VoIP Görüşmelerinde Güvenlik Yöntemleri

ÖZ

Şifreleme kullanarak görüşmelerin dinlenmesini veya anlaşılmasını önleyin.

Güvenli ağlar kullanarak görüşmelerin ağ üzerindeki güvenliğini sağlayın.

Kimlik doğrulama kullanarak yalnızca kullanıcının kendi hesabına erişmesini sağlayın.

Kötü amaçlı yazılımlardan korunmak için antivirüs ve güvenlik yazılımı kullanın.

Güvenli şifreler kullanarak kimlik bilgilerinizi koruyun ve kötü amaçlı yazılımlardan kaçının.

.

Giriş

Günlük hayatımızın birçok alanında internet yer almaktadır. Mevcut internet altyapımız üzerinden VoIp (Voice over IP) teknolojisi ile ses ve video iletimi gerçekleşmektedir. Gerçek zamanlı olan ses iletişimi için gereksinim olan paket kayıpsız, gecikmesiz iletişim bu teknoloji ile sağlanabilmektedir. 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. VoIP teknolojisinde iki tür protokol kullanılır. Sinyalleşme protokolleri ve medya iletim protokolleri. Sinyalleşme için SIP ve H323 protokolleri, medya iletimi için ise RTP protokolü kullanılır. RFC 3261 belgelerinde 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.

VoIP, Paket anahtarlamalı IP ağı üzerinden ses iletimidir. Analog işaretler sayısal işaretlere dönüştürülüp sıkıştırılır, paketlere bölünerek IP ağı üzerinden gönderilir ve alıcıda tekrar analog işaretlere dönüştürülür. Böylece tek bir IP ağı üzerinden veri, ses ve video iletimini sağlanır. VoIP'in artan popülerliğinde etkili olan faktörlerin başında düşük maliyet ve telefon servislerine yeni servislerin (video, konferans.) ve uygulamaların eklenme kolaylığı gelmektedir.

VoIP Protokolleri

SIP (Session Initiation Protocol)

Oturum Başlatma Protokolü (SIP), iki ya da daha fazla katılımcı arasında bağlantı kurulmasını, oturum başlatılmasını gerçek zamanlı protokoller aracılığıyla veri taşınmasını sağlayan bir ağ protokolüdür. SIP, sesli, görüntülü, sohbet veya anlık mesajlaşmanın yanı sıra etkileşimli oyunlar ve sanal gerçeklik oturumları başlatmak için yaygın olarak kullanılır.

SIP, IETF tarafından RFC 3261,3262, 3263, 3264 ve 3265'te tanımlanmış bir protokoldür. SIP, uygulama katmanında çalışan bir protokoldür. Sunucu- istemci mantığı ile çalışır. Çoklu ortam ya da ses oturumlarının başlatılması, değiştirilmesi veya sonlandırılması için kullanılır.

Proxy Server: SIP isteklerini alıp bir ilgili sunucuya iletir.

Redirect Server: UAC'dan gelen bilgileri yorumlar.

Registration / Location Server: SIP kullanıcılarından kaydolma isteklerini alıp asıllamayı yapar ve kullanıcıların o anki yer bilgisini günceller.

Bir SIP isteği alındığında bu istek için next-hop'u belirler ve kullanıcıya bildirir.

SIP sinyalleşmesi sırasında kullanılan SIP mesajları aşağıdaki gibidir:

INVITE: Oturumu başlat

ACK: Son gelen cevabı onayla **BYE**: Oturumu sonlandır **CANCEL**: İptal et

REGISTER: Kaydolma

INFO: Oturum sırasındaki bilgilendirmeler

OPTIONS: Desteklenen özellikler

REFER: Taraflara SIP isteğini işlemesi isteğinde bulunma (örn: transfer)

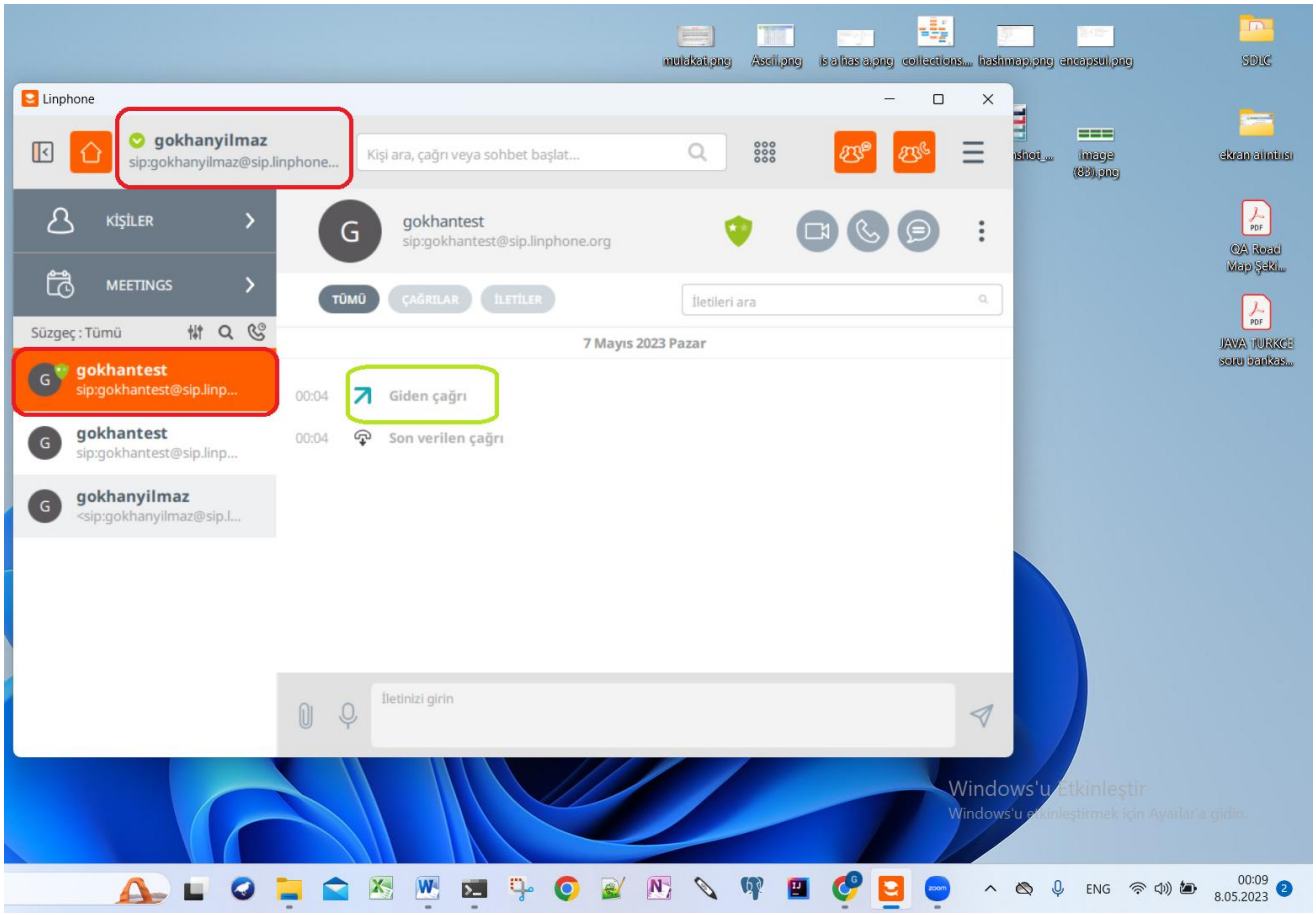
NOTIFY: Aboneleri bilgilendirme

SUBSCRIBE: Bir olaya abone olmak (örn: presence, adres defteri.)

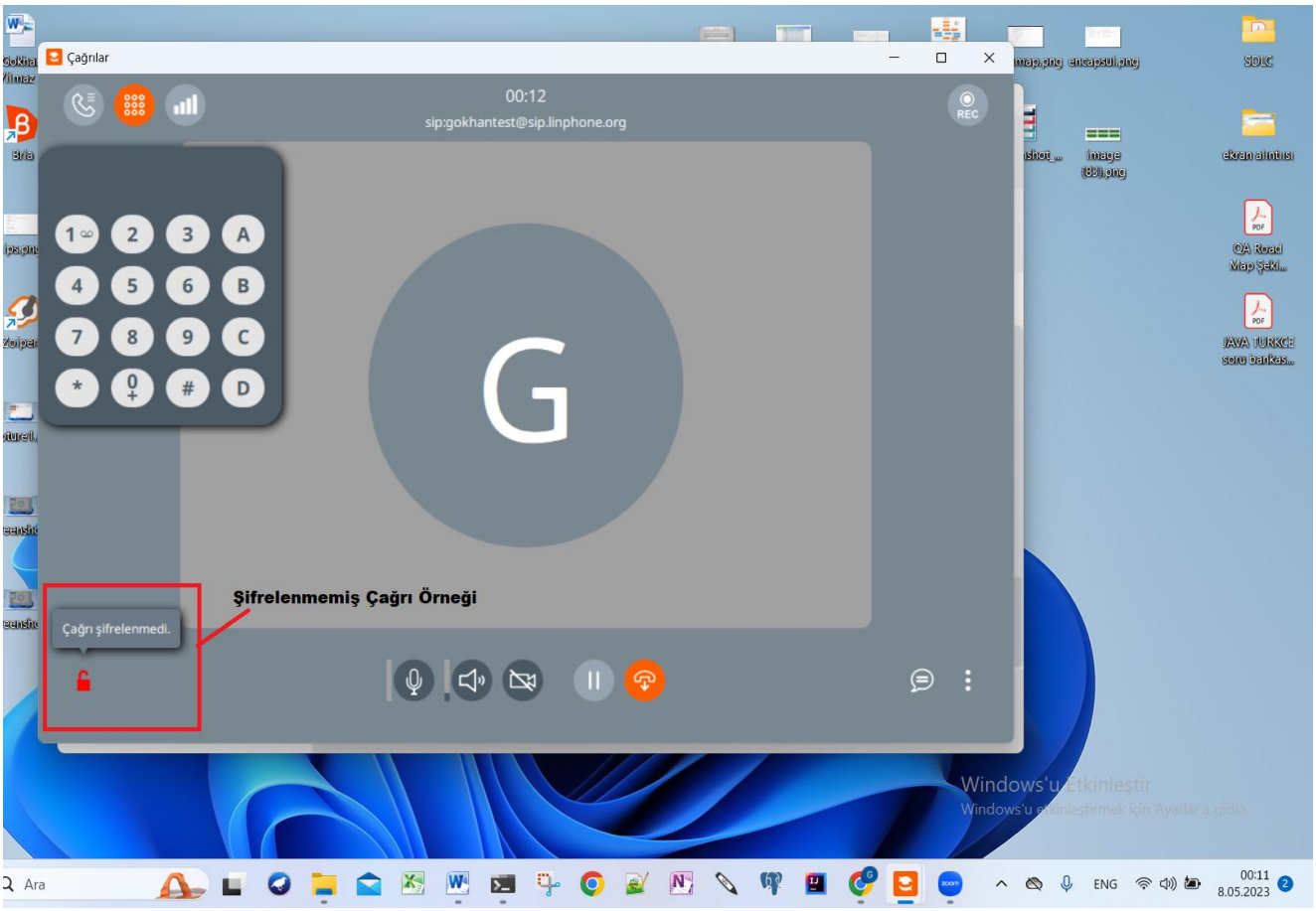
SIP mesajlaşmasında kullanılan cevap kodları, aşağıdaki gibi gruplara ayrılmıştır:

- 1xx – Geçici cevaplar (100 Trying, 180 Ringing)
- 2xx – Başarılı (200 OK, 204 No Notification)
- 3xx – Yönlendirme (301 Moved Permanently, 305 Use Proxy)
- 4xx – istek başarısız (400 Bad Request, 404 Not Found)
- 5xx – Sunucu kaynaklı hata (502 Bad Gateway, 505 Version Not Suported)
- 6xx – Genel hata (600 Busy Everywhere, 608 Rejected)

TCP Protokolu Kullanılarak 2 ayrı softphone uygulaması arasında yapmış olduğum aramanın uçtan uca şifrelenmemiş çağrı sonuçları aşağıdaki şekilde bulunmaktadır.(Şekil 1 , Şekil 1.1)

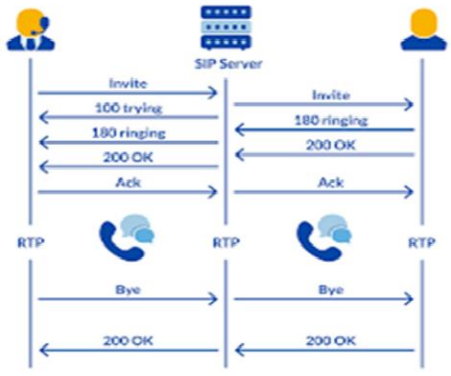


Şekil 1



Şekil 1.1

Basit bir VoIP görüşmesinin yapılabilmesi için gerekli oturumun kurulması, kontrolü ve sonlandırılmasını gösteren örnek bir SIP sinyalleşmesi şekilde görüldüğü gibidir:




```
INVITE sips:Bob@TMC.com SIP/2.0
   Via: SIP/2.0/TLS client.ANC.com:5061;branch = z9hG4bK74bf9
   Max-Forwards: 70
   From: Alice<sips:Alice@TTP.com>;tag = 1234567
   To: Bob<sips:Bob@TMC.com>
   Call-ID: 12345601@192.168.2.1
   CSeq: 1 INVITE
   Contact: <sips:Alice@client.ANC.com>
   Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, NOTIFY
   Supported: replaces
   Content-Type: application/sdp
   Content-Length: ...

   v = 0
   o = Alice 2890844526 2890844526 IN IP4 client.ANC.com
   s = Session SDP
   c = IN IP4 client.ANC.com
   t = 3034423619 0
   m = audio 49170 RTP/AVP 0
   a = rtpmap:0 PCMU/8000
```

Şekil1: En Çok Kullanılan SIP Mesajları ve Anlamları

REGISTER: To başlığı alanında listelenen URI'yi bir SIP sunucusuna kaydetmek ve Contact başlığı alanında verilen ağ adresiyle ilişkilendirmek içindir.

INVITE: Arama yapmak için bir iletişim başlatır. İstek bir kullanıcı istemcisi (ör. IP telefon) tarafından bir SIP sunucusuna gönderilir. Hali hazırda kurulmuş bir iletişim sırasında gönderildiğinde (RE-INVITE), oturumu değiştirir (ör. çağrıyı beklemeye alma).

ACK: Bir INVITE isteğine son bir yanıt aldığını doğrulamak için kullanılır.

BYE: Bir iletişimin sonlandırıldığını bildirir ve çağrıyı bitirir.

CANCEL: Bekleyen tüm istekleri iptal eder. Hala çalan bir çağrıyı cevaplamadan önce, sonlandırmak için kullanılır.

UPDATE: İletişim durumunu değiştirmeden oturumun durumunu değiştirir

REFER: Alıcıdan çağrıyı aktarmak amacıyla bir talepte bulunmasını ister.

PRACK: Geçici onay. Geçici bir yanıta yanıt olarak gönderilir.

SUBSCRIBE: Bir bildirimden gelen olayların bildirilmesi için bir abonelik başlatır.

NOTIFY: Yeni bir etkinliğin bildirimlerini bir aboneye bildirmek için kullanılır.

PUBLISH: Bir etkinliği bildirim sunucusunda yayınlamak için kullanılır.

MESSAGE: Kısa mesaj gönderir. Anlık mesajlaşma uygulamalarında kullanılır.

INFO: Oturum durumunu değiştirmeyen oturum ortası bilgileri göndermek için kullanılır. Bu yöntem genellikle DTMF rölesi için kullanılır.

OPTIONS: Bir uç noktanın yeteneklerini sorgular. Genellikle NAT ve keepalive için kullanılır.

SIP mesajlarında çok sayıda gizli bilgi açık bir şekilde iletilmektedir. Bağlantıda kullanılan IP ve port bilgileri, kullanıcı adları, SIP adresleri, kullanımda olan codec bilgisi gibi. Bu özellikleri, SIP protokolünde güvenlik açığı oluşturmaktadır.

RTP (Real-Time Transport Protocol)

RTP protokolü, gerçek zamanlı veri iletimi için kullanılır. RTP, ses ve video iletimi için standartlaşmış bir protokoldür. Ulaşım katmanında UDP protokolünü kullanır.

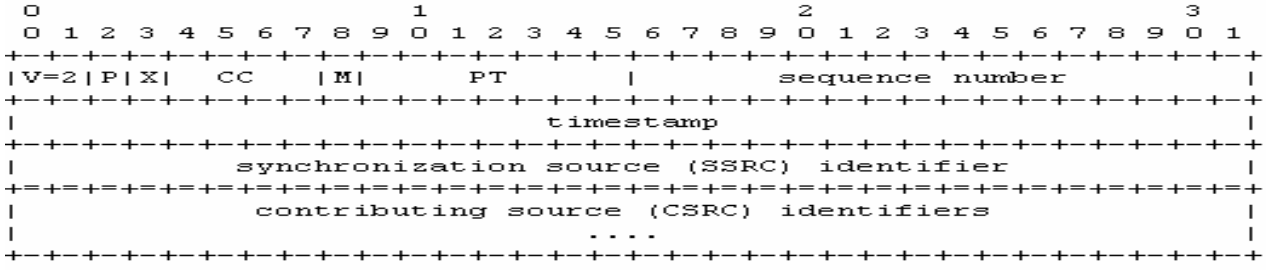
Bir VoIP görüşmesinde karşılıklı olarak (bir gidiş, bir geliş) olarak iki RTP ve bir RCTP oturumu kurulur. RTP, sırasız gelen paketleri sıralar. RTP protokolünün ‘dizi numarası’ ve ‘zaman damgası’ adlarında iki önemli bilgi biti bulunmaktadır. RTP, UDP gibi bağlantısız protokollere paketin alındığına dair birtakım bilgiler ekler.

RTP sahip olduğu dizi numaraları sayesinde veriyi alan tarafta ses veya görüntünün tekrar birleştirme işini kolaylaştırır. Bununla birlikte, RTP’nin içerdiği zaman damgası etiketi ile de sistemdeki senkronizasyon işlemleri gerçekleştirilmektedir. Tüm RTP mesajları aynı formattadır. Bu mesajlar farklı yüklerdeki verileri taşımak için tasarlanmışlardır. Bu yükler arasında G.729 gibi ses kodlayıcıları (codec) yapıları olabildiği gibi JPEG görüntü standardı da bulunabilir. Örnek bir RTP başlığı ve RTP protokolünün sağladıkları şu şekildedir;

Zaman Etiketleme

Kaynak Belirleme

Bu başlıkta bulunan PT alanı, RTP payload tipini ve formatını belirtir



Şekil2: RTP Başlığı

VoIP Güvenlik Tehditleri

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.

VoIP için var olan güvenlik tehditlerini aşağıdaki gibi gruplayabiliriz:

- Hizmeti Engelleme (Dos-Denial of Service)
- Telekulak (Eavesdropping)
- Ortadaki Adam Saldırısı (Man-in-the-middle Attack)
- Yanıltma (Spoofing)
- Dolandırma (Fraud)

Hizmetin Engellenmesi (DoS ve DDos Saldırıları)

DoS saldırısı, hizmeti engellemeye yönelik bir saldırı türüdür. DoS; disk alanı, bandgenişliği, işlemci zamanı gibi kaynakları tüketmek; konfigürasyon bilgilerini bozmak, DoS ya da DDoS ataklarında, mevcut SIP sunucusunun hizmetinin kesintiye uğratılması veya servis yanıltma amaçlanır.

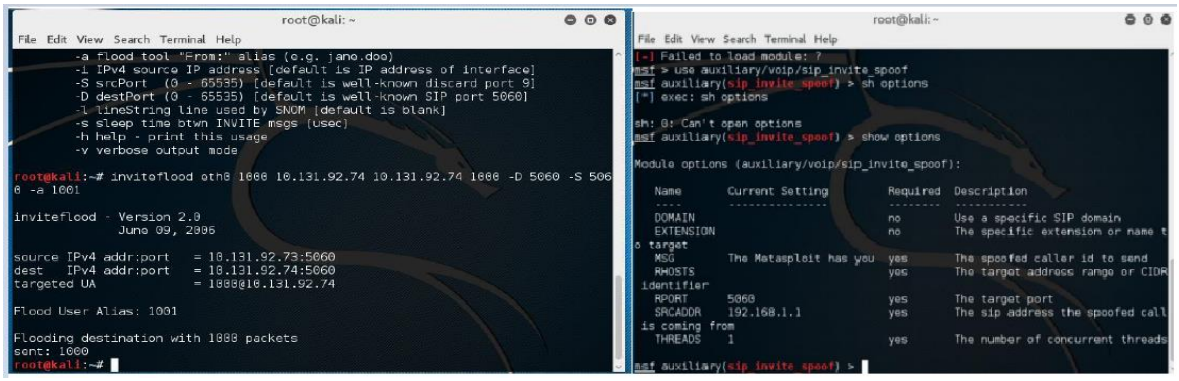
Yeterli bilgileri ele geçirdikten sonra, sunucu savunmasız kalmaktadır. Aynı anda birden fazla saldırganın hedef sunucuyu etkisiz hale getirmek için yaptığı DDoS saldırıları SIP için en sık karşılaşılan ve en ağır sonuçlar doğuran saldırı çeşididir.

Bu saldırıyı gerçekleştirebilmek için çeşitli saldırı araçları bulunmaktadır; bu saldırı için en bilineni ise 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.

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.

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. Her iki saldırı içinde örnek çıktılar aşğıdaki gibidir.



Şekil3: Kali Linux ile DoS saldırısı- Metasploit ile DoS saldırısı gerçekleştirilmesi

Telekulak Saldırısı (Wiretapping Attack)

Telekulak saldırısı, istenmeyen kişiler tarafından, özel telefon görüşmelerinin dinlenmesi ya da kaydedilmesidir. Günümüzde birçok uygulamada telefonda, sosyal güvenlik numarası, kredi kartı bilgileri gibi kritik, kişiye özel bilgilerin verilebildiği göz önünde bulundurulursa, telekulak saldırısı, çok önemli sonuçlar doğurabilir. Bu saldırıda ağa erişerek veri paketlerine erişim ve kişisel bilgilere ulaşılması amaçlanmaktadır. Saldırgan sistem üzerindeki zafiyet ve açıkları bulmak amacı ile de telekulak saldırısı yapabilir. VoIP teknolojisinde, erişimin kolay olması nedeni ile IP ağına erişimi bulunan saldırganın iletilen paketleri görüntüleyebilir ve yakalayabilir.

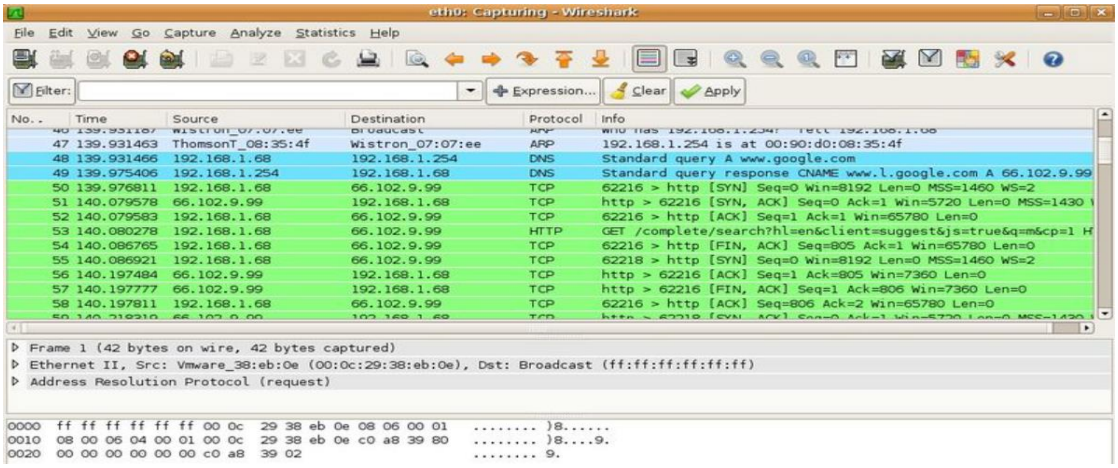
VoIP kullanımı, geleneksel telefon sistemindeki tapping teknikleriyle karşılaştırıldığında; geleneksel telefon sistemindeki telekulak saldırısında, saldırısı ile bir telefon görüşmesine erişilebilirken VoIP ağına yapılan bir telekulak saldırısı ile birden fazla VoIP oturumuna (telefon konuşmasına) ulaşılabilir. Bu yönden VoIP ek riskler getirmektedir.

VoIP ağında telekulak saldırısını kolaylaştıran etkenlerin başında, sesin iletiminde kullanılan RTP protokolünde şifreleme ya da asıllama yapılmıyor olmasıdır. RTP başlığında PT (payload type) alanında kullanılan codec ile ilgili bilgi vardır. İnternette kolayca erişilebilen, RTP trafiğini kaydetmeye yarayan araçları kullanarak RTP trafiğini kesip kaydeden biri, codec bilgisi de elinde bulunduğundan, bu RTP trafiğini daha sonra decode edip dinleyebilir ya da tekrarlama saldırıları gibi birçok saldırı amacıyla kullanabilir.

Şekil4: Telekulak saldırısı

Ortadaki Adam Saldırısı (Man in the Middle Attack)

Ortadaki adam saldırısı (man-in-the-middle attack), araya girenin, tarafların haberi olmadan iki taraf arasındaki mesajları okuyabilmesi ve değiştirebilmesi olarak tanımlanabilir. Ortadaki adam saldırısı, DoS ya da telekulak gibi diğer saldırı türlerini gerçekleştirmek için de kullanılabilir.



Şekil5: Wireshark ile paketlerin dinlenmesi

Bu saldırılar, farklı şekillerde gerçekleştirilebilir:

- Kayıt bilgilerini değiştirmek (Registration Manipulation)
- 3XX Cevap kodlarını kullanmak (Call Redirect)

Kayıt Bilgilerinin Değiştirilmesi (Change of Register Data)

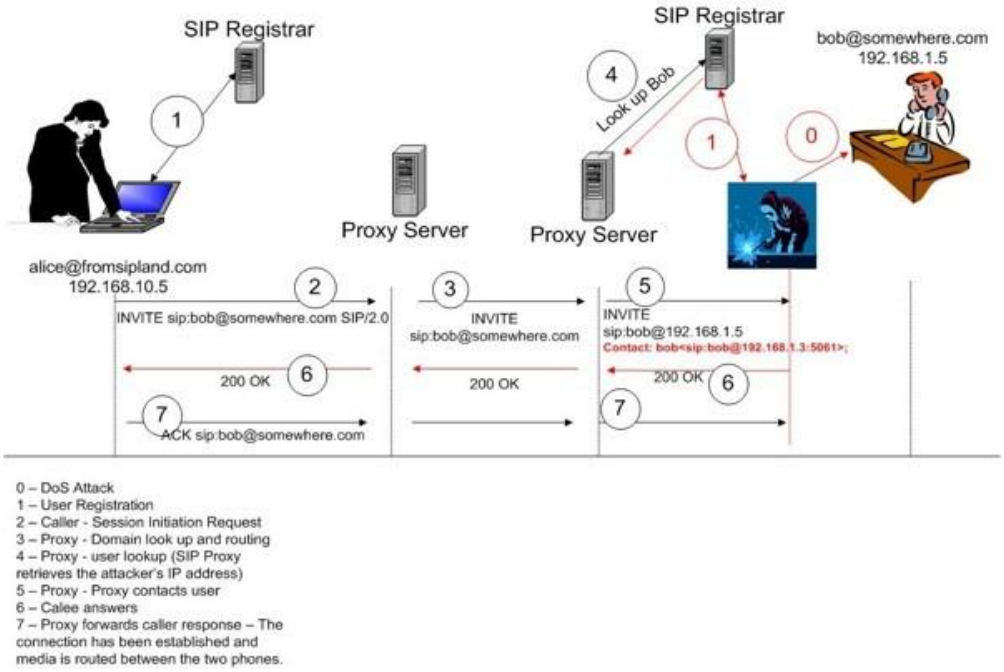
Bu saldırı türünde, saldırıda bulunan, sistemdeki kullanıcıların kayıt bilgilerini değiştirerek, kullanıcıya gelen tüm isteklerin kendisine yönlenmesini sağlayabilir.

Registrar sunucusu, UA (user agent)'in kimliğine göre doğrulama yapar. Bir SIP isteğinin 'from' başlığı değiştirilerek kolaylıkla sahte kayıtlar yapılabilir. Aynı zamanda kayıt isteklerinin gönderilmesi için kullanılan UDP protokolü, bağlantısız bir protokoldür ve kolayca spoof edilebilir. SIP Registrar sunucusu, kayıt isteğinde bulunan kullanıcıları (UA), asıllamak zorunda olmadığından genelde güvenilir olduğuna inanılan intranet içinde asıllama yapılmaz.

Asıllama yapılsa bile, güçlü bir asıllama algoritması kullanılmaz; yalnızca kullanıcı adı, şifre ve zaman damgasının MD5 özü kullanılır.

Saldırgan, öncelikle Bob kullanıcısına DoS saldırısında bulunarak bu kullanıcının terminalini iş göremez hale getirir. Daha sonra SIP Registrar sunucuya Bob kullanıcısının kullanıcı adını kullanarak kaydolma isteğinde bulunur ve böylece kayıt bilgilerini, Bob kullanıcısı saldırganın IP'sinden kaydolacak şekilde değiştirir. Bu aşamadan sonra, Bob'un kayıtlı olduğu SIP proxy'ye gelen tüm istekler, saldırganın IP'sine yönlendirilecektir. Alice, Bob'u aramak ister ve proxy'ye Bob'u aramak üzere bir INVITE mesajı gönderir. Proxy, isteği Bob olduğunu zannettiği saldırgana gönderir, sinyalleşme tamamlanıp çağrı kurulduğunda, Alice, Bob ile konuştuğunu zannederken, saldırgan ile konuşmaktadır.

Kayıt bilgilerinin değiştirilmesi ile yapılan saldırıya bir örnek aşağıdaki şekilde görülmektedir



Şekil6: Kayıt Bilgilerinin Değiştirilmesine dayalı ortadaki adam saldırısı

3xx Cevap Kodları Kullanımı (Call Redirect):

SIP 3XX cevap kodları, yönlendirme için kullanılır. Istekte bulunanı, isteğin gerçekleştirilmesi için yapması gerekenler konusunda bilgilendirip ilgili yere yönlendirir. SIP saldırılarındaki 3XX cevap kodları, sahte cevaplar için kullanılır.

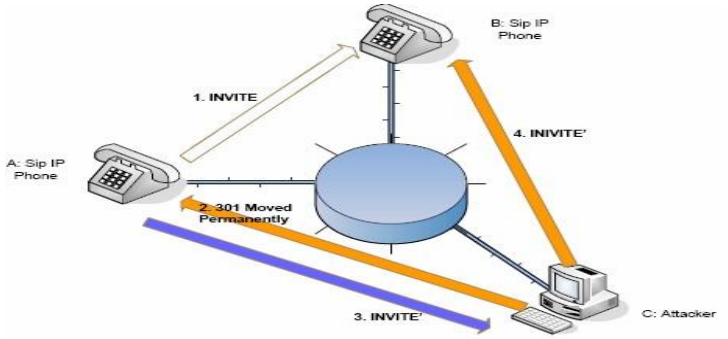
SIP sistemine kayıtlı olan bir kullanıcı, bir SIP isteğinde bulunur (örneğin INVITE isteği). Saldırıda bulunan, istekte bulunan kullanıcıya 3xx cevabı gönderir. Burada saldırgan, UA ya da SIP bileşenlerinden birinin yerine geçmiştir. 3XX mesajını alan kullanıcının haberleşmesi, saldırganın istediği tarafa yönlenmiş olur. Örnek 3XX mesajları; '301-Moved Permanently', '302- Moved Temporarily', '305- Use Proxy' gibi mesajlardır.

Bu saldırı tipine basit bir örnek, 301 mesajı kullanılarak yapılan call hijack saldırısıdır. Bu senaryoda, saldırgan, kullanıcının bir INVITE ile istekte bulunduğunu farkettiği anda, kullanıcıya 301- moved permanently mesajı gönderir ve bu mesaj ile isteği, kendisine yönlendirir. Bunun üzerine kullanıcı, SIP isteğini gerçekleştirebilmek için saldırgan ile bağlantı kurar.

Bu saldırı, SIP 302 cevap kodunun kullanılması ile gerçekleştirilebilir. Saldırgan yine SIP isteği üzerine 302- moved temporarily mesajı gönderir ve kullanıcının geçici olarak kendi Ipsine yönlendirilmiş olduğunu bildirir. Böylece geçici bir süre için kullanıcının SIP isteğini gerçekleştirmek için kendisi ile bağlantı kurmasını sağlamış olur.

Başka bir örnek de '305 – Use Proxy' mesajının kullanılması ile gerçekleştirilebilir. Bu saldırı tipinde ise, saldırgan, proxy'nin yerini almıştır. Bir kullanıcı, kayıtlı olduğu proxy'ye bir SIP isteği ilettiğinde, saldırgan 305 mesajı göndererek, kullanıcıya, yapmış olduğu istek için kendi IPsinde bulunan proxy'yi kulanmasını söyler. Böylece kullanıcı, bundan sonraki isteklerini, kayıtlı olduğu proxy yerine saldırgana gönderir.

Belirtilen saldırı tipi aşağıdaki şekilde de görülmektedir:



Şekil7: 3XX cevap kodlarını kullanarak çağrı yönlendirme saldırısı

Tekrarlama Saldırısı (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 gerçekleştirilen saldırı türüdür. Bu saldırı ile tek bir arama için oturum başlatılacakken birden çok oturum başlatılması ile birden çok arama gerçekleştirilmesi sağlanır. 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.

Dolandırıcılık (Fraud)

Teknolojinin gelişmesiyle birlikte, fraud (sahtekarlık, dolandırıcılık) saldırılarını gerçekleşmesi kolaylaşmıştır. Devre anahtarlamalı ve paket anahtarlamalı sistemlerin birleştirilmesi, sahtekarlık saldırıları için bir fırsat oluşturdu. İletişim dolandırıcılığı, telekomünikasyon sağlayıcıları ve taşıyıcıları için, en büyük sorunlardan birini oluşturmaktadır. Dünya üzerindeki iletişim dolandırıcılığı, İletişim Sahtekarlığı Kontrol Birliği (Communications Freud Control Association) tarafından denetlenmektedir.

Yazılımsal ve donanımsal araçların kolaylıkla erişilebilir olması, sahtekarlık saldırılarının hızla yaygınlaşmasına yardımcı olmaktadır. VoIP dolandırıcılığı için, birçok tehdit vardır. Bu tehditleri şu faktörler desteklemektedir.

Yeni teknolojiler, beraberinde güvenlik sınırlılıklarını ve zayıflıklarını getirmektedir.

Teknolojinin karmaşık hale gelmesi, kararsızlık ve dikkatsizliği artırmaktadır.

Alınması Gereken Güvenlik Önlemleri

Genel Önlemler

VoIP'deki güvenlik tehditleri, IP dünyasındaki VoIP'e özel olmayan diğer tehditleri de içermektedir. Bu nedenle, IP ağının güvenliği için alınması gereken önlemler, VoIP güvenliği için de gereklidir.

Öncelikle, standard bir VoIP ağında, ses, çoklu ortam ve veri paketleri aynı ağda bulunmakta ve bu nedenle de birbirlerinden etkilenmektedirler. Veri iletiminin yapıldığı IP ağına olan bir saldırı, tüm ağdaki ses görüşmelerine de zarar verecektir. Bu nedenle alınması gereken ilk önlem, ses ve veri trafiğini birbirinden yalıtmaktır. Bunun için de ses ve veri trafiği için ayrı VLAN'ler

kullanılarak ses trafiği izole edilmeli, ACL kullanarak ses ve veri VLANleri arasında erişim kısıtlanmalıdır.

VoIP ağında bulunan sunuculara istenmeyen kişilerin erişmesini engellemek amacıyla cihazlara telnet erişimi kısıtlanmalı ve SSH erişimi sağlanmalıdır.

VoIP ağının güvenliği için güvenlik duvarlarının (firewall) kullanımı da önemlidir. VoIP oturumu iki bölümden oluşur; oturumun kurulması sırasındaki sinyalleşme ve ses haberleşmesini taşıyan veri iletimi kısmı. Sinyalleşme kısmında, paketler kullanıcılar ile SIP proxy arasında gidip gelirken ses iletiminde paketler doğrudan uç terminaller (kullanıcılar) arasında iletilir. SIP kullanılan bir sinyalleşme kısmında genelde UDP/TCP 5060 portu kullanılır. Önceki bölümde bahsedilen telekulak gibi saldırılara karşı savunmasızdır. Ses verisinin iletildiği, uç noktalar arasında bulunan bağlantı için de aynı güvenlik açıkları söz konusudur. IP adreslerini gizlemek için NAT kullanılabilir. NAT, IP paketlerini üçüncü katmanda değerlendirir; IP adresi ve port değişimi sağlar. Ancak VoIP protokollerinde IP adresi bilgisi beşinci katmanda gömülü olarak bulunur. Bu da klasik NAT uygulaması ile uyumsuzluğa sebep olmaktadır. Buna çözüm olarak; VoIP uyumlu NAT cihazları ya da SBC (Session Border Controller) gibi ek bir cihaz kullanılabilir.

DoS saldırılarına karşı dayanıklılık için VoIP ağındaki sunucular için yedeklilik sağlanmalıdır (redundant network).

Ses ve sinyalleşme paketleri şifrelenmelidir.

TLS (Transport Layer Security)

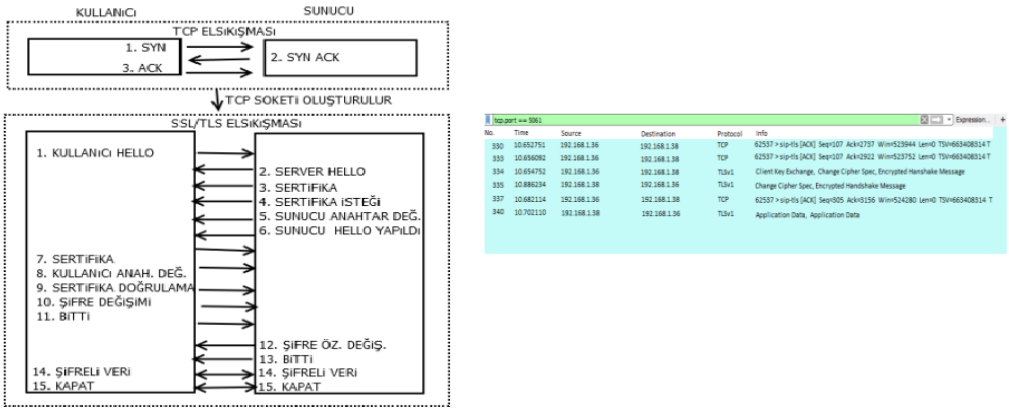
TLS, SIP mesajlarının ulaşım katmanında güvenliğinin sağlanması için kullanılır. TLS protokolü, RFC 2246'da tanımlanmaktadır. TLS, güvenli oturumların kurulmasında önemli bir rol oynamaktadır. Bu da SIP oturumunun kurulması için gerekli istemci/sunucu haberleşmesi için TLS veya SSL bağlantısı kurulması ile sağlanır. TLS protokolünün iki katmanı vardır:

TLS record protocol- simetrik anahtarlı şifreleme kullanır

TLS handshake protocol- sunucu ve istemci arasında asıllama ve şifreleme algoritmasına, kullanılacak anahtara karar verilmesi

SIP mesajındaki HTTPS benzeri SIPS URI uzantısı, TLS kullanır. Eğer SIPS URI isteğindeki route üzerinde TLS bağlantısı varsa, istek kabul edilir, aksi halde edilmez.

TLS, bağlantılı bir ulaşım katmanı protokolünün kullanımını gerektirir. Bu nedenle TCP ile kullanılır; UDP ile kullanılamaz. TLS'in UDP-tabanlı SIP sinyalleşmesinde kullanılması mümkün değildir. Normal SIP bağlantılarında güvenilir olmayan 5060 portu kullanılıyor iken TLS sonrası güvenilir bağlantı da 5061 portu kullanılmaktadır.



Şekil12: SIP TLS ile çağrı akışı ve SIP TLS paketleri

IPSec (IP Security)

IPSec, çağrı kurulması ve kontrolü için kullanılan SIP mesajlarının ağ katmanında güvenliğinin sağlanmasında kullanılır. IPSec, IETF tarafından geliştirilmiş bir protokoller bütünüdür (RFC 2401).

Iki ayrı protokolü vardır; AH (Authentication Header) ve ESP (Encapsulating Security Payload).

IPSec'de, ulaşım kipi ve tünel kipi olmak üzere iki güvenlik kipi vardır. Ulaşım kipinde yalnızca veri (payload) şifrelenir, daha güvenli olan tünel kipinde ise hem paket başlığı hem veri şifrelenir.

IPSec kullanılarak; asıllama, mesaj bütünlüğü, tekrarlama saldırısına karşı koruma ve ulaşım kontrolü sağlanır (hem ESP hem AH ile). ESP kullanılarak, ek olarak verinin şifrelenmesini ve kişisel gizlilik sağlanabilir.

SIP mesajlaşmasının güvenliği için IPSec kullanımı paket başlığına ek yük getirir.

Aşağıdaki komutlar ile tek ip adresinden gelen çoklu istekler engellenmektedir.

```
>>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;)
```

```
>>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;)
```

Şekil9: Çoklu istek ataklarını önleme komutları

SRTP (Secure Real-Time Transport Protocol)

Buraya kadar anlatılan güvenlik önlemleri, IP ağı için kullanılan genel önlemler olup, VoIP için geliştirilmiş protokoller değildirler. SRTP ise VoIP için geliştirilmiş olan bir protokol olup, VoIP'de media paketlerinin aktarılması için kullanılmaktadır. Bu nedenle raporda SRTP'ye diğer çözümlere ve protokollere göre daha geniş yer verilmiştir.

SRTP, RTP paketlerinin güvenliği için kullanılır. SRTP, Mart 2004'teIETF tarafından RFC 3711 ile yayınlanmıştır. Ses ve video gibi gerçek zamanlı verinin iletimi için kullanılan RTP protokolünün güvenliğini arttırmayı amaçlamaktadır. RTP paketlerine gizlilik, asıllama, tekrarlama saldırısına karşı koruma gibi özellikler eklemektedir. SRTP, şifreleme, asıllama gibi özellikleri ortak bir çatı altında toplarken, yüksek throughput sağlamakta ve RTP paketlerine gelecek ek yükü de minimuma indirmektedir. SRTP, RTP stack implementasyonundan ve kullanılan anahtar yönetimi algoritmasından bağımsızdır. Farklı implementasyonlar ve protokoller ile çalışabilir; ancak Multimedia Internet Keying (MIKEY)

SRTP ile çalışmak üzere tasarlanmıştır. Bu nedenle anahtar yönetimi için genelde MIKEY kullanılır.

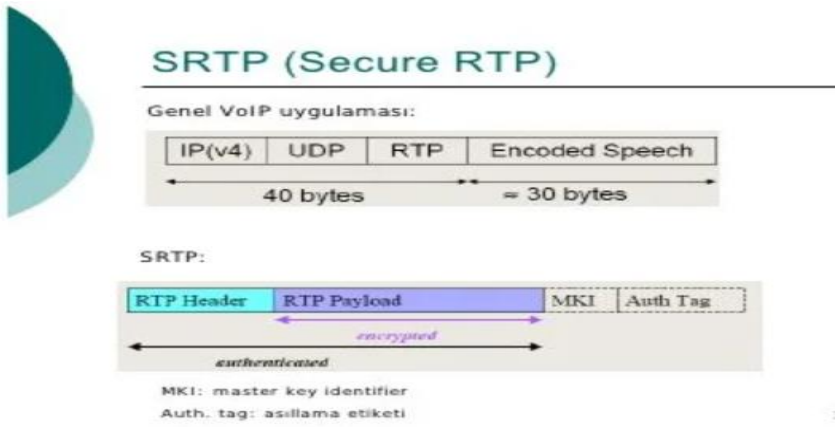
SRTP'de şifreleme, asıllama gibi tüm özellikler isteğe bağlıdır. Eğer şifreleme kullanılıyorsa,

Şifreleme için ön tanımlı olarak AES-CM (Advanced Encryption Standard- counter mode). Anahtar uzunluğu 128 bittir. Asıllama için öntanımlı olarak HMAC-SHA1 kullanılır. Asıllama anahtarı uzunluğu 160 bit ve asıllama etiketi uzunluğu 80 bittir.

SRTP'nin RTP ile karşılaştırıldığında sağladığı birçok avantaj vardır. Bunlar aşağıdaki gibi sıralanablir:

- RTP ve RTCP için payload şifrelenmesi ile sağlanan güvenilirlik
- Tekrarlama saldırısına karşı koruma ile RTP ve RTCP için mesaj bütünlüğünün sağlanması
- Oturum anahtarlarını periyodik olarak yenileme imkânı ile belli bir anahtar tarafından üretilmiş şifreli metin miktarını azaltmak

- Güvenli bir oturum anahtarı üretme algoritması (her iki uçta pseudo-random fonksiyon ile)
- Unicast ve Multicast RTP uygulamaları için güvenlik



Şekil13: SRTP Başlığı

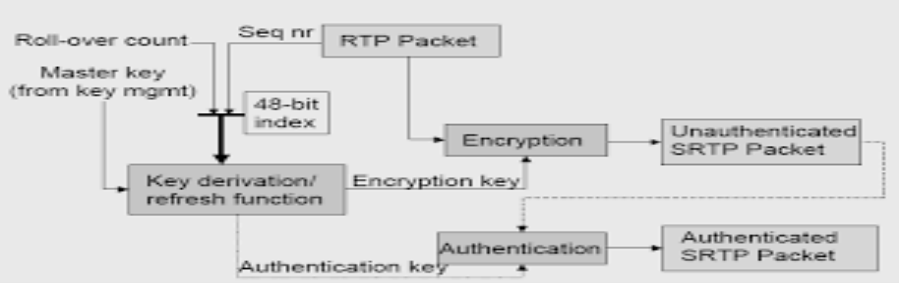
- MKI (master key identifier), hangi anahtarın kullanılacağını belirtir.
- SRTP akışına geçmeden önce SRTP kriptografik içeriğinde kullanılan parametrelere bakacak olursak;
- SEQ: sekans numarası (16 bit)
- ROC:roll over count (32 bit) RTP sekans numarasının kaç defa resetlendiği
- İndex (48 bit)

$$i=2^{16} * ROC * SEQ$$

- Asıllama algoritması belirteci
- Şifreleme algoritması belirteci
- Master anahtar
- Tekrarlama listesi (replay list)

SRTP Akışı:

Şekilde görüldüğü gibi, SRTP'de öncelikle, RTP mesajının sekans numarası ve ROC kullanılarak 48 bitlik index hesaplanır. Index ve master anahtar, anahtar elde etme ve yenileme fonksiyonundan geçirilerek biri şifreleme anahtarı ve diğeri asıllama anahtarı olmak üzere iki anahtar elde edilir. Şifreleme anahtarı kullanılarak RTP paketi şifrelenir. Şifrelenmiş olan metin, asıllama anahtarı kullanılarak asıllanmış SRTP paketi elde edilir.



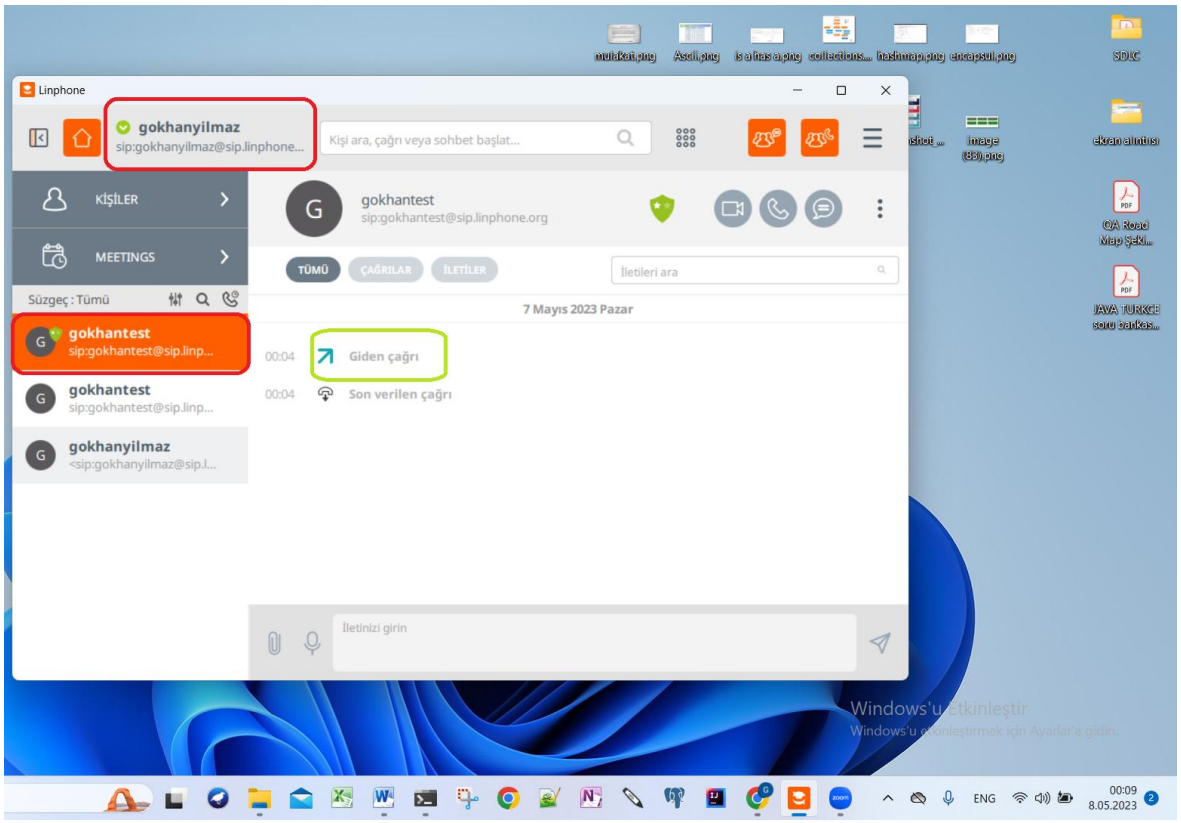
Şekil14: SRTP Akışı

SRTP Şifreleme:

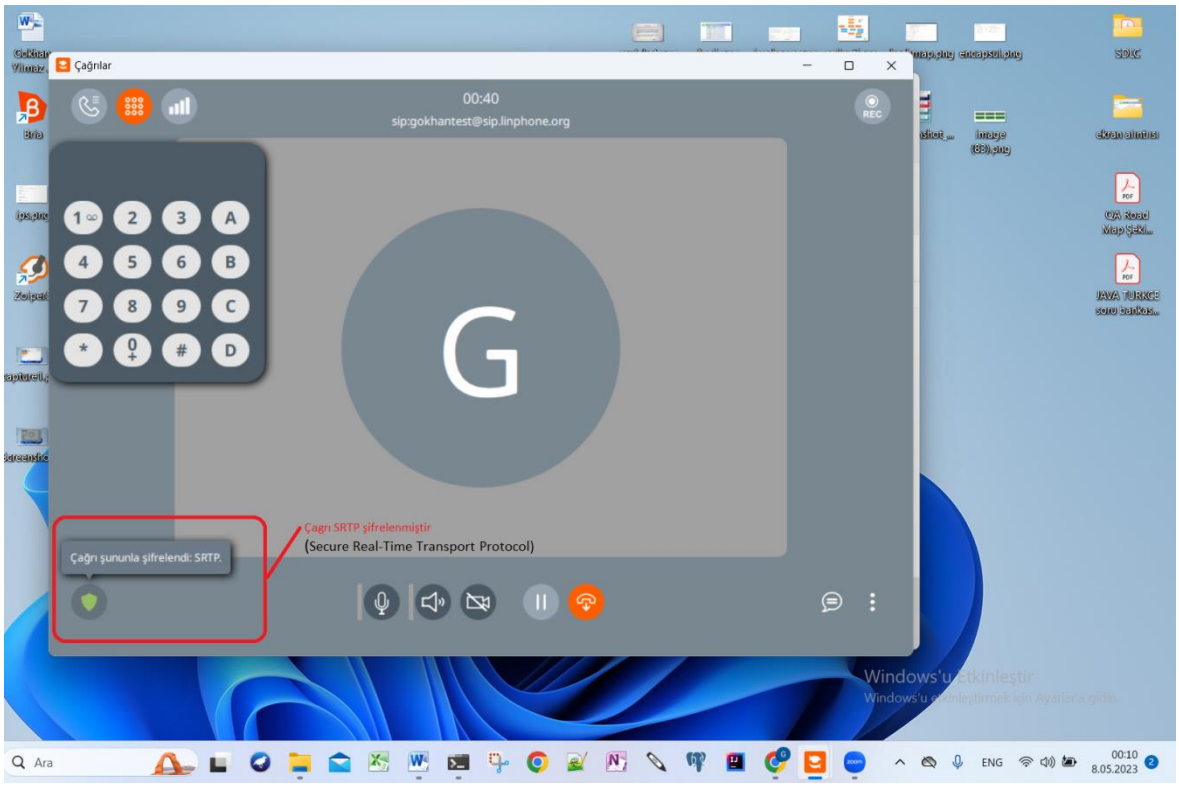
RTP mesajının şifrelenmesinde, AES- CM kullanılır. Şifreleme akışı aşağıdaki şekilde görüldüğü gibidir. Şifreleme dönüşümü, SRTP paket indexini ve 128 bitlik anahtarı pseudo- random bir bit dizisinde birleştirir. Her bit dizisi bir RTP paketini şifrelemede kullanılır. Bir RTP paketinin şifrelenmesi iki kısımdan oluşur:

- Pakete karşılık gelen anahtar stream'inin oluşturulması
- Anahtar steami ile RTP payload'unun, şifrelenmiş SRTP metnini oluşturmak üzere bit bit exorlanması

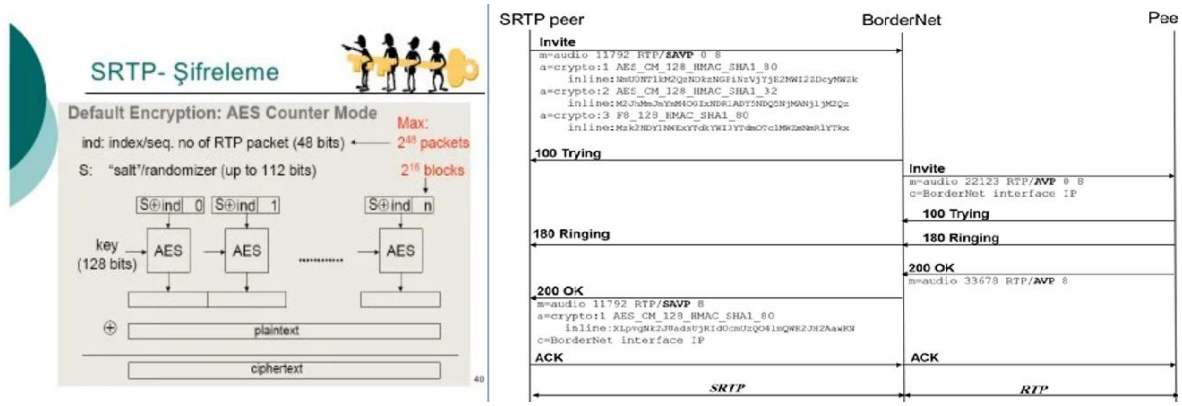
SRTP Protokolu Kullanılarak 2 ayrı softphone uygulaması arasında yapmış olduğum aramanın uçtan uca şifrelenmiş çağrı sonuçları aşağıdaki şekilde bulunmaktadır.(Şekil 2, Şekil 2.1)



Şekil 2



Şekil 2.1

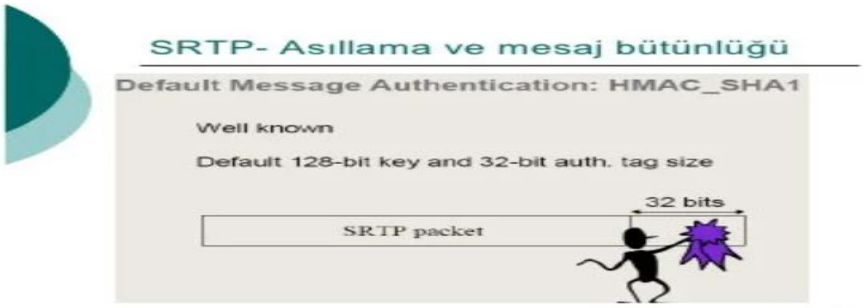


Şekil15: SRTP şifreleme

SRTP Asıllama

Asıllama etiketinin hesaplanması şu şekilde tanımlanabilir; gönderici asıllama etiketini hesaplar ve mesajın sonuna ekler. Alıcı, seçilen algoritmayı ve oturum asıllama anahtarını kullanarak yeni bir asıllama etiketi hesaplar ve mesaj/etiket ikilisini, göndericiden aldıkları ile karşılaştırır. İkisi aynı ise mesaj geçerlidir, aksi halde asıllama başarısız olur.

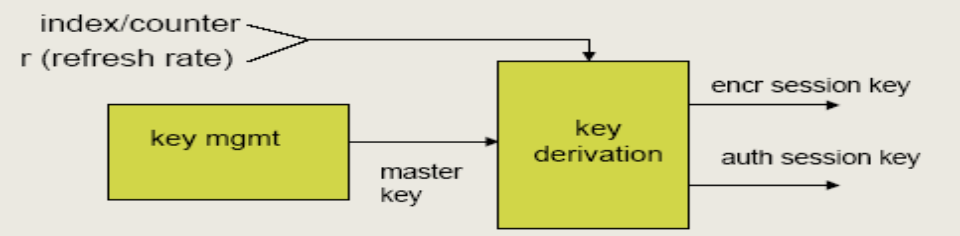
SRTP mesajının asıllanmasında HMAC-SHA1 kullanılır.



Şekil16: SRTP Asıllama

SRTP Anahtar Yönetimi

SRTP'de asıllama ve şifreleme için oturum anahtarları gereklidir. Başlangıçta bu anahtarlar master key'den elde edilir. Her r'inci Pakette anahtar elde etme algoritması, oturum anahtarını yeniler. Anahtar elde etme algoritması, AES-CM'a dayalıdır.



Şekil17: SRTP anahtar elde etme

Sonuç

VoIP, hala gelişmekte olan bir teknolojidir ve VoIP kullanımı hızla yaygınlaşmaktadır. VoIP güvenliği konusundaki çalışmalar çıkan güvenlik zafiyetleri karşısında sürekli gelişmektedir.

Günümüzde yapılan çalışmalarla, VoIP güvenlik açıkları teorik olarak belirlenmiş ve tanımlanmıştır. Saldırganlar için VoIP teknolojisinin popülerliği arttıkça, VoIP konusundaki bilgi eksikliği azaldıkça, saldırganların bu konuya ilgisi de artmaktadır. İnternet üzerinden ses (VOIP) tabanlı iletişim ağlarında sinyalleşme için kullanılan Oturum Başlatma Protokolü (SIP) en çok tercih edilen protokollerden birisidir. Bunların yanında VoIP için hem sinyalleşme hem de media paketlerinin güvenliğini sağlamaya yönelik yapılan çalışmalar vardır. RTP paketlerinin güvenliği için geliştirilen SRTP protokolü, bu konuda standard halini almış güçlü bir protokoldür. Diğer sinyalleşme protokollerine göre konfigürasyonu ve yönetimi daha kolay olan SIP protokolü, günümüzde birçok VOIP uygulamada kullanılmaktadır. Yaygın kullanımına karşılık, beraberinde zayıf noktalarının da bulunması, bu protokolü saldırılara açık hale getirmektedir. Tehditlere yönelik zafiyetleri çeşitli güvenlik önlemleri ile giderilmekle birlikte farklı saldırılar için farklı önlemlerin alınması gerekmektedir. Çok fazla tehdit unsuru bulunmasına karşın, oluşturulan test senaryosunda, savunmasız bir sisteme Hizmet Kesintisi (DoS) ve telekulak saldırıları gerçekleştirilmiş ve sonuçları gözlenmiştir. Bu saldırılara karşı Taşıma Katmanı Güvenliği (TLS) protokolü uygulanarak ve Saldırı Tespit Sistemi (IDS) ve Saldırı Önleme Sistemi (IPS) kullanılarak önlem alınmış, bu sayede ağın ya da kullanıcıların hiçbir şekilde saldırılardan etkilenmediği gözlemlenmiştir.

Kısaltmalar:

ACL: Access Control List

AES: Advanced Encryption Standard

CM: Counter Mode

AH: Authentication Header

CLID: Call Lineidentification

ESP: Encapsulating Security Payload EQ: Sekans Numarası

HMAC: Hashed Message Authentication Code IPSec: IP Security

MKI: Master Key Identifier ROC: Roll Over Count

RTP: Real-Time Transport Protocol SBC: Session Border Controller SDP: Session Description Protocol SIP: Session Initiation Protocol

SRTP: Secure Real-Time Transport Protocol TLS: Transport Layer Security

UAC: User Agent Client UAS: User Agent Server

UDP: User Datagram Protocol URI: Uniform Resource Identifier VLAN: Virtual Local Area Network

Kaynaklar

http://www.ietf.org/rfc.html

- RFC 3261-65 – SIP Protocol
- RFC 3550 – Real-time Transport Protocol
- RFC 3711 – Secure RTP
- RFC 2401 – IPSec
- RFC 2246 – TLS Protocol
-

https://www.3cx.com/voip/srtp/

- Security for Real-Time

https://www.linphone.org/

https://www.wireshark.org/download.html