# VoIP Güvenliği

Ağ Güvenliği
Prof Dr. Bülent Örencik

Sinem YAVAŞ
Bilgisayar Bilimleri
704051013

**İÇİNDEKİLER:**

1. Giriş....4
2. VoIP Protokolleri....4
   2.1. SIP (Session Initiation Protocol)....4
   2.2. RTP (Real-Time Transport Protocol)....6
3. VoIP Güvenlik Tehditleri....6
   3.1. Hizmeti Engelleme (DoS)....6
      3.1.1. SIP Bombing....7
      3.1.2. SIP CANCEL/ BYE DoS....7
      3.1.3. SIP 4xx, 5xx ve 6xx cevap kodlarını kullanarak DoS....8
   3.2. Ortadaki Adam Saldırısı ve Call Hijack....8
      3.2.1. Kayıt Bilgilerinin Değiştirilmesi....8
      3.2.2. 3xx Cevap Kodları Kullanımı (Call Redirect)....9
   3.3. Telekulak Saldırısı (Eavesdropping)....10
   3.4. Yanıltma (Spoofing)....11
4. Çözüm Önerileri....12
   4.1. Genel Önlemler....12
   4.2. IPSec (IP Security)....13
   4.3. TLS (Transport Layer Security)....13
   4.4. SRTP (Secure Real-Time Transport Protocol)....13
      4.4.1. SRTP Akış....15
      4.4.2. SRTP Şifreleme....15
      4.4.3. SRTP Asıllama....16
      4.4.4. SRTP Anahtar Yönetimi....16
5. Sonuç....16
6. Kaynaklar....17

**ŞEKİLLER:**

Şekil1: SIP mesajlaşması
Şekil2: RTP Başlığı
Şekil3: SIP Bombing DoS saldırısı
Şekil4: SIP CANCEL/BYE DoS saldırısı
Şekil5: Kayıt Bilgilerinin Değiştirilmesine dayalı ortadaki adam saldırısı
Şekil6: 3XX cevap kodlarını kullanarak çağrı yönlendirme saldırısı
Şekil7: Telekulak saldırısı
Şekil8: Yanıltma (spoofing) saldırısı
Şekil9- SRTP Başlığı
Şekil10- SRTP Akışı
Şekil11-SRTP- şifreleme
Şekil12- SRTP- Asıllama
Şekil13- SRTP- anahtar elde etme

**KISALTMALAR:**

ACL: Access Control List
AES: Advanced Encryption Standard
AES- CM: Advanced Encryption Standard- Counter Mode
AH : Authentication Header
CLID: call line identification
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

# 1.GİRİŞ

Haberleşme servislerinin varolan IP ağı altyapısı üzerinde birleştirilmesi motivasyonu uzun yıllar önce e-posta ile başlayıp hızlı mesaj servisi (instant message) ile devam etmiş ve telefon gibi, varolan klasik servisterin de integrasyonu ile bir adım daha yol almıştır. Ilk IP telefon servisi 1995'te Vocaltec tarafından verilmiştir. Ilk PC'den telefona arama 1998'de gerçekleşmiş ve onu telefondan telefona görüşme izlemiştir. Cisco, Nortel ve Lucent'ın ilk VoIP switchleri geliştirmesiyle hız kazanmış ve VoIP trafiği, 2000 yılında toplam ses trafiğinin 3%'ünü geçmiştir. Bu oranın 2008'de %44'e ulaşması bekleniyor.
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 populerliğinde etkili olan faktörlerin başında düşük maliyet ve telefon servislerine yeni servislerin (video, konferans..) ve uygulamaların eklenme kolaylığı gelmektedir.

Standard telefon sisteminde oldugu gibi, VoIP teknolojisinde iki tür protokol kullanılır; sinyalleşme protokolleri ve media iletim protokolleri. Sinyalleşme için SIP ve H323 protokolleri, media iletimi için ise RTP protokolü kullanılır.

# 2. VoIP Protokolleri

## 2.1. SIP (Session Initiation Protocol)

SIP, IETF tarafından RFC 3261,3262, 3263, 3264 ve 3265'te tanımlanmış bir protokoldür. SIP, uygulama katmanında çalışan HTTP benzeri, metin içerikli bir protokoldür. Sunucu-istemci mantığı ile çalışır. Çokluortam ya da ses oturumlarının başlatılması, değiştirilmesi ve sonlandırılması için kullanılır.
SIP bileşenleri, User Agent ve SIP proxy'den oluşur. User Agent, kullanıcıyı temsil eden uç birimdir. İki şekilde çalışabilir; SIP isteğinde bulunan birim UAC (User Agent Client) ve SIP isteklerini dinleyip cevaplayan birim UAS (User Agent Server) . SIP proxy de farklı bileşenlerden oluşur. Bu bileşenler aşağıdaki gibidir:

- **Registration / Location Server :** SIP kullanıcılarından kayıt olma isteklerini alıp asıllamayı yapar ve kullanıcıların o anki yer bilgisini günceller
- **Proxy Server :** SIP isteklerini alıp bir ilgili sunucuya iletir.
- **Redirect Server :** UAC'dan gelen bilgileri yorumlar
  Bir SIP istegi alındığında bu istek için next-hop'u belirler ve kullanıcıya bildirir.

SIP sinyalleşmesi sırasında kullanılan SIP mesajları aşağıdaki gibidir:

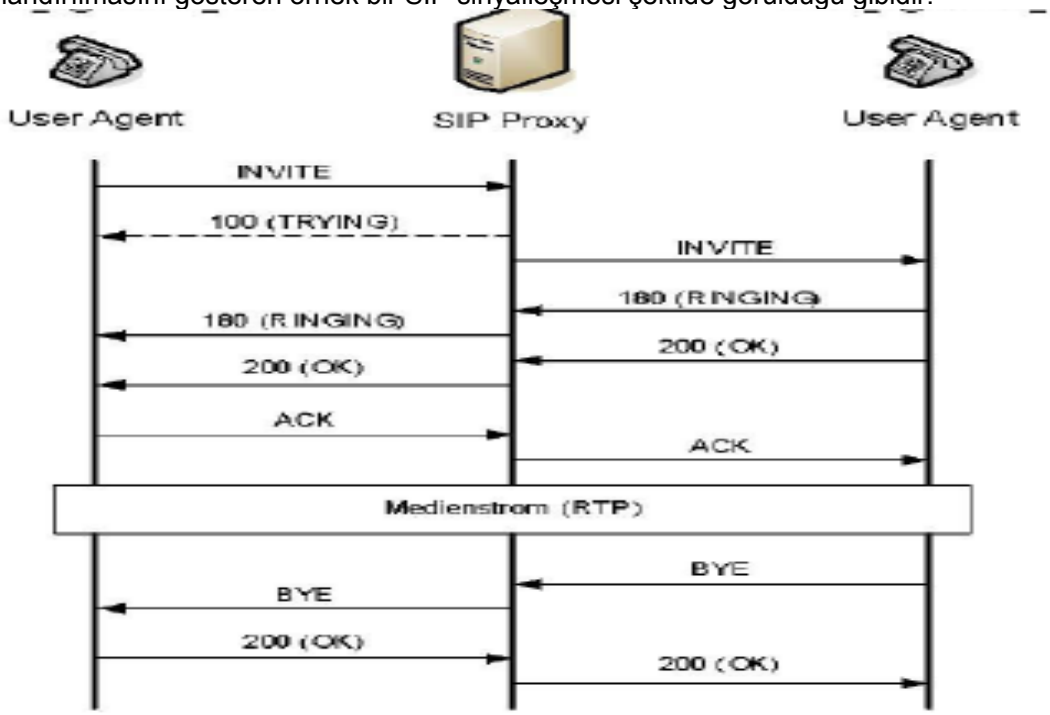
INVITE: oturumu başlat
ACK: son gelen cevabı onayla
BYE: oturumu sonlandır
CANCEL : iptal et
OPTIONS: desteklenen özellikler
REGISTER: kayıt olma
INFO: oturum sırasındaki bilgilendirmeler
SUBSCRIBE: bir olaya abone olmak (örn: presence, adres defteri..)
NOTIFY: aboneleri bilgilendirme
REFER: taraflara SIP isteğini işlemesi isteğinde bulunma (örn: transfer)

SIP mesajlaşmasında kullanılan cevap kodları, aşağıdaki gibi gruplara ayrılmıştır:

- 1xx – Geçici cevaplar
- 2xx – Başarılı

- 3xx – Yönlendirme
- 4xx – istek başarısız (kullanıcı kaynaklı)
- 5xx – Sunucu kaynaklı hata
- 6xx – Genel hata

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




**Şekil1: SIP mesajlaşması**

Öncelikle VoIP sistemindeki iki kullanıcının arama yapabilmesi için REGISTER mesajını kullanarak SIP sunucusuna kayıt olmaları gerekir. Daha sonra yukarıdaki gibi oturum kurulabilir. Örneğin A kullanıcısı B kullanıcısını arayacağı zaman, A kullanıcısı, kayıtlı olduğu sunucuya INVITE mesajı gonderir. Bu INVITE mesajının içeriğinde aramak istediği kullanıcının bilgisi, kendi bilgileri (kullanıcı adı, oturum için gerekli IP adresi ve port bilgisi, oturumda kullanmaı tercih ettiği codec bilgisi, ne tür bir istekte bulunduğu – ses, video gibi ..) bulunur. INVITE mesajını alan sunucu, bu mesajı kendisine kayıtlı olan B kullanıcısına gönderir ve böylece A'nın görüşme isteğini B'ye iletir. (Eğer B kullanıcısı aynı sunucuya kayıtlı bir kullanıcı değilse, sunucu bu isteği, B'nin kayıtlı olduğu sunucuya yönlendirir ve mesaj bu şekilde B'ye ulaştırılır). B terminalinin çalması sırasında A'ya 180 Ringing mesajı gönderilir. B, isteği kabul ettiğini belirten 200 OK mesajını A'ya gönderilmek üzere kayıtlı oldugu proxy'ye gönderir. Bu mesajın içinde kendisine ait oturum için gerekli bilgileri gönderir (IP ve port bilgisi, tercih ettiği codec bilgisi,..). A kullanıcısı 200 OK mesajını aldığını belirten ACK mesajını BB'ye gönderilmek üzere sunucuya iletir ve böylece üç yollu el sıkışma tamamlanmış olur. BU aşamadan sonra iki kullanıcı birbirlerinin IP adresi ve port bilgilerini öğrenmişler ve hangi koşullarda hangi seçeneklerle haberleşecekleri konusunda anlaşmışlardır. Böylece iki kullanıcı arasında gerçek-zamanlı veri ileti (ses, video..) başlar. Gerçek zamanlı verinin iletimi kullanıcılar arasında gerçekleşir, bu aşamada SIP sunucu devreye girmez. Taraflardan biri oturumu sonlandırmak istediğinde yine sunucular aracılığı ile karşı tarafa BYE mesajı gönderir. Bu mesajı alan kullanıcı mesajı aldığını, kabul ettiğini belirten 200 OK mesajını gönderir ve böylece oturum sonlandırılır.

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

## 2.2. RTP (Real-Time Transport Protocol)

RTP protokolü RFC 3550 ile tanımlanmaktadır. Ilk olarak RFC 1889 ile tanımlanmış, daha sonra değişikliklerle RFC3550'de son halini almıştır. RTP protokolü, gerçek zamanlı veri iletimi için kullanılır. RTP, ses ve video iletimi için standartlaşmış bir protokoldür. Ulaşım katmanında UDP protokolünü kullanır. Kodlayıcı olarak G729 ve G711'i destekler. RTP, sırasız gelen paketleri sıralar. Zaman damgası sayesinde senkronizasyonu sağlar. Örnek bir RTP başlığı aşağıdaki gibidir:

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|V=2|P|X|  CC   |M|     PT      |       sequence number         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                           timestamp                           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|           synchronization source (SSRC) identifier            |
+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
|            contributing source (CSRC) identifiers             |
|                             ....                              |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

**Şekil2: RTP Başlığı**

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

# 3. VoIP Güvenlik Tehditleri

IP için varolan güvenlik tehditleri, VoIP için de geçerlidir. Bunun dışında yalnızca VoIP'e özel tehditler de vardır. VoIP güvenlik tehditlerini aşağıdaki gibi gruplayabiliriz:

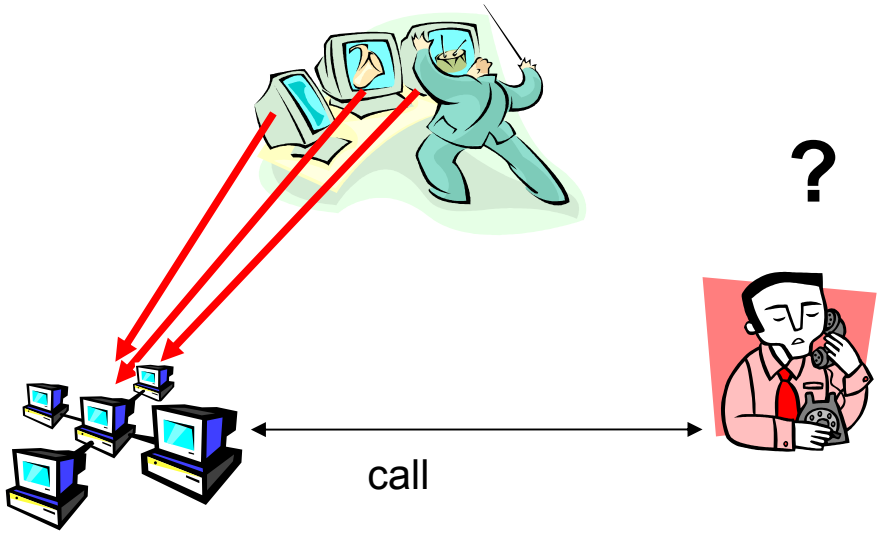
- Hizmeti engelleme (DoS- Denial of Service)
- Ortadaki adam saldırısı (Man-in-the-middle attack)
- Call Hijack
- Çağrı yönlendirme (Call redirect)
- Telekulak (Eavesdropping)
- Yanıltma (Spoofing)
- Tekrarlama saldırısı (replay)

## 3.1. Hizmeti Engelleme (DoS)

DoS saldırısı, hizmeti engellemeye yönelik bir saldırıdır. DoS; bandgenişliği, disk alanı, işlemci zamanı gibi kaynakları tüketmek; konfigurasyon bilgilerini bozmak; sistemin cevap veremeyeceği kadar çok sayıda istekte bulunmak ya da fiziksel network bileşenlerini bozmak gibi farklı şekillerde gerçekleştirilebilir. VoIP'e özel DoS saldırıları; VoIP sistemine çok sayıda yalancı SIP mesajının gönderilerek sistemin çalışamaz hale getirilmesi; SIP oturumunun başlamasından sonra kullanıcıya CANCEL ya da BYE mesajı göndererek oturumunu

sonlandırmak ya da 4xx, 5xx, 6xx cevap kodlarını kullanarak varolan SIP oturumlarını sonlandırmak şeklinde gerçekleştirilebilir.

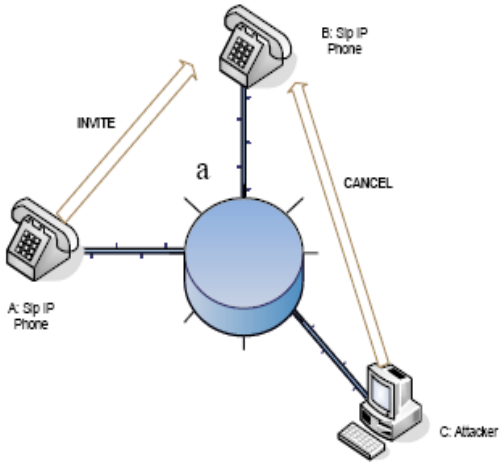
### 3.1.1. SIP Bombing




**Şekil3: SIP Bombing DoS saldırısı**

Yukarıdaki şekilde SIP bombing örneği görülmektedir. Saldırıda bulunan, SIP sistemine aynı anda çok sayıda yalancı SIP mesajı ile istekte bulunmaktadır. Gelen isteklerin sayısı, sistemin cevap verebileceğinden fazladır. Sistem kaynakları, bu istekleri proses etmekle meşgul olmaktadır. Aynı anda, sisteme kayıtlı olan kullanıcılar servis isteğinde bulunduğunda, sistem bu isteklere cevap veremez. Böylece DoS saldırısı amacına ulaşmış, sistem kullanıcılarına hizmet veremez hale gelmiştir.

### 3.1.2. SIP CANCEL/ BYE DoS:




**Şekil4: SIP CANCEL/BYE DoS saldırısı**

Şekilde A kullanıcısı, VoIP sistemi üzerinden B kullanıcısını aramaktadır. A kullanıcısı, çağrıyı baişlatmak içim, B kullanıcısına bir INVITE mesajı gönderir.Saldırıda bulunmak isteyen C o anda ağı dinlemektedir. C, A kullanıcısından B kullanıcısına bir INVITE mesajı

gittiğini farkettiği anda B kullanıcısına bir CANCEL mesajı gönderir. Böylece A kullanıcısından B kullanıcısına kurulmakta olan oturum sonlandırılmış olur. Burada saldırının başarılı olması için gerekli bazı koşullar vardır. Saldırganın göndermiş olduğu CANCEL mesajının callID'si ve mesaj sekans numarası, A kullanıcısının göndermiş olduğu INVITE mesajı ile uyumlu olmalı ve aynı zamanda saldırıda bulunan, B kullanıcısı, INVITE isteğine cevap vermeden, yani iki kullanıcı arasındaki oturum kurulmadan önce CANCEL mesajını göndermeli.
Bu tür saldırının diğer bir şekli BYE mesajını kullanarak gerçekleştirilebilir. Aynı şekilde A kullanıcısı B kullanıcısını arar. Mesajlaşma tamamlanıp iki kullanıcı arasında oturum kurulur. Oturum kurulduktan sonra, kullanıcılar konuşmaya devam ederken herhangi bir anda, saldırıda bulunmak isteyen biri, kullanıcılardan birine BYE mesajı göndererek oturumu sonlandırabilir.Saldırıda bulunan, CANCEL mesajını kullanarak gerçekleştirilen saldırıdaki kriterlere dikkat etmelidir; yalnızca zamanlama konusunda diğer saldırıda olduğu gibi hız çok önemli değildir; oturumun başlamasından sonlanmasına kadarki herhangi bir zamanda gerçekleştirilebilir.

### 3.1.3. SIP 4xx, 5xx ve 6xx cevap kodlarını kullanarak DoS

Bu saldırı tipinde, saldırıda bulunan, 4xx, 5xx ve 6xx cevap kodlarını kullanarak, varolan bir SIP oturumunu sonlandırabilir. Örneğin 487-request terminated, 480 temporarily unavailable, 503-service unavailable, 603-decline mesajları kullanılabilir. Sistemde varolan bir kullanıcı bir SIP isteğinde bulunduğunda, saldırıda bulunan, kullanıcıya, 603-decline mesajı göndererek, isteğinin reddedildiğini bildirebilir. Böylece isteğin gerçekleşmesini engeller. Sisteme kayıtlı bir kullanıcı servis isteğinde bulunduğunda, saldırıda bulunmak isteyen biri kullanıcıya 480 temporarily unavailable mesajı göndererek istenen servisin ya da aranan kişinin geçici olarak ulaşılamaz durumda olduğunu bildirebilir. Aynı şekilde diğer cevap kodları kullanılarak da kullanıcıların servis alması engellenebilir.

## 3.2. Ortadaki Adam Saldırısı ve Call Hijack

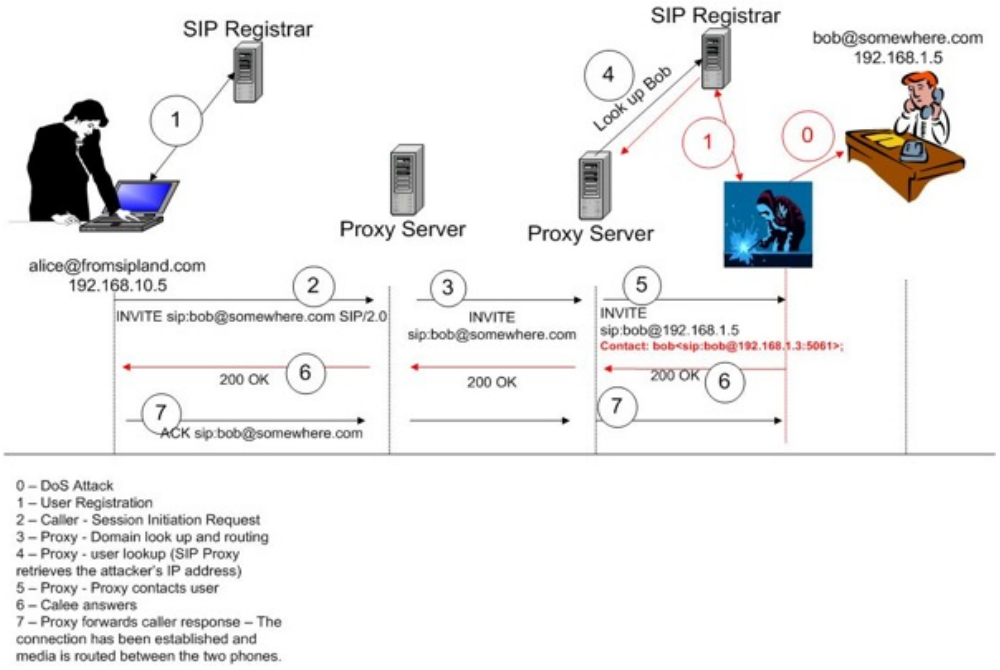
Ortadaki adam saldırısı (man-in-the-middle attack), araya girenin, tarafların haberi olmadan iki taraf arasındaki mesajları okuyabilmesi ve değiştirebilmesi olarak tanımlanabilir. Ortadaki adam saldırısı, DoS ya da telekulak gibi diğer saldırı türlerini gerçekleştirmek için de kullanılabilir.
Call Hijack, saldırıda bulunanın, taraflardan birinin yerine geçmesi durumudur. Call Hijack saldırısında bulunan biri, şüpheleri arttırmamak için bunu MITM saldırısına dönüştürebilir.

Bu saldırılar, farklı şekillerde gerçekleştirilebilir:

1. Kayıt bilgilerini değiştirmek (registration manipulation)
2. 3xx cevap kodlarını kullanarak (call redirect)

### 3.2.1. Kayıt Bilgilerinin Değiştirilmesi:

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 değildir ve 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. Kayıt bilgilerinin değiştirilmesi ile yapılan saldırıya bir örnek aşağıdaki şekilde görülmektedir:



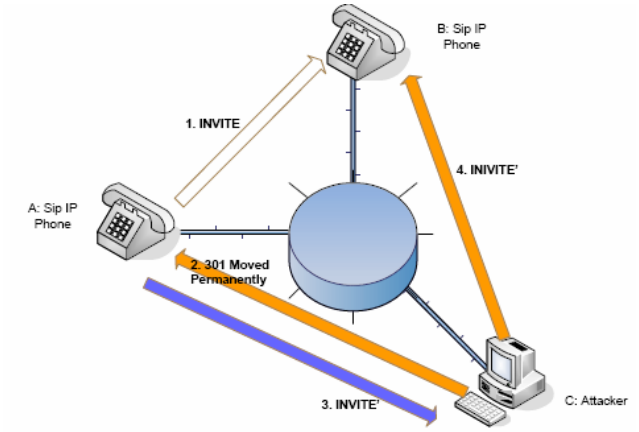

**Şekil5: Kayıt Bilgilerinin Değiştirilmesine dayalı ortadaki adam saldırısı**

Şekilde, saldırgan, öncelikle Bob kullanıcısına DoS saldırısında bulunarak bu kullanıcının terminalini iş göremez hale getirir. Daha sonra SIP Registrar sunucuya Bob kullanıcısının kullanıcı adını kullanarak kayıt olma isteğinde bulunur ve böylece kayıt bilgilerini, Bob kullanıcısı saldırganın IP'sinden kayıt olacak şekilde değiştirir.Bu aşamadan sonra, Bob'un kayıtlı olduğu SIP proxy'ye gelen tüm istekler, saldırganın IP'sine yönlendirilecektir. Örneğin şekilde görüldüğü gibi, 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.

### 3.2.2. 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 tipi aşağıdaki şekilde de görülmektedir:




**Şekil6: 3XX cevap kodlarını kullanarak çağrı yönlendirme saldırısı**

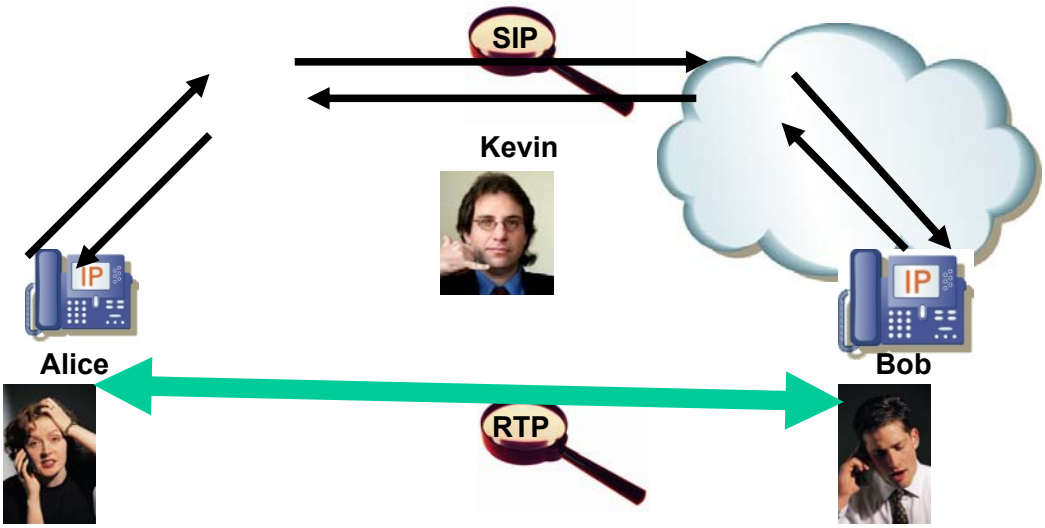
Bu saldırı, SIP 302 cevap kodunun kullanılması ile gerçekleştirilebilir. Saldırgan yine SIP isteği üzerine 302- moved temporarily mesajı gönderir ve kullanıcının geçici olarak kendi Ipsine yönlendirilmiş olduğunu bildirir. Böylece geçici bir süre için kullanıcının SIP isteğini gerçekleştirmek için kendisi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

## 3.3. Telekulak Saldırısı (Eavesdropping):

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. Çok sayıda ağ protokol analiz etme araçlarının ve ağı dinleme araçlarının internette kolayca erişileblir olduğu düşünülürse, telekulak saldırısını gerçekleştirmek son derece kolaydır. Ağa erişim gerekiyor olsa da, bu ağda bulunan cihazlara ya da kablolara direk erişimi gerektirmemektedir; örneğin paylaşılan ortam oluşturan hub gibi cihazların kullanımı, saldırıyı kolaylaştırmaktadır. Burada erişim denetim listelerinin (access control list) ve fiziksel güvenlik önlemlerinin önemi gözden kaçırılmamalıdır. Anahtar (switch) kullanılan ağlarda, saldırganın switch konfigurasyonunu kontrol etme yetisi ve fiziksel erişimi olmadığı düşünülürse; ağı dinleme yetkisi, subnet içinde sınırlanmış olur.
Bazı protokol analiz edici programlar, yalnızca VoIP trafiğini dinlemek ve daha sonraki analizler için saklamak üzere konfigüre edilebilir.
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 getirmiştir.

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. Internette 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 saldırılarısı gibi birçok saldırı amacıyla kullanabilir.

Telekulak saldırısı örneği, aşağıdaki şekilde de görülebilir:




**Şekil7: Telekulak saldırısı**

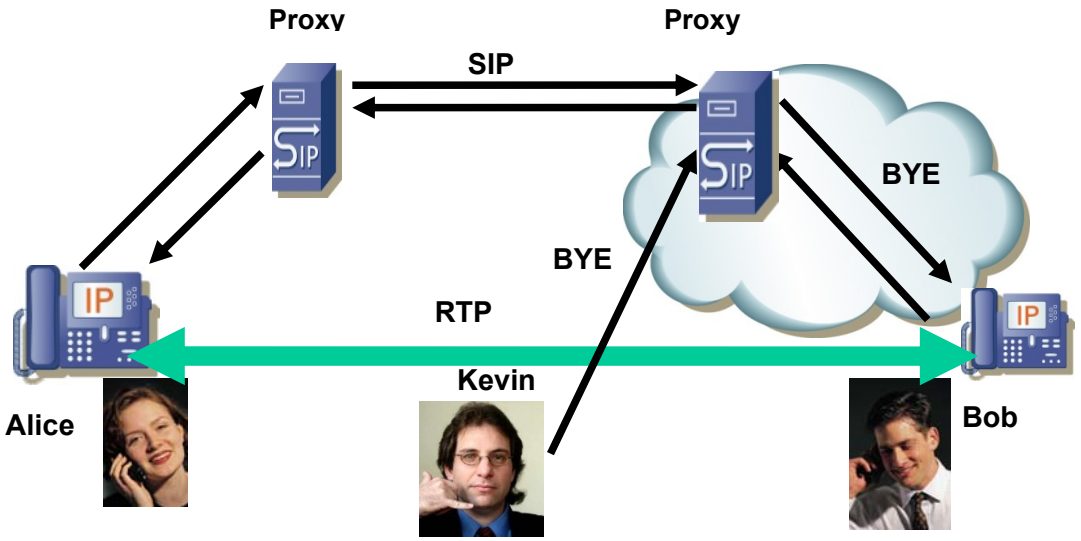
## 3.4. Yanıltma (Spoofing):

Spoofing, IP paketlerinin, yanlış kaynak adresi kullanılarak gönderilmesidir. Saldırıda bulunan kişinin IP adresini gizlemesi; başka bir taraf ya da kişiyi saldırıyı yapan olarak göstermesi; güvenilir bir kullanıcı gibi görünmesi yanında network trafiğini dinleme ya da ele geçirme ve ortadaki adam saldırısı gibi saldırıları gerçekleştirmek için kullanılabilir.

Bu tür yanıltma saldırısındaki bir risk, kimlik hırsızlığıdır.Örneğin bir müşteri, sipariş vermek üzere biryeri arayıp telefonda kredi kartı numarası gibi önemli bilgilerini verebilir. Ne yazık ki müşteri, satış departmanı yerine, onun yerine geçmiş olan saldırganla konuşmaktadır. Bu, klasik bir 'man-in-the-middle spoofing' saldırısıdır.

Bir başka yanıltma türü de arayan ID'si (Caller ID) ya da CLID (call line identification) değiştirilerek yapılabilir. Yalancı bir kullanıcının ya da varolan bir kullanıcının telefon numarası değiştirilebilir. Bu da; arayan numaraya göre asıllama yapan sistemlere zarar vermek için kullanılabilir.
Bazı VoIP cihazları periyodik olarak belli bir sunucudan firmware yuklemek uzere konfigüre edilmiş olabilir. Spoofing ile cihaza yanlış bir firmware dosyası yüklenmesi sağlanabilir

Örnek bir spoofing saldırısı, aşağıdaki şekilde görülmektedir. Alice ve Bob kullanıcıları, VoIP sistemi üzerinden konuşurken, araya giren saldırgan (Kevin), Bob'a Alice adına bir BYE mesajı göndererek, iki kullanıcı arasındaki oturumun sonlandırılmasına sebep olur. Bob, BYE mesajının Alice'den geldiğini zannetmektedir. Alice ise, oturumun sonlanma sebebinden haberdar değildir.




**Şekil8: Yanıltma (spoofing) saldırısı**

# 4. ÇÖZÜM ÖNERİLERİ

## 4.1. 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. Örneğin 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.

- 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.

## 4.2. IPSec (IP Security)

IPSec, çağrı kurulması ve kontrolu 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.

## 4.3. 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 uzerinde 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.

## 4.4 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 verilecektir.

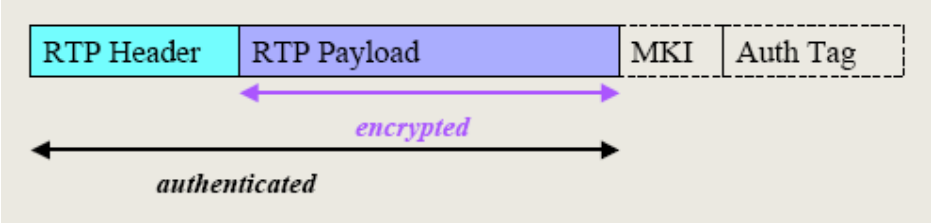
SRTP, RTP paketlerinin güvenliği için kullanılır. SRTP, Mart 2004'teIETF tarafından RFC 3711 ile yayınlanmıştır. Ses ve video gibi gerçek zamanlı verinin iletimi için kullanılan RTP protokolünün güvenliğini arttırmayı amaçlamaktadır. RTP paketlerine gizlilik, asıllama, tekrarlama saldırısına karşı koruma 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 öntanımlı 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 birlikte, RTP ve RTCP için mesaj bütünlüğünün sağlanması
- Oturum anahtarlarını periyodik olarak yenileme imkanı 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

Örnek bir SRTP başlığı şekil9'da görüldüğü gibidir:



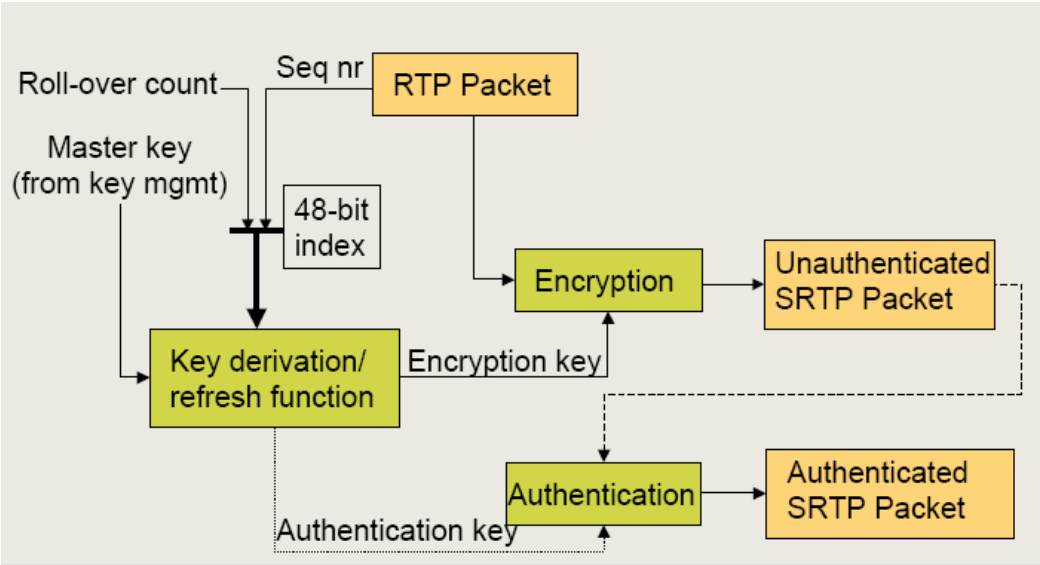

**Şekil9- SRTP Başlığı**

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)
  $i=2^{16} * ROC * SEQ$
- Tekrarlama listesi (replay list)
- Master anahtar
- Asıllama algoritması belirteci
- Şifreleme algoritması belirteci

### 4.4.1 SRTP Akışı:



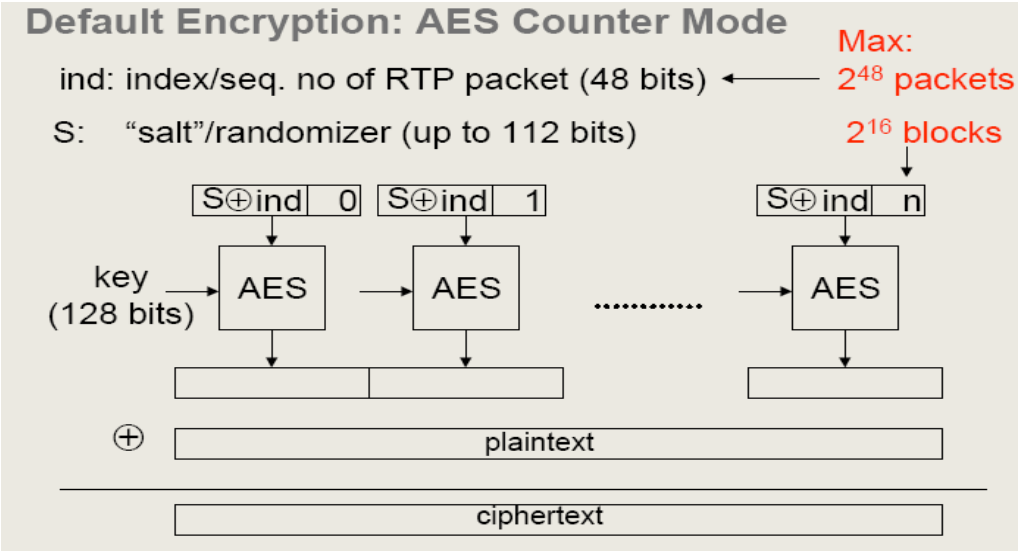

**Şekil10- SRTP Akışı**

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.

### 4.4.2. 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:

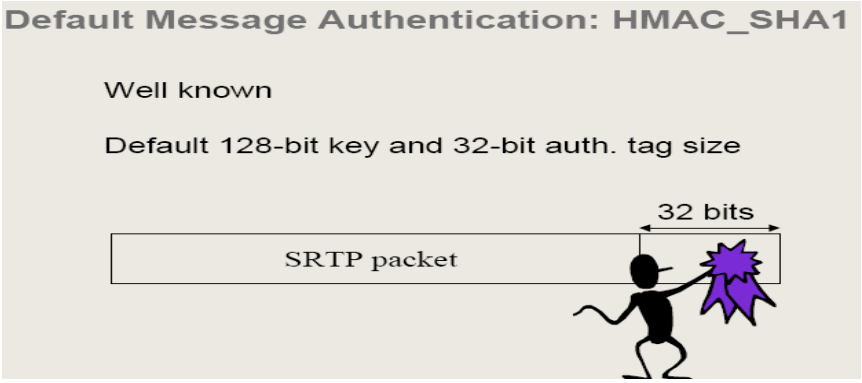
1. pakete karşılık gelen anahtar stream'inin oluşturulması ve
2. anahtar steami ile RTP payload'unun, şifrelenmiş SRTP metnini oluşturmak üzere bit bit exorlanması




**Şekil11-SRTP şifreleme**

### 4.4.3. SRTP Asıllama

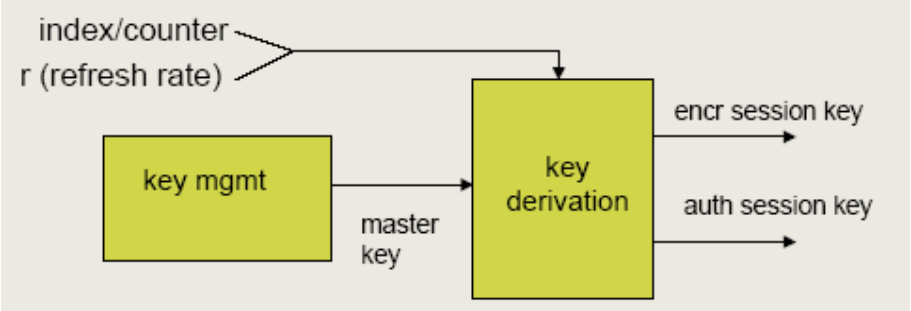
Asıllama etiketinin hesaplanması şu şekilde tanımlanabilir; gönderici asıllama etiketini hesaplar ve mesajın sonuna ekler. Alıcı, seçilen algoritmayı ve oturum asıllama anahtarını kullanarak yeni bir asıllama etiketi hesaplar ve mesaj/etiket ikilisini, göndericiden aldıkları ile karşılaştırır. İkisi aynı ise mesaj geçerlidir, aksi halde asıllama başarısız olur.
SRTP mesajının asıllanmasında HMAC-SHA1 kullanılır.




**Şekil12- SRTP Asıllama**

### 4.4.4. 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.




**Şekil13- SRTP anahtar elde etme**

## 5. SONUÇ

VoIP, hala gelişmekte olan bir teknolojidir ve VoIP kullanımı hızla yaygınlaşmaktadır. VoIP güvenliği konusundaki çalışmaların henüz başlangıç evresinde olduğunu söyleyebiliriz. Günümüzde yapılan çalışmalarla, VoIP güvenlik açıkları teorik olarak belirlenmiş ve tanımlanmıştır. Ancak bu açıkları pratiğe taşımak zordur. Bunun nedeni ise; saldırganlar için VoIP konusundaki bilgi eksikliği ve VoIP test ortamı kısıtıdır. VoIP teknolojisinin popülerliği arttıkça, saldırganların bu konuya ilgisi de artacaktır. Bu da saldırı türlerini ve dolayısıyla güvenlik tehditlerini arttıracaktır. VoIP güvenliği konusunda yapılan birçok çalışma vardır. Ilk olarak önerilen VoIP için geliştirilmemiş ancak IP güvenliği için kullanılmakta olan çözümlerdir. Bunların yanında VoIP için hem sinyalleşme hem de media paketlerinin güvenliğini sağlamaya yönelik yapılan çalışmalar vardır. SIP standardında güvenliği arttırmaya yönelik henüz standard haline gelmiş bir çalışma yoktur. RTP paketlerinin güvenliği için geliştirilen SRTP protokolü, bu konuda standard halini almış güçlü bir protokoldür.

## 6. 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**
- **http://www.hackingvoip.com/**
- **Security Considerations for Voice Over IP Systems- . Richard Kuhn, Thomas J. Walsh, Steffen Fries –. National Institute of Standards and Technology, January 2005**
- **www.just-us.org**
- **http://www.ccip.govt.nz/ccip-publications/ccip-reports/ccip-reports.htm**
- **Security for Real-time Multimedia in Heterogeneous Environments- J. Arkko, R. Blom, E. Carrara, F. Lindholm, and K. Norrman**