Elektronik Mühendisliği, Teknoloji Fakültesi, Gazi Üniversitesi, Ankara, Türkiye
mmervecosgun@gmail.com,ozturk@gazi.edu.tr
(Geliş/Received:05.02.2017; Kabul/Accepted:15.07.2017)
DOI: 10.17671/gazibtd.331042

Özet— Bu çalışmada, sesin gerçek zamanlı olarak IP üzerinden iletilmesi (VoIP) için kullanılan Session Initiation Protocol (SIP) güvenlik açıkları incelenmiş ve çözüm yöntemleri önerilmiştir. Günümüzde, SIP tüm VoIP sunucu, IP telefon, yazılım tabanlı telefon ve VoIP çalışan uygulamalar için kullanılan en yaygın protokol olup tüm hepsi tarafından da desteklenmektedir. SIP protokolünün bu kadar popüler ve geniş kapsamda kullanılması birtakım tehditleri de beraberinde getirmektedir. Kullanıcılar arasındaki bağlantının koparılması, sunucuya ulaşılamaması, hizmet kesintisi, görüşmelerin manipüle edilmesi vb. amaçları taşıyan birçok saldırı ile istenmeyen sonuçlar doğabilir. Özellikle savunmasız sistemlerde uygulaması kolay olan DoS hizmet kesintisi, telekulak ve ortadaki adam saldırılarının gerçekleştirilmesi bu çalışmanın temelini oluşturmuştur. Bu saldırıları gerçekleştirebilmek için gerekli olan yazılım ve araçlar incelenmiştir. Gerçekleştirilen saldırıların sistemdeki olumsuz etkilerini en aza indirmek için ise, IDS/IPS olarak kullanılan yazılım ile çeşitli kurallar tanımlanmış ve saldırı anında alarm vermesi sağlanmıştır. Paket yakalama yazılımları ile mesajların ele geçirilmesini önlemek için ise kriptolama teknolojilerinin kullanılmasının gerekli olduğu görülmüştür.

Anahtar Kelimeler— SIP, SIP saldırı, SIP güvenlik, VoIP

SIP Attacks and Security Methods

Abstract— In this study, vulnerabilities of Session Initiation Protocol (SIP) used for voice transmission over IP (VoIP) in real time are examined and solution methods are proposed. Nowadays, SIP is the most common protocol used for all VoIP servers, IP phones, software-based phones and applications running via VoIP, and is supported by all of them. The use of SIP protocol in such a popular and broad scope leads to some threats. Among these threatsare flooding attack, instant message session hijacking, denial of service. Undesirable results can occur with many attacks that aim disconnecting the users, unreaching the server, service interruption, manipulating the communication, etc. Especially, implementations of DoS service interruption, wiretapping and man-in-the-middle attacks, which are easy to be applied in vulnerable systems, form the basis of this study. Necessary software and tools have been analyzed to execute these attacks. To degrade the negative impacts of performed attacks on the system,several rules are described with software that is used as IDS/IPS and make them generate alarms duringattack.It is seen that encryption technologies must be used to avoid capturing messages through packet capturing software.

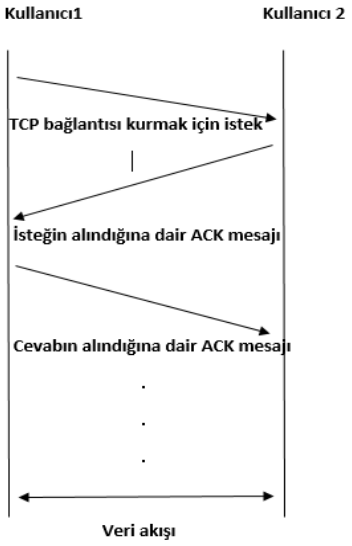
Keywords— SIP, SIP attack, SIP security, VoIP

1. GİRİŞ (INTRODUCTION)

İnternet günlük yaşantımızın birçok alanında kullanılmaktadır. VoIP (Voice over IP) teknolojisi ile internet altyapısı üzerinden ses iletimi gerçekleştirilmektedir. Gerçekzamanlı olan ses uygulamalarının ihtiyacı olan gecikmesiz, paket kayıpsız iletişim bu teknoloji ile sağlanabilmekte olup, mevcut data (veri) hattını kullanması ve herhangi bir fiziksel analog/dijital santrale gerek duymaması ile maliyet olarak da büyük bir kazanç sağlamaktadır. Mevcut PSTN (Public Switched Telephone Network) tabanlı telefonlar ile kıyaslandığında sunduğu avantajlar ile tercih edilmektedir.

SIP (Session Initiation Protocol) ise VoIP teknolojisinin en temel protokollerinden biri olmakla birlikte, aynı özellik için kullanılan H323, MGCP, SCCP benzeri protokoller arasında en çok tercih edilen protokoldür [1]. RFC 3261 dokümanlarında açıklanan bu protokol; IETF, ETSI gibi birçok uluslararası kuruluş tarafından da kabul görmektedir.Uygulama katmanında çalışan SIP, metin içerikli bir protokoldür; arayan ve aranan bilgisi, mesaj türü (davet, başlatma, bitirme), domain bilgisi gibi bilgileri içeriğinde barındırır. En çok karıştırıldığı RTP (Real-Time Transfer Protocol) protokolü ile kıyaslandığında, SIP' in oturum başlatmak amaçlı kullanıldığı, RTP'nin ise ses ve görüntünün taşınmasından sorumlu olduğu görülmektedir.

Web ile birlikte çalışabilmesi, beraberindeki uygulamalara kolayca entegre olabilmesi SIP'in en önemli ve tercih edilmesine neden olan özelliklerinden biridir. Ayrıca kurulmuş olan oturuma video eklemesi de gerçekleştirebilmektedir.TCP desteği ile Şekil-1'de akış diyagramı verilen kullanıcılar arası handshaking (el sıkışma) yapılarak bağlantının kesin oluştuğundan emin olunur. UDP desteği ile de anlık ses iletimi için gerekli olan kesintisiz iletişim gerçekleştirilmektedir. [2]. Aynı zamanda ölçeklenebilir ve farklı mimarilere de rahatlıkla uygulanabilir.



Şekil 1. TCP el sıkışma akış diyagramı (Flowchart of TCP handshaking)

SIP protokolü ile oturum kurulabilmesi için kullanıcıların kaydolacağı bir SIP sunucusuna ihtiyaç duyulmaktadır. Bu sunucu bir SIP Proxy sunucusu olabileceği gibi registrar (kayıt) sunucusu da olabilir. Gelen isteklere bu sunucu cevap vermektedir [3]. Bu sunucuya yapılabilecek olan olası bir saldırı ise tüm sistemi etkileyebilecek tehlikeli bir durum oluşturabilir. Ağa dâhil olan bir saldırgan iletişim halindeki iki kullanıcı arasındaki SIP mesaj içeriğini rahatlıkla dinleyebilir ve mesaj içeriğini değiştirebilir [4]. Sosyal ve hizmet aksatma saldırıları ile de SIP haberleşmesi sabote edilebilir [5]. Hizmet kesintisine neden olan ve en sık karşılaşılan saldırı, Denial of Service (DoS)'dur. DoS saldırı türleri arasında ise, genellikle istem dışı başlatılan oturum sayısı ve sunucudan kaçak geçen paket sayısı gibi saldırılar bulunmaktadır [6].

Kullanıcı sunucu haberleşmesinde genellikle yetkilendirme yapılarak, istekler yanıtlanır [7]. Ayrıca SIP sunucularda TLS (Transport Layer Security) kullanımı ile de güvenli iletişim gerçekleşmesine olanak sağlanabilir [8]. Yine güvenilir iletişim için S/MIME kullanımı ile de SIP mesajlarına güvenilirlik ve gizlilik katılmaktadır [9]. IPSEC uygulaması ile de SIP mesajları dışarıdan okunamaz hale getirilerek, güvenilirliği arttırılabilir [10].

Tablo-1'de, benzer çalışmalarda, SIP DoS ve oturum bilgilerinin çalınması saldırılarına karşı alınan güvenlik önlemleri listelenmiş ve hangi tarz önlem alındığı belirtilmiştir.

Tablo 1. Örnek çalışmalar ve incelenen güvenlik önlemleri (Example studies and investigated security precautions)

Yazar	İncelenen Güvenlik Önlemi
Yang C-C.[11]	SIP AuthenticationMethod
Voznak M.[12]	TestingTopology
Özçelik,İ. [13]	IDS
Sengar, H.[14]	StateMachines
Tas, I. [15]	TLS
Ding, Y. [16]	PetriNets
Rescorla, E. [17]	TLS
Tiller,J. [18]	IPSec
Rosenberg, J. [19]	S/MIME

Bu çalışmada SIP ile haberleşen kullanıcılara hizmet aksatma (DoS) saldırısı, telekulak saldırısı ve oturum bilgilerinin çalınması gerçekleştirilmiş ve bu saldırılar karşısında hangi tür önlemler alınması gerektiği belirtilmiştir.

2. SIP TEMEL ÖZELLİKLERİ (SIP BASIC CHARACTERISTICS)

SIP oturum kurulurken temel alınan çeşitli özellikler şunlardır:

- Aralarında oturum başlatılacak olan kullanıcıları tespit ederek bu bilgiyi içeriğinde sunmak
- Bağlantıyı başlatmak, sonlandırmak, çağrı parametrelerini ayarlamak
- Kullanıcı konum bilgilerini içermek
- Çağrının yönetimini gerçekleştirmek
- Çağrı özelliklerini değiştirmek: Sadece ses iletişimi yapılan bir görüşmeye video iletimi de eklenmesi.
- Mobilite:Kullanıcı bağlantı sırasında konum değişikliği yapsa dahi bağlantı kopmaması.
- Medya parametrelerini ayarlamak

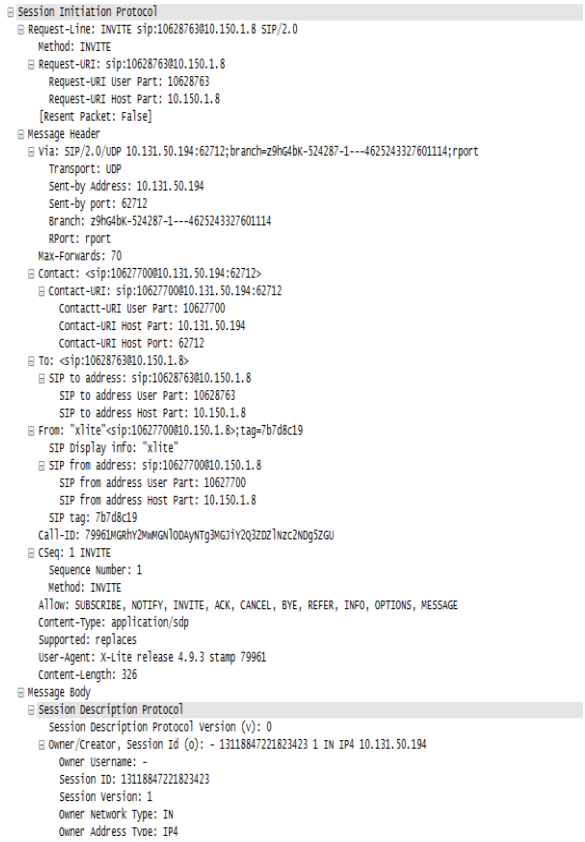
2.1. SIP Mesaj İçeriği (SIP Message Content)

Tipik bir SIP mesajlaşma örneği Şekil-2'de verilmektedir. SIP temelde iki tür mesajdan oluşur; talep ve cevap. Bu iki mesaj tipi içeriğinde başlangıç, başlık ve içerik olmak üzere üç bölümü barındırır.

Başlangıç satırı, talep ya da durum satırı olabilir. Protokol sürümünü taşıyan bu satır, istek mesajı ise (invite, cancel, register) istek yaptığı kullanıcıyı belirten bir URI (Uniform Resource Identifier) kodu içermektedir. SIP-URI gösterimi ise, sip:deneme@makale.com şeklindedir. Eğer durum mesajı ise numerik durum kodu bu mesajda belirtilir.

Başlık, http benzeri yapıda olduğundan dolayı ad ve değer girdileri bulunmaktadır. Örneğin, bir davet isteği gönderen kullanıcı kendi kullanıcı adı ve domain bilgisini; from:SIP:kullanici1@domain.com ile bağlantı kuracağı kullanıcı bilgisini; to:SIP:kullanici2@domain.com ile başlık bilgisinde gönderir.

İçerik, bağlantıyı tanımlamak için metin içerikli veriyi taşımaktadır. Başlangıç ve başlık satırlarında belirtilen bilgilerin ayırım yapılmasını da sağlamaktadır. Örneğin, içerik türü (text/html), içerik uzunluğu, içerik dili benzeri bilgiler içerik de tutulur.



Şekil 2. SIP mesaj içeriği (SIP message content)

En çok kullanılan SIP mesajları: [20]

- INVITE (oturum başlatma isteği)
- ACK (onaylama)
- CANCEL (oturumu iptal etme)
- BYE (oturumu bitirmek)
- REGISTER (konum bilgilerini de kullanarak kayıt olma)

Yapılan isteğe yanıt kodları ise aşağıdaki gibidir:

- 1XX : Bilgi içerikli yanıtlar (180 RINGING)
- 2XX : Başarı yanıtları (200 OK)
- 3XX : Yeni adrese yönlendirme yanıtları (305 USE PROXY)
- 4XX : Talebin yerine getirilememesi (404 NOT FOUND)
- 5XX : Sunucu hataları (500 INTERNAL SERVER ERROR)
- 6XX : Global arızalar (603 DECLINE)

2.2. SIP Haberleşmesi (SIP Communication)

VoIP görüşmesinin yapılabilmesi için gerekli olan SIP haberleşmesi için öncelikli olarak kullanıcıların SIP sunucuya kayıtlı olması ve bir kullanıcının oturum başlatmak istediği kullanıcı bilgileri içeren INVITE mesajını kayıtlı olduğu sunucuya göndermesi gerekir. Sunucu bu mesajı yine kendisine kayıtlı olan diğer kullanıcıya yönlendirir. Aranan kullanıcının çalması sırasında arayan kullanıcıya RINGING durum kodu dönülür. İsteği kabul eden aranan kullanıcı 200 OK durum kodu ile oturum isteğini kabul ettiğini bildirir. Arayan kullanıcı kendisine OK mesajının ulaştığını ACK mesajı ile aranan kullanıcıya bildirir. Bu iletişim şekline "Üç Yollu El Sıkışma" denilmektedir. Aralarında oturum oluşmuş olan kullanıcılar iletmek istedikleri gerçek zamanlı verileri RTP (Real-Time Transfer Protocol) paketleri ile iletirler. Oturum sonlandırılmak istendiğinde ise kullanıcılardan biri BYE mesajı yollayarak istekte bulunur. Sunucu bu mesajı diğer kullanıcı ile paylaşır ve kullanıcıdan 200 OK cevabı döndükten sonra oturum bitirilir [21].

3. SIP SALDIRI YÖNTEMLERİ (SIP ATTACK METHODS)

SIP protokolü kullanarak başlatılan oturumlarda, kullanıcıya ve kaydolduğu sunucuya ait bilgiler şifrelenmeden gönderildiği için söz konusu bilgilerin ait olduğu cihaz ve sistemler saldırılara karşı da savunmasızdır. Bu güvenlik açığı nedeniyle birçok saldırı gerçekleştirilebilecek olup, bu saldırılar ile gerek hizmet kesintisi gerekse konuşmaların dinlenmesi gibi birçok istenmeyen sonuçlar doğabilir.

VoIP teknolojisinin gerçek zamanlı ses iletimi olmasından dolayı gerçek zamanlı güvenlik önlemlerine ihtiyaç duyulmaktadır. SIP ya da VoIP trafiğinin hizmet dışı kalması diğer uygulama katmanında çalışan teknolojiler ile kıyaslandığında kabul edilemez bir yapıya sahiptir; ses verileri herhangi bir yerde depolanmaz veya tekrar iletilemez. Ayrıca SIP trafiği paketler ile taşındığı için manipülasyona ve orta adam saldırıları ile kimlik hırsızlığına maruz kalınabilmektedir. SIP saldırıları temelde altı grupta incelenebilir.

3.1. DoS ve DDoS Saldırıları (DoS and DDoS Attacks)

DoS ya da DDoS ataklarında, mevcut SIP sunucusunun hizmetinin kesintiye uğratılması veya servis yanıltma amaçlanır. 2004 CSI/FBI raporuna göre hırsızlıktan bile daha fazla mali zarara neden olmaktadır [22]. Bu atakta, yeterli bilgileri ele geçirdikten sonra, sunucu savunmasız kalmaktadır. Aynı anda birden fazla saldırganın hedef

sunucuyu etkisiz hale getirmek için yaptığı DDoS saldırıları ise SIP için en sık karşılaşılan ve en ağır sonuçlar doğuran saldırı çeşididir [23]. SIP için yapılan DDoS saldırıları, çok fazla sayıda REGISTER ya da INVITE paketinin sunucuya gönderilmesi, SIP paketlerinin yapısının değiştirilmesi ya da SIP durum kodları değiştirilmesi olarak karşımıza çıkabilir. Özellikle açık internet erişimi bulunan ve network dışından da çağrı kabul eden sunucular bu saldırılara karşı savunmasızlardır. Sunucu tarafından imzalanmış ya da şifrelenmiş ses paketleri dahi bu saldırıdan etkilenmektedir. Paket iletiminin gerçek zamanlı gerçekleştirildiği bu sistemlerde, zararlı yazılımlar DDoS saldırıları ile çoğalarak sistem trafiğini artırır ve sistemi yanıt veremez hale getirir.

SIP paket tekrarlama saldırısı, SIP paket ekleme saldırısı, TLS bağlantı sıfırlama saldırısı, flood saldırıları, sahte mesaj saldırıları en bilinen DoS saldırılarındandır. Bu tür saldırılara karşı SIP destekli güvenlik duvarı kullanarak, ayrıca IDS ve IPS cihazlarına SIP odaklı kurallar ekleyerek detaylı ağ analizi yapılması sağlanabilir ve saldırılar önlenebilir.

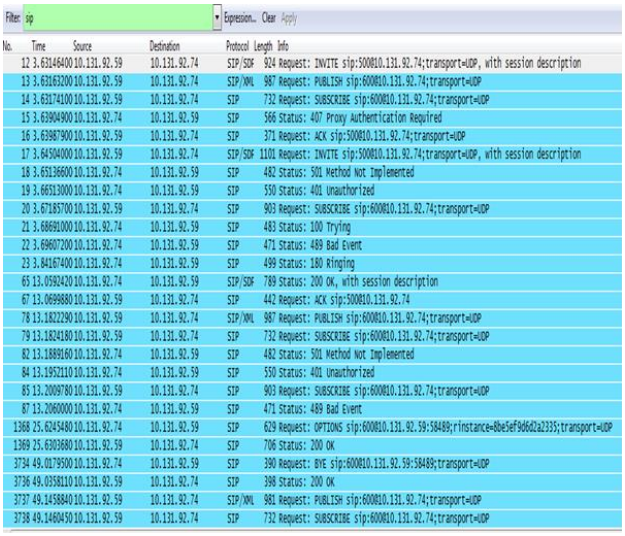
3.2. Telekulak Saldırısı (Wiretapping Attack)

Bu saldırıda ağa erişerek veri paketlerine erişim ve kişisel bilgilere ulaşılması amaçlanmaktadır. Saldırgan sistem üzerindeki zafiyet ve açıkları bulmak amacıyla da telekulak saldırısı gerçekleştirebilir. VoIP teknolojisinde, erişimin kolay olması nedeniyle IP ağına erişimi bulunan saldırgan iletilen paketleri görüntüleyebilir ve yakalayabilir [24]. Bazı paket yakalama programları ile bu saldırı rahatlıkla gerçekleştirilebilmektedir. Şekil-3'de Wireshark paket yakalama yazılımı ile yakalanan SIP paketleri bulunmaktadır.

3.3. Ortadaki Adam Saldırısı (Man in the Middle Attack)

Oturum başlatmak üzere ya da oturumu başlamış olan kullanıcıların iletişim kurmak üzere paylaştığı paketlerin, saldırgan tarafından ele geçirilerek, trafiğin kendi üzerinden geçecek şekilde ayarlanması ortadaki adam saldırısıdır. Bu yönlendirme ile gerekli olan bilgileri ele geçiren saldırgan ayrıca sistemde değişiklik yapma hakkına da sahip olur.

Oturumda kullanıcılar arasına giren saldırganı kullanıcılar fark etmeyebilir. Bağlantı için istek yapan kullanıcı ve yanıt veren kullanıcı arasına giren saldırgan istek yapan kullanıcının isteğini yanıtlar ve iletişim kurulacak olan kullanıcıya da saldırgan kendisi istekte bulunur. Diffie-Hellman anahtar değişimi ile iki farklı anahtar üreterek akış şifrelenir. Bu sayede her iki kullanıcı da herhangi bir sıkıntı sezmez. Diffie-Hellman değerleri yetkilendirilmediği sürece bu saldırının gerçekleşmesi mümkündür.



Şekil 3. Wireshark ile paketlerin dinlenmesi
(Listening to packages through Wireshark)

3.4. Kayıt Bilgilerinin Değiştirilmesi (Change of Register Data)

Bu saldırı ile sistemdeki kullanıcıların kayıt bilgileri değiştirilerek, yapılan tüm isteklerin farklı bir sunucuya gitmesi sağlanarak istekler yönlendirilebilir. SIP mesaj içeriğinde bulunan, isteğin kimden yapıldığına dair bilgiler değiştirilerek sahte kullanıcı kayıtları yapılabilir. Kullanıcı veri bloğu iletişim kuralları (User Datagram Protocol - UDP) mesajlarının kontrolsüz olması sebebi ile saldırgan hem kendini sisteme kaydedebilir hem de sistemdeki aktif kullanıcıları kendine yönlendirebilir. Birçok SIP tabanlı sistemde herhangi bir yetkilendirme istenmediği için bu saldırı rahatlıkla gerçekleştirilebilmektedir. Bu saldırıyı başarıyla gerçekleştirdikten sonra ortadaki adam saldırısı gerçekleştirmek de daha kolay bir hal almaktadır. Yetkilendirme yapılarak söz konusu saldırının önüne geçilebilir.

3.5. Tekrarlama Saldırıları (Repeat Attacks)

SIP mesajlarının ele geçirilmesi ve belli bir süre sonra aynı mesajların geri gönderilmesi ile gerçekleşir. Genelde yetkili bir kullanıcının bilgilerinin çalınması ve onun yerine geçilmesi ile gerçekleştirilir [25]. Bu saldırı ile tek bir arama için oturum başlatılacakken birden çok oturum başlatılması ile birden çok arama gerçekleştirilmiş olur bu da gerek sistemi meşgul etmesi gerekse maddi açıdan kayıp oluşturması nedeni ile önlem alınması gereken bir durumdur. Yine aynı şekilde yetkilendirme ve şifreleme senaryoları ile bu saldırı türü engellenebilir.

3.6. Oturum Bozma Saldırısı (Session Corruption Attack)

Var olan bir sinyalleşme ya da oturumu kesmek amacıyla gerçekleştirilir. İletişim halinde bulunan kullanıcılar arasına saldırganın girmesi ve aradaki bağlantıyı, BYE mesajı yollayarak bitirmesi ile sonuçlanır [26]. HTTP

Digest Authentication kullanılmış olsa dahi saldırgan zararlı ACK ya da CANCEL istekleri ile oturumların düşmesine neden olabilir. Güvenli oturum kurulması sağlanarak ve gerekli yetkilendirmeler yapılarak oturuma dâhil olunması engellenebilir ve bu sayede de oturumun devamlılığı sağlanabilir.

4. 4. SIP GÜVENLİĞİ YÖNTEMLERİ (SIP SECURITY METHODS)

SIP tabanlı iletişimin birçok saldırı türüne açık olması sebebi ile çeşitli güvenlik önlemlerinin alınması gerekmektedir. Paketlerin açık bir şekilde şifrelenmeden yollanması, kötü niyetli kişiler tarafından bu paketlerin yakalanarak, oluşturulan tüm oturumların dinlenmesine sebebiyet verebilmektedir. SIP ile istek mesajları iletildiğinde, istek yapılan kullanıcı isteği yapan kişiye ait bilgileri sorgulamadan ve doğrulamadan (yetkilendirmeden) isteğe cevap verebilir. Herhangi bir doğrulama yapılmadığı sürece oturumlar yanlış kişilerce kurulabilir ya da kabul edilebilir. Bu sorunu çözmek için doğrulama teknolojileri kullanılabilir. SIP metin tabanlı bir protokol olduğu ve HTTP yapısında çalıştığı için HTTP'ye ait doğrulama teknolojileri kullanılabilir.

Mesajların anahtar ve şifreleme yöntemleri kullanılarak gönderilmesi de mesajın bütünlüğünün ve gizliliğinin sağlanması açısından önemlidir. Uçtan uca mesaj içeriğinin kodlanması IPsec ile sağlanabilmektedir. Kişiye özel anahtarlar ve genel anahtarın kullanılması ise S/MIME teknolojisi ile gerçekleştirilmektedir. SIP belli parametrelere karşı paket gecikmesine ve kaybına (jitter) duyarlıdır ve bu nedenle de güvenlik önlemleri alınmalıdır. Bazı güvenlik çözümleri; IDS, IPS, diğer güvenlik cihazları, paketlerde gecikme ve kayıp oluşmasına yol açarlar. Ayrıca ses servislerinin sürekli ulaşılabilir olması ve sistemin güvenilir, bütünlüğü korunaklı ve kaliteli olması istenmektedir. Bu nedenle, genelde kurulan topolojide ses paketlerine öncelik tanınarak herhangi bir gecikme ve kayıp önlenmeye çalışılır. Diğer veri haberleşmeleri ile kıyaslandığında sesin herhangi bir paket kaybına tolerans göstermemesi, ona yapılan saldırıları da kritik hale getirmektedir.

4.1. Güvenlik Gereksinimleri (Security Requirements)

Güvenlik gereksinimleri şöyle sıralanabilir:

- Gizlilik: Bilginin ya da kaynakların gizlenmesi olarak tanımlanır. SIP mesaj içeriğinin ve SIP başlığının gizli olması gerekir.
- Bütünlük: SIP mesajları yetkili olmayan kişilerce değiştirilememeli veya başka bir SIP mesajını yanıltmamalıdır.
- Erişilebilirlik: SIP mesajlarının rahatlıkla iletilmesi için kullanıcıların kayıtlı olduğu sunucunun sürekli erişilir olması gerekmektedir.
- Reddetmeme: Alıcının iletişimin gerçekten gerçekleştiğini ve veriyi yollayan kişinin kimliği hakkında bilgi sahibi olduğunu ön görmektedir.
- Sunucu Doğrulama: Kullanıcı verilen sunucu kimliğine güvenmelidir [27]. Arayan ve aranan bilgileri SIP mesajında tutulur ve aranan kullanıcı arayan kullanıcının kimlik bilgilerine güvenir.
- Kullanıcı dostu olması: Kullanıcılar SIP ve SIP güvenliği hakkında bilgi sahibi olmayabilir. Bu durumda bile kullanıcının güvenliğini sağlamak esastır.

4.2.Güvenlik Yöntemleri (Security Methods)

Temel güvenlik yöntemleri şöyle açıklanabilir;

- HTTP Digest Authentication (Özet Doğrulama): SIP protokol yapısının HTTP yapısına benzemesinden dolayı, HTTP güvenliğinde kullanılan özet doğrulama teknolojisi kullanılmaktadır [28]. Kullanıcı isteği yaparken sunucuya kullanıcı adı ve şifre gönderir, fakat sunucu bu bilgileri direkt olarak algılamaz, talebi yapan kullanıcıya anlık bir değer göndererek sorgular, kullanıcı çeşitli bilgileri içeren toplam bir değer hesaplar ve sunucuya geri gönderir. Sunucu da iletilen bilgiyi doğrular. Fakat bu süreçte araya kötü niyetli kullanıcı ya da saldırganlar girmesi ile iletilen mesajlar değiştirilebilir. Bunun önüne geçmek için doğrulamaya ve dolayısı ile mesaj bütünlüğünün korunmasına ihtiyaç duyulmaktadır. Hashlenmiş olan şifrenin ağ üzerinde iletilmesi ile paketlerin ve şifrelerin yakalanması zorlaşmış olur, böylece telekulak ve tekrarlama saldırılarını gerçekleştirmek de zorlaşır. Doğrulama ve tekrarlama koruması sağlamasına karşın bu teknoloji, gizlilik ve bütünlük prensiplerini sağlayamaz. RFC 3261' e göre sadece bu güvenlik önlemi ile ortadaki adam saldırılarına karşı savunmasız kalınabilir.

- S/MIME: SIP mesajlarının şifrelenmesi ve bütünlüğünün korunması amacıyla kullanılan S/MIME, aslında e-posta iletilerine çeşitli içeriklerin eklenmesine olanak sağlayan ve bunu şifreleyerek yapan bir teknoloji olarak üretilmiştir [29]. Doğrulama, gizlilik, bütünlük ve tekrar etmeme özelliklerini sağlaması ile mesajın kendisine koruma sağlamaktadır. SIP mesajı S/MIME gövdesi ile tünellenir ve MIME gövdesi ayrı bir imza ile imzalanır. Orijinal mesaj contenttype:message:SIP bilgisi altında tünellenmiş halde bulunur. Açık anahtar yapısı ve sertifikalar kullanılması son kullanıcılar açısından zorluk olarak görülebilmektedir ve karmaşık gelebilmektedir.

- TLS: RFC 2246 tarafından tanımlanan TLS, OSI iletim katmanında çalışan bir protokoldür. Tamamen güvenlik amacıyla oluşturulmuş olup, bağlantı yönelimli ve güvenilir iletim gerektirdiğinden sadece TCP ile çalışır UDP ile çalışmaz. Mesajın gizliliğini, doğrulamayı ve mesaj bütünlüğünü sağlamaktadır. TLS bağlantısı kurmak için kullanıcılar birbirlerine belirli mesajlar gönderirler ve alım bittikten sonra güvenli oturum kurulmuş olur. TLS iki protokol kullanmaktadır; kayıt protokolü ve el sıkışma protokolü. Kayıt protokolünde, kullanıcılar simetrik/asimetrik anahtarlı şifreleme kullanır. El sıkışma protokolünde ise kullanıcı ve sunucu arasında algoritmalara ve kullanılacak olan anahtara karar verilir. TLS bağlantısı kurulması üç aşama ile gerçekleşir. İlk

olarak kullanıcılar desteklenen şifreleme algoritmalarını belirler. Sonrasında kullanıcılar arasında anahtar değişimi gerçekleşir ve birbirlerini doğrularlar. Son aşamada ise mesajları şifrelemek için bu anahtarları kullanırlar ve iletişim kurarlar. Bağımsız ve kendine yeten bir güvenlik protokolü olması sebebiyle TLS şifreleme için en çok kullanılan teknolojilerden biridir [30-31].

- IPSEC: OSI ağ katmanında güvenlik sağlayan IPSEC, tüm IP iletişimini şifrelemek ve doğrulamak için kullanılan bir standarttır [32]. AH (authetication header) ve ESP (encapsulation security payload) protokollerini bulundurur, AH protokolü sadece doğrulama sağlamakta olup, ESP protokolü hem doğrulama hem de şifreleme sağlamaktadır. Ulaşım ve tünel kiplerine sahiptir. Ulaşım kipinde sadece veri şifrelenmektedir. Tünel kipinde ise hem paket başlığı hem de veri şifrelenir. Kullanıcılar arasında karşılıklı kimlik doğrulaması yapılır ve güvenlik anlaşması yapılır. Tüm veriler şifrelenerek kullanıcılar arasında iletilir. Kullanıcılar veri iletimine başlamadan önce veriyi nasıl koruyacaklarına dair bir anlaşma yaparlar. Bu anlaşmaya SA "Güvenlik Anlaşması" denir. IKE (Internet Key Exchange) bu anlaşmayı yönetir. Anahtar yönetimi manuel olarak da otomatik olarak da yapılabilir. Eğer çok fazla sayıda güvenlik anlaşması var ise ve yapı karmaşık ise otomatik olarak, küçük yapıda ise manuel olarak yapılması tercih edilir. Asıllama, mesaj bütünlüğü, gizlilik ve tekrarlama saldırılarına karşı koruma sağlamaktadır. Fakat tüm verinin hatta başlığında şifrelenmesi ekstra bir yük getirmekte olup, gerçek zamanlı çalışan ve bu da herhangi bir gecikmeye tolerans göstermeyen VoIP teknolojisinde sıkıntı yaratabilmektedir.

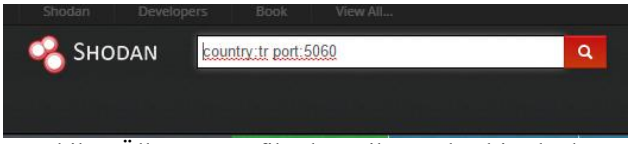
- Güvenlik Duvarı ve Nat Kullanımı: Doğrulanmayan erişim ve zararlı trafik için oluşturulan ilk korumacı cihaz güvenlik duvarıdır (firewall). Genellikle iç ağ ve dış Internet trafiği arasına konumlandırılarak tüm gelen ve giden paketlerin buradan geçmesi sağlanır. Üzerinden gelen paketleri kabul edip etmeyeceğini belli kurallara göre yapan bu cihaz, IP ve port numarası bilgileri girilerek kural tanımlanmasına olanak sağlar. Güvenlik duvarlarında yüksek bağlantı noktası aralıkları açılmaz, çünkü bu durum yetkisiz bağlantılara da izin verir. NAT ise IP adresini korumak için kullanılır. Güvenlik duvarından geçen SIP mesajları için açılması ve kapanması gereken portlar kontrol edilir. Yerel ağ içinde kullanılan IP'ler dış trafiğe (internete) erişmek için genel (public) bir IP'ye ihtiyaç duyarlar. Bunu sağlamak için de NAT çözümüne ihtiyaç duyulur; bu durumda özel IP'ler genel IP'lere dönüştürülür [33]. SIP sinyalleşmesi için NAT ve güvenlik duvarı yanında gereken RTP portlarını da açmak gerekecektir. Bu da aslında bir güvenlik açığına neden olacaktır. SIP protokolünün yapısında NAT olmadığı için geçiş problemleri yaşanmaktadır. Buna çözüm için SIP ALG, STUN, ICE gibi çeşitli öneriler de bulunulmaktadır. Ayrıca data (veri) için kullanılan güvenlik duvarları uygulama katmanını tamamen görüntüleyemezler. Sinyalleşme ve medya için farklı portları kullanması da SIP için data(veri) güvenlik duvarlarını yetersiz kalmasına neden olmaktadır. Bazı güvenlik duvarlarının SIP paketlerini tam olarak algılayamaması da çağrıların düşmesine ya da konuşmanın standartlara uygun olmasına engel olmaktadır.

5. SALDIRININ TESPİT EDİLMESİ (DETECTION OF ATTACK)

SIP ile haberleşen bir VoIP ağına saldırı gerçekleştirmek için öncelikle o ağ hakkında bilgi toplanması ve sistemin açıklarının bulunması gerekir. Sistemin zayıf noktaları bulunduktan ve gerekli IP ler elde edildikten sonra o sisteme sızma denemelerine başlanır. Gerekli güvenlik önlemleri alınmamış olan sistemde açık portların ve IP bilgisinin kullanılması ile sunucuya kayıt olunabilir, yapılan görüşmeler manipüle edilebilir veya VoIP/SIP hizmeti kesintiye uğratılabilir.

5.1. Savunmasız Sistemlerin Bulunması (Finding Vulnerable Systems)

Internet üzerinde bulunan birçok site üzerinden 5060 SIP portunu kullanan ve dışarıya açık olan savunmasız sistemler rahatlıkla bulunabilir. Bunun için kullanılan en bilindik adresler: Shodan ve Google'dır. Shodanpentest çalışmaları için geliştirilmiş olup, özellikle hacker'lar tarafından sıkça kullanılan bir arama motorudur. İnternete açık olan her türlü sistemi çeşitli filtreler kullanarak bulabilmeye ve onlar hakkında bilgi elde edebilmeye olanak sağlar. Ülke ve port filtreleme ile yapılan bir arama Şekil-4'de gösterilmektedir. Google arama motorunu kullanarak ise, yine belli filtreler ile istenen sistem bilgilerine ulaşmak mümkün olmaktadır.



Şekil 4. Ülke ve port filtreleme ile yapılan bir Shodan araması (Shodan search with country and port filtering)

5.2. Port Tarama (Port Scan)

IP bilgisi ya da domain adı elde edilen sistem için hangi portların açık olduğu, üzerinde şu an hangi protokollerin çalışabildiği, hangi güvenlik önlemleri alındığı (güvenli protokollerin port numarasına bakarak) bilgisine ulaşılabilir. Bunun için "nmap ","zenmap" gibi birçok açık kaynak kodlu program bulunmaktadır. Bu yazılımlar Şekil-5 görüldüğü gibi güvenlik açıklarını tespit etmenin yanında ağ haritası çıkarma gibi özelliklere de sahiptir. Zenmap programı Windows işletim sistemine sahip bilgisayarlarda kullanılabileceği gibi, nmap programı Linux işletim sistemine sahip bilgisayarlarda çalışmaktadır. Ayrıca bu programlar, penetrasyon testleri etik saldırganlar için tasarlanmış olan Kali Linux ile birlikte gelmektedir.Şekil-5'te görüleceği gibi hedef IP ve taramak istenilen network protokolü (TCP-UDP) bilgileri

girilerek yapılan aramada açık olan portların dökümü yapılmıştır.

Nmap Output | Ports / Hosts | Topology | Host Details | Scans

Port	Protocol	State	Service	Version
21	tcp	open	ftp	vsftpd 2.0.5
22	tcp	open	ssh	OpenSSH 4.3 (protocol 2.0)
80	tcp	open	http	Apache httpd 2.2.3 ((CentOS))
111	tcp	open	rpcbind	2 (RPC #100000)
443	tcp	open	http	Apache httpd 2.2.3 ((CentOS))
3306	tcp	open	mysql	MySQL (unauthorized)
4445	tcp	open	upnotifyp	
68	udp	open|filtered	dhcpc	
69	udp	open|filtered	tftp	
111	udp	open	rpcbind	2 (RPC #100000)
123	udp	open	ntp	NTP v4.2.2p1@1.1570-o (secondary server)
199	udp	open|filtered	smux	
497	udp	open|filtered	retrospect	
1200	udp	open|filtered	scol	
5060	udp	open	sip-proxy	Asterisk PBX

Şekil 5. Zenmap programı ile açık olan portların taranması (Zenmap search with open ports)

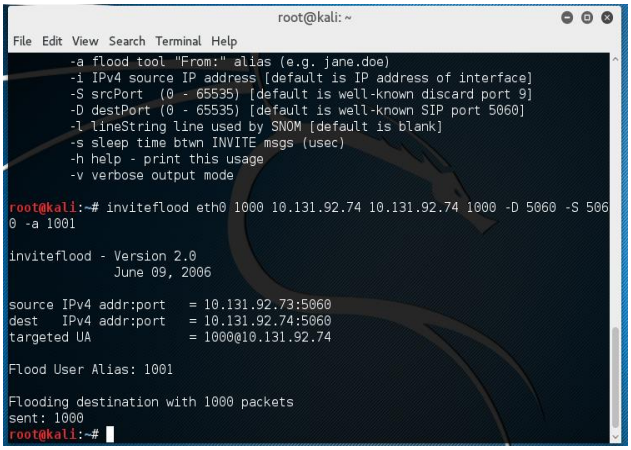
5.3. Saldırı Tipinin Belirlenmesi (Determination of Attack Type)

IP bilgileri ve açık portların bulunmasından sonra bu bilgiler ile hangi saldırının gerçekleştirileceğinin belirlenmesi gerekir. Örneğin, SIP sunucusuna dışarıdan ulaşılabilen savunmasız bir yapıda, DDoS saldırısı gerçekleştirilerek, sistem kesintiye uğratılabilir. Bu saldırı, bazı kullanıcılar için anlık kesinti olarak algılansa da özellikle çağrı merkezi benzeri yapı kullanan büyük firmalarda çok kısa süren bir kesinti bile maddi ve manevi olarak büyük zarara uğratabilmektedir. Bu saldırıyı gerçekleştirebilmek için çeşitli saldırı araçları bulunmaktadır; en bilineni ise Şekil-6'da gösterilen Kali Linux işletim sistemidir. Bu sistem, pentest çalışmaları için geliştirilmiş olup, içerisinde birçok pentest uygulamaları (nmap, wireshark,,vb) bulunmaktadır.

Kali üzerinden DoS saldırısı için işletim sistemi üzerinde bulunan uygulamalar kullanılabileceği gibi, işletim sistemi terminalinden de belli komutlar girilerek DoS saldırısı gerçekleştirilebilir. Örneğin, Hping3 ve inviteflood komutları çoklu ip paketleri gönderimi ile saldırıyı gerçekleştirmektedir. Inviteflood komutunun kullanımı;

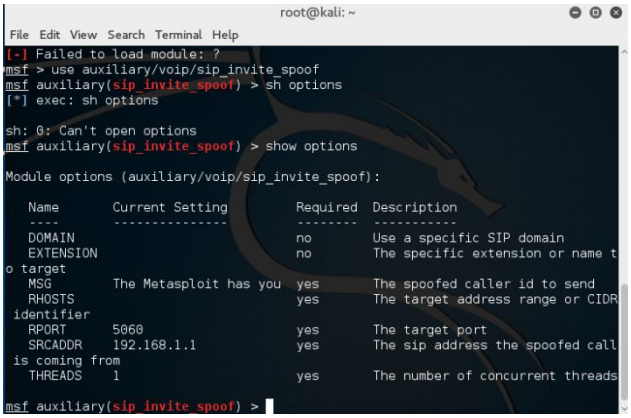
#inviteflood eth0 1000 10.131.92.74 10.131.92.74 1000 -D 5060 -S 5060 -a 1001

Bu komutta girilen değerlere bakacak olursak, eth0 ile hangi interface' in kullanılacağı, 1000 ile hedef alınan kullanıcı (UA), ilk IP ile kaynak IP'si, ikinci IP ile hedef IP'si (burada aynı girilmiştir çünkü networke dâhil olunmuş ve aynı sistemden çıkıldığı varsayılmıştır.), 1000 ile yollanacak paket miktarı, -S 5060 ile kaynak port, -D 5060 ile hedef portu, 1001 ile akışın yapılacağı sahte UA belirtilmiştir. Bu saldırı sonucunda kendisine 1000 paket ulaşan 1000 kullanıcısı, hizmet kesintisine uğrayacak ve VoIP hizmetini kullanamayacaktır.



Şekil 6. Kali Linux ile DoS saldırısı (DoS attack through Kali Linux)

Aynı saldırı yine Kali Linux işletim sisteminin bir parçası olan Metasploit uygulamasından yararlanılarak da gerçekleştirebilir. Pentest çalışmalarında sıkça kullanılan Metasploit uygulamasında VoIP ağ için de bolca kaynak bulunmaktadır. Şekil-7'deMetasploit aracılığı ile yapılmış olan DoS saldırısı gösterilmektedir.



Şekil 7. DoS saldırısının Metasploit gerçekleştirilmesi (DoS attack through Metasploit)

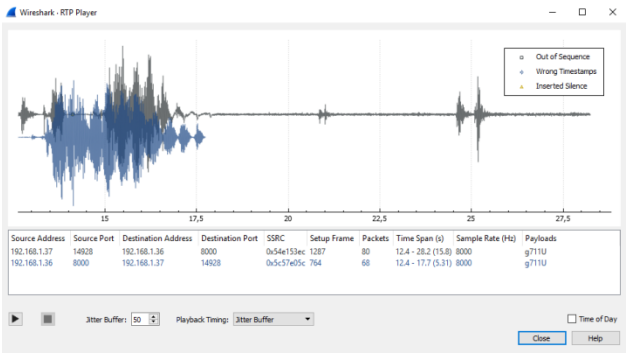
Bu saldırının nasıl gerçekleştirildiği incelenecek olursa, DOMAIN ile hedef kullanıcı bilgileri, SRCADDR ile hedefteki IP bilgisi, RHOSTS ile de saldırgan IP adresi spoof edilerek farklı IP adresi gösterilmiştir. Bu saldırı gerçekleştirildiği sırada hedef kullanıcıda Wireshark yazılımı açılarak gelen paketlerin içeriği detaylı olarak incelenmiş ve INVITE isteklerine rastlanmıştır. Bu mesajların içeriğinde, gelen bilgisinin tanımlı olduğu kısımda "Metasploit has you" ibaresinin yer aldığı görülmüştür. Bu da az önce gerçekleştirilen Metasploit DoS saldırısının hedefe ulaştığını ve gerçekleştiğini göstermektedir.

Bir diğer saldırı örneği incelemesinde ise telekulak saldırısı gerçekleştirilmiş ve yine network'e dâhil olunmuş, sniffing (dinleme) özelliğine sahip uygulama ya

da araçlar ile (bu saldırı da Wireshark kullanılmıştır) SIP mesajları paket içeriği incelenmiştir. Paketler incelenirken gerek kullanıcı bilgileri gerekse ağa dair birçok bilgi elde edinilmiştir. Söz konusu mesajlara müdahil olunarak, mesaj içeriği değiştirebileceği gibi elde edilen bilgiler ile sonrasında başka saldırılar da oluşturulabilmektedir. Ayrıca bu saldırı ile oturum kurmuş olan kullanıcılar arasındaki ses paketleri de kaydedilebilmekte ve dinlenebilmektedir. Bu saldırıyı gerçekleştirirken Kali Linux işletim sisteminde çalışan Ettercap ve Wireshark uygulamalarından yararlanılmıştır. Kullanıcılar arasında oturum kurulduktan sonra karşılıklı ses paketleri gönderimi başlamaktadır. Bu paketleri yakalayabilmek için de ağa dâhil olunarak ağ trafiğinin saldırı gerçekleştirilen yöne yönlendirilmesi gerekmektedir. ARP Poisoning ile ağa dâhil olunarak ağ üzerinde kayıtlı kullanıcıların bilgileri elde edilebilmektedir. Bunun için aşağıdaki komutun girilmesi yeterlidir:

```
# ettercap -T -M ARP -i eth0
```

Bu komut ile eth0 interface üzerinden ağa dâhil olunmuş ve ARP istekleri bu yöne çekilmiştir. Sonrasında ise Wireshark aracılığı ile tüm ses paketleri dinlenmiştir. Bu durum Şekil-8'de gösterilmektedir. Son olarak, oturum çalma saldırısı gerçekleştirilmiş ve SIP ağındaki kullanıcıların oturum bilgileri ele geçirilerek kullanıcı adı, şifre, girilen siteler, indirilen fotoğraflar gibi birçok tehlikeli bilgi elde edilmiştir.



Şekil 8. Wireshark ile RTP ses paketlerinin dinlenmesi
(Listening to RTP voice packets with Wireshark)

Kali Linux işletim sisteminde bulunan Ettercap, Hamster ve Ferret uygulamaları ile ağa dâhil olunarak dinleme işlemleri gerçekleştirilebilmektedir. Bir önceki saldırıda ağa dahil olunduğu gibi burada da yine Ettercap ile ARP Poisoning yapılarak ağa dahil olunmuş ve Hamster ile de interface üzerinden geçen trafiğin çalma işlemi gerçekleştirilmiştir. Şekil-9'da Hamster ile çalma işlemi görülmektedir. Ferret ile dinlemeyi yapan saldırgan, Hamster ile de bilgileri ve oturumu çalmaktadır. Dinlenilen ağ trafiğinin saldırı anındaki tüm aksiyonları yakalanabilmektedir.

```
root@kali:~# hamster
--- HAMPSTER 2.0 side-jacking tool ---
begining thread
Set browser to use proxy http://127.0.0.1:1234
DEBUG: set_ports_option(1234)
DEBUG: mg_open_listening_port(1234)
Proxy: listening on 127.0.0.1:1234
hamster.txt: unknown entry contents
```

Şekil 9. Hamster ile çalma işleminin gerçekleştirilmesi
(Stealing with Hamster)

5.4. Alınması Gereken Güvenlik Önlemleri (Security Precautions to Be Taken)

Anlık hizmet kesintisine yönelik saldırıların tespitinde genellikle IDS/IPS sistemleri kullanılmaktadır. Bu sistemler ile aynı anda gönderilen çoklu miktar paketler tespit edilip sistem, yöneticisini uyarabilir. Sınırlandırma, ağ içerisinden olmayan kullanıcılardan gelen paketlerin kabul edilmemesi şeklinde olabileceği gibi tek IP üzerinden gelen paket adedini sınırlandırma şeklinde de olabilmektedir. Ayrıca sunucu üzerinden gerçekleşen saldırı anında "ngrep" benzeri araçlar ile de ağ paketleri izlenerek saldırı manuel olarak tespit edilebilmektedir.

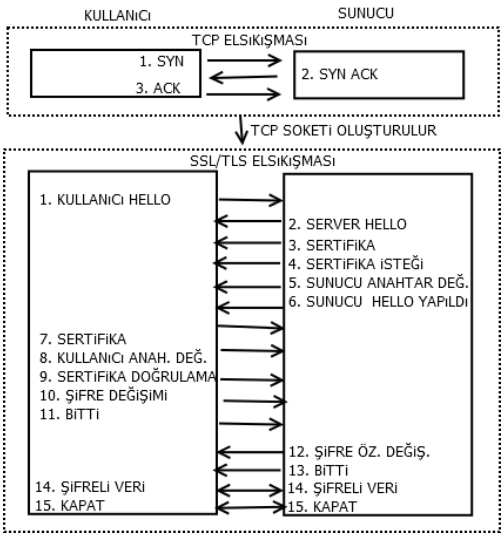
Kali işletim sisteminde çalışan ve IDS/IPS özelliği sunan Snort uygulaması ile sınırlandırma ve engelleme için kurallar oluşturularak SIP ağına uygulanması ile de saldırılar engellenebilmektedir. Aşağıdaki komut ile tek IP adresi üzerinden çoklu istekler sınırlandırılabilmektedir.

>>alerttcpanyany -> SIP_PROXY_IP any \ (msg: "TCP SYN packetfloodingfromsinglesource"; \ threshold: typeboth, trackbysrc, count 100, seconds 20; \ flow:stateless; flags:S,12; sid:5000100; rev:1;)

Gerçekleştirilen Inviteflood atağını önlemek için tanımlanabilecek olan kurallardan birisi de aşağıdaki gibidir. Bu kural ile çoklu invite paketi gönderimi olması durumunda, Snort "Possible TCP DoS be Careful" şeklinde alarm üretecek ve hedef sistemi uyaracaktır.

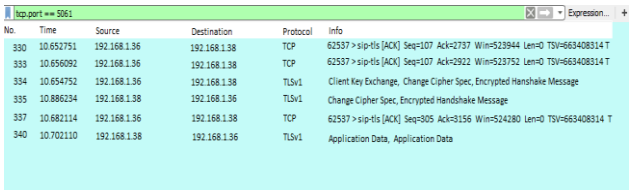
>>alert ip anyany -> SIP_PROXY_IP SIP_PROXY_PORTS \ (msg: "Possible TCP DoS Be Careful!"; content:"INVITE"; depth:6 ; \ threshold: typeboth, trackbysrc, count 100, seconds 60; \ sid:1000100; rev:1;)

Telekulak ve oturum çalma saldırılarında, sisteme dahil olduktan sonra paketleri yakalamak ve içeriğini izlemek çok kolay olduğu için, bu tarz saldırıları önlemek amaçlı şifreleme teknolojileri kullanılmalıdır. Özellikle IPSEC ya da Şekil-10'da çağrı akışı verilen TLS ile oturum ve bağlantının şifrelenmesi ile saldırgan oturum bilgilerine de (IP, kullanıcı ID, domain, vb) ses kayıtlarına da ulaşamayacak olup, sistemin güvenliği sağlanacaktır.



Şekil 10. SIP TLS ile çağrı akışı (Call stream with SIP TLS)

IPSEC, ağ boyunca iletilen verilerin şifrelenerek gönderilmesini sağlamakta iken, TLS oturumun güvenli yapılmasına olanak vermektedir. SIP TLS uygulanarak oturumun güvenli hale getirilmesi, kullanılan SIP sunucular üzerinde gerekli konfigürasyonların yapılması ile mümkün olmaktadır. Üretilen RSA özel anahtarlar ile istek yapan kullanıcılar ve sunucu arasında anahtar değişimi yapılarak, şifrelenen ve özel anahtarlar ile açılması gereken bağlantı bilgileri açılarak güvenli bağlantı kurulumu gerçekleştirilir. SIP için güvenilir olmayan bağlantı da 5060 portu kullanılıyor iken TLS sonrası güvenilir bağlantı da 5061 portu kullanılmaktadır. Şekil-11'de SIP TLS paketleri görülmektedir.



Şekil 11. SIP TLS paketleri (SIP TLS packages)

4. SONUÇLAR VE ÖNERİLER (CONCLUSIONS AND SUGGESTIONS)

Bu çalışmada, SIP tabanlı çalışan sistemlerin tanıtımı yapılarak olası saldırılara yönelik alınması gerekli olan güvenlik önlemleri açıklanmıştır. Saldırı gerçekleştirilecek olan sistemin açıkları bulunduktan sonra, bulunan veriler de değerlendirilerek hangi saldırı yapılacağı belirlenmiş ve bu saldırıların nasıl gerçekleştirildiği tanımlanmıştır.

İlk saldırı tipinde DoS kullanılmış ve sunucu bilgileri port tarama programları ile elde edildikten sonra Kali işletim sistemi üzerinden SIP sunucusuna çoklu INVITE istekleri yapılmış ve bu isteklerin sunucu üzerindeki etkisi incelenmiştir. Tamamen güvensiz olan sistemin de güvenli olan sistemin de bu saldırıdan etkilendiği, bu saldırı için tamamen koruma sağlanamadığı fakat anlık izleme yazılımları (IDS/IPS) ile çoklu taleplerin görüntülenebildiği belirlenmiştir. Ayrıca firewall kullanımı ile de söz konusu saldırı paketleri ulaştığında, önceden tanımlı politikalar ile çoklu paket saldırıları belirlenerek paketler engellenebilir. Fakat maalesef bu saldırının çok fazla farklı çeşitleri olup, hepsine ait kural ve politika girmek mümkün değildir. Bu nedenle alınması gereken en büyük önlem, sunucunun dış dünya ile iletişimini kesmek ve sadece yerel ağ içerisinde ulaşımı mümkün kılmaktır. İkinci saldırı tipinde ise telekulak yapılmış ve sunucuya kayıtlı kullanıcılar arasına müdahil olunmuş ve oturum bilgileri, yaptıkları görüşmeler ele geçirilmiştir. Wireshark paket yakalama programı ile iletilen paketlerin içerisinde taşınan ses kayıtları dinlenmiş ve konuşmalar farklı bir alana kaydedilmiştir. Gerek oturuma müdahil olunması gerekse ses paketlerinin dinlenmesi ile sistemin savunmasızlığı gözler önüne serilmiştir. Saldırıdan etkilenmemek için alınması gereken güvenlik önlemi şifreleme olarak belirtilmiş ve TLS kullanımı ile 5060 portu kullanılarak oluşturulan oturumlar 5061 portuna alınmış ve güvenli oturum olması amacı ile TLS gövdeleri şifrelenmiştir. Ayrıca IPSEC kullanımı ile de tüm veri paketleri şifrelenmiştir. Bu şekilde bir koruma ile telekulak saldırısı gerçekleştirmek isteyen bir saldırganın başarılı olması mümkün değildir. Fakat bu koruma ile de sisteme ek yük binmekte ve hattın kullanım oranı artmaktadır. Bunu önlemek içinse çeşitli QoS (quality of service) konfigürasyonları ile gerek ses ve data(veri) trafiği ayrılabilir, gerekse öncelik tanımlanabilir ve bant genişliğini belli akışlar için ayarlama yapılabilir. Son saldırı türü olan oturum çalma saldırısında ise, ağa dâhil olunarak, ağ üzerinden geçen trafik, saldırı gerçekleştirilen bilgisayara ARP Poisoning ile yönlendirilmiştir. Bu yönlendirme sonucunda kullanıcıların yaptığı her arama, indirdiği her dosya rahatlıkla saldırgan bilgisayar tarafından yakalanmış, hatta kullanıcı adı ve şifreleri de elde edilmiştir. Söz konusu saldırıdan etkilenmemek, ağı tamamen güvenilir tutmak için yine şifreleme yapılarak SIP için kullanılan 5060 portu yerine güvenilir iletişim sağlayan SIP portu olan 5061 portu kullanılmıştır. Bu portu kullanabilmek için IPSEC, TLS, S/MIME gibi mesaj içeriklerini şifreleyen veya güvenilir oturum başlatan teknolojiler uygulanmaktadır. Uygulamamızda, SIP TLS tercih edilmiş ve oturum başlatmak için talep geldiğinde, TLS protokolü ile TCP (güvenilir bağlantı) handshaking gerçekleştirilmiş ve bağlantı verileri şifrelenmiştir. Bu korumanın alınmasından sonra ağa dâhil olmaya çalışan saldırgan, public ya da private (hangi şifreleme türü kullanılıyor ise) şifreyi bilmediği sürece oturum başlatamayacaktır.

Bu çalışma ile SIP protokolü ve ona karşı gerçekleşen saldırılar incelenmiş ve bu saldırılara karşı hangi önlemlerin alınması gerektiği belirlenmiştir. SIP protokolünün VoIP teknolojisi içinde en yaygın kullanılan protokol olması sebebiyle, ona karşı yapılacak olan saldırılara karşı nasıl korunma yöntemi belirlenmeli ve sistemin zayıf yönleri bulunarak gerekli tedbirlerin alınması gerekmektedir. SIP gerçek zamanlı bir protokol olduğu için kısa süreli bir saldırının bile kritik sonuçlar doğurabileceği unutulmamalıdır. Tek katmanlı bir

güvenlik protokolünün kullanılması yerine tam koruma sağlanması için farklı katmanlarda farklı işlevleri olan güvenlik protokolleri kullanılmalıdır.

KAYNAKLAR (REFERENCES)

[1] A. Steffen, D. Kaufmann, Andreas Sticker, **Comparative overview of the security mechanisms recommended by the SIP standard**, LectureNotes in Informatics (LNI) P-55, BonnerKöllenVerlag 2004.

[2] V. Kumar, M. Korpi, S. Sengodan, **IP Telephony with H323: Architectures for Unified Networks and Integrated Services**, John Wiley&Sons, 2001.

[3] K.K. Tan, H.L. Goh, "Session Initiation Protocol, Industrial Technology", IEEE ICIT '02. 2002 IEEE International Conference, IEEE ICIT'02, THAILAND, 2002, 2, pp. 1310 - 1314, 11-14 Dec. 2002.

[4] R. Zhang, X. Wang, X. Yang, X. Jiang, "On the billingvulnerabilities of SIP-basedVoIPsystems", *Computer Networks*, 54(11), 1837-1847, 2010.

[5] A. D. Keromytis, "A ComprehensiveSurvey of Voice over IP Security Research", *IEEE Communications Surveys&Tutorials*, 14(99), 2012.

[6] E. Y. Chen, "DetectingDoSattacks on SIP systems", **1st IEEE Workshop on VoIP Management and Security 2006**, pp. 53-58

[7] Q. QIU, **Study of Digest Authentication for Session Initiation Protocol (SIP)**, Master's Project Report, University of Ottawa, December, 2003.

[8] C. Shen, E. Nahum, H. Schulzrinne, C. Wright, "The Impact of TLS on SIP Server Performance: Measurement and Modelling", *IEEE/ACM Transactions on Networking*, 20(4), 1217-1230, 2012.

[9] S. Islm, M. Rahman, "Voip End-to-End Security Using S/MIME and a Security Toolbox", *Global Journal of Computer Science and Technology*, 14(5), 39-42, 2014.

[10] E. C. Cha, H. K. Choi and S. J. Cho, "Evaluation of Security ProtocolsfortheSessionInitiation Protocol,"**2007 16th International Conference on Computer Communications and Networks**, HI, 2007, Honolulu, pp. 611-616.

[11] Yang C-C, Wang R-C, Liu W-T, "Secure authentication scheme for session initiation protocol", *ComputSecur*, 24(5), 381–386, 2005

[12] M.Voznak and J. Safarik "DoS attacks targeting SIP server and improvements of robustness", *International Journal of Mathematics and Computers ın Sımulatıon*, 177-184, 2012.

[13] I. Özçelik, R.R. Brooks, "Deceiving entropy based DoS detection", *Computers&Securıty*, 48, 234-245, 2015.

[14] H.Sengar, D. Wıjesekera, H. Wang, S. Jajodia,"VoIP Intrusion Detection Through Interacting Protocol State Machines", 2006, Dependable Systems and Networks, 2006.

[15] I.Taş, O. Özbirecikli, U. Çağal, E. Taşkın H. taş,"SIP Kayıt Silme Saldırısı Anatomisi ve Savunma Stratejileri", SIU, 2014.

[16]Y.Ding and G.Su, "Intrusion detection for signal based SIP attacks through timed HCPN", Int. Conf. On Availability, Reliability and Security. IEEE,2007.

[17] E. Rescorla, " SSL and TLS Designing and Building Secure Systems" . Addison Wesley, 2000.

[18] J. Tiller, "A technical guide to IPSec Virtual Private Networks" Auerbach publications,2000.

[19] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Spark, M. Handley, and E. Schooler, " Session Initiation Protocol", RFC 3261 IETF,2002.

[20] D. Seo, H. Lee, and E. Nuwere, "Detecting More SIP Attacks on VoIP Services by Combining Rule Matching and State Transition Models", **IFIP International Federationfor Information Processing, Volume 278; Proceedings of the IFIP TC 11 23rd International Information Security Conference**,397-411, 2008.

[21] J. Tang, Y. Cheng and Y.Hao, "Detection and prevention of SIP flooding attacks in voiceover IP networks", **2012 Proceedings IEEE INFOCOM**, Orlando, FL, 2012, pp. 1161-1169.

[22] S. Ehlert, G. Zhang, D. Geneiatakis, G. Kambourakis, T. Dagiuklas, J. Markl, D. Sisalem, "Two layer Denial of Service prevention on SIP VOIP Infastructure", *Computer Communications*, 31, 2443–2456, 2008.

[23] H. Y. Lam, C. P. Li, S. T. Chanson and D. Y. Yeung, "A Coordinated Detection and Response Scheme for Distributed Denial-of-Service Attacks,"**2006 IEEE International Conference on Communications**, 2006, İstanbul, pp. 2165-2170.

[24] T.Al-Kharobı, M.Al-Mendhar, "Comprehensive Comparison of VoIP SIP Protocol Problems and Cisco VoIP System", *International Journal of Network Security & Its Applications*, 4(4), 137-152, 2012.

[25] A. B. Johnston, **SIP: Understanding the Session Initiation Protocol**, Artech House, 2009, Boston, 3rdEdition.

[26] Internet: M. Collier, Basic Vulnerability Issues for SIP Security, http://download.securelogix.com/library/SIP_Security030105.pdf, 01.02.2017

[27] D. Sisalem, J. Kuthan and S. Ehlert, "Denial of service attacks targeting a SIP VoIP infrastructure: attack scenarios and prevention mechanisms", *IEEE Network*, 20(5), 26-31, 2006.

[28] Internet: J. Franks, P. Hallam-Baker, J. Hostetler, S. Lawrence, P. Leach, A. Luotonen, L.Stewart, HTTP Authentication: Basic and Digest Access Authentication, 1999,RFC-2617, http://www.rfc-base.org/txt/rfc-2617.txt, 01.02.2017.

[29] P. Fontanini, **VOIP Security**, Master Thesis, Gjovik University College, Dep. Of Comp. Science and Media Tech., 2008.

[30] Internet: T. Dierks, C. Allen, The TLS Protocol", IETF 1999, RFC 2246, http://www.rfc-base.org/txt/rfc-2246.txt, 01.02.2017.

[31] D. Geneiatakis et al.,, "Survey of security vulnerabilities in session initiation protocol", *IEEE Communications Surveys&Tutorials*, 8(3), 68-81,3rd. Qtr. 2006.

[32] J. S. Tiller, **A Technical Guide to IPSec Virtual Private Networks**, New York, Auerbach Publications,December- 2000.

[33] G. Asghar, **Security Issues of SIP**, Master Thesis, Blekinge Institute of Technology, School of Engineering June- 2010.