T.C.
MARMARA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

VoIP TEKNOLOJİLERİNDE GÜVENLİK

Ceyhun ÇAKIR

YÜKSEK LİSANS TEZİ
ELEKTRONİK VE BİLGİSAYAR EĞİTİMİ ANABİLİM DALI
ELEKTRONİK VE HABERLEŞME EĞİTİMİ PROGRAMI

DANIŞMAN
Yrd. Doç. Dr. Hakan KAPTAN

İSTANBUL 2009

T.C.
MARMARA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

VoIP TEKNOLOJİLERİNDE GÜVENLİK

Ceyhun ÇAKIR
(141101020060248)

YÜKSEK LİSANS TEZİ

ELEKTRONİK VE BİLGİSAYAR EĞİTİMİ ANABİLİM DALI
ELEKTRONİK VE HABERLEŞME EĞİTİMİ PROGRAMI

DANIŞMAN
Yrd. Doç. Dr. Hakan KAPTAN

İSTANBUL 2009

TEŞEKKÜR

Tez çalışmam boyunca desteğini ve bilgilerini esirgemeyen tez danışmanım, Yrd. Doç. Dr. Hakan KAPTAN'a, ihtiyaç duyduğum her an yanımda olan arkadaşlarıma ve hayatım boyunca desteğinin her an yanımda hissettiğim aileme teşekkür ederim.

Şubat 2009 **Ceyhun ÇAKIR**

İÇİNDEKİLER

SAYFA

ÖZET

VoIP TEKNOLOJİLERİNDE GÜVENLİK

VoIP, internet üzerinden veri paketlerinin taşınmasını sağlayan bir teknolojidir. Bu teknoloji, çok hızlı bir gelişim göstermiş ve kullanım oranları ciddi boyutlara ulaşmıştır. VoIP teknolojisinin getirdiği, düşük maliyet, kolay geliştirilebilen esnek bir yapı, kurulum ve kullanım kolaylığı gibi etkenler, bu teknolojinin yaygınlaşmasını sağlamıştır. VoIP, var olan internet altyapısını kullanması, kullanıcılar için her an her yerde erişilebilir olması anlamına gelmektedir. Ancak bu durum, internet üzerinden gelebilecek tehditlere açık olması sonucunu doğurmaktadır.

VoIP teknolojisindeki en büyük sorunlardan biri, güvenlik tehditleridir. Güvenlik açıkları kullanılarak, VoIP sistemlerine saldırılar düzenlenebilir. Bu saldırılar sonucunda VoIP trafiği saldırganlar tarafından kesilebilir, kopyalanabilir, engellenebilir, yavaşlatılabilir veya değiştirilebilir. Bir VoIP sistemindeki güvenlik açıkları, kullanılan cihazlardan, yazılımlardan ve protokollerden kaynaklanabilir. VoIP teknolojisi kullanarak, güvenli iletişimin sağlanabilmesi için, bu parametreler doğru belirlenmeli ve sistem tasarımları bu ölçülere göre yapılmalıdır.

Bu tez çalışmasında, VoIP mimarisi incelenmiş, bu teknolojide kullanılan protokoller ve çalışma şekillerine değinilmiştir. Daha sonra, VoIP teknolojisine karşı ne tür tehditler olduğu belirtilmiştir. Ardından, güvenlik tehditlerine karşı geliştirilen önlemler ve teknolojiler aktarılmıştır. VoIP güvenliği alanında yapılan çalışmalar araştırılarak, yapılan uygulamalar ve geliştirilen teknolojiler incelenmiştir. Bu tez çalışmasında, laboratuar ortamında gerçek bir VoIP sistemine saldırılar düzenlenmiş ve sistemin farklı güvenlik seviyelerindeki tepkisi değerlendirilmiştir. Son olarak, opnet programı kullanılarak, güvenlik simülasyonları gerçekleştirilmiş, güvenli VoIP teknolojisinde güvenli iletişim için gereken unsurlar ortaya konmuştur.

Şubat 2009 **Ceyhun ÇAKIR**

ABSTRACT

SECURITY on VoIP TECHNOLOGIES

VoIP is a technology that enables the transport of data packets on the Internet. This technology has shown a rapid development and utilization rate has reached important dimensions. VoIP technology obtains low cost, easy and flexible structure that can be developed, such factors as ease of setup and use. So, VoIP became widespread. VoIP uses the existing Internet infrastructure. This means that everyone can use VoIP at everytimetime and everywhere. However, this may result in being exposed to the threats via internet.

One of the biggest problem in VoIP technology is the security threats. The attacks with the use of vulnerability on VoIP systems can be arranged. As a result of this attack, VoIP traffic can be interrupted, can be copied, can be prevented, can be slowed or changed by an attacker. Vulnerability in a VoIP system can arise from equipment, software and protocols. To ensure secure communications using VoIP technology, these parameters must be set correctly and the system design must be made according to these standards.

In this thesis, VoIP architecture were examined, and the protocols used in these technologies have been mentioned. Then, the kind of threats that are used on VoIP technology have been specified. Development of standards against security threats and technologies have been develeoped. Examines the practices and technologies were developed in the area of VoIP security by researching the Works. In this thesis, attacks were made on a real VoIP system in a laboratory environment and the response of the system in different security levels was evaluated. Finally, by using opnet program, security simulations were performed, secure VoIP technology components required for secure communication have been identified.

Şubat 2009 **Ceyhun ÇAKIR**

KISALTMALAR

3DES :Triple-DES
AES :Advanced Encryption System
AH :Authentication Header
ARP :Address Resolution Protocol
BES :Back End Server
DES :Data Encryption Standard
DNS :Domain Name System
DoS :Denial of Service
ESP :Encapsulating Security Payload
HTML :Hyper Text Markup Language
HTTP :Hypertext Transfer Protocol
IDEA :International Data Encryption Algorithm
IETF :Internet Engineering Task Force
IP :Internet Protocol
IPSEC :Internet Protocol Security
ISDN :Integrated Services Digital Network
ITU :International Telecommunication Union
L2TP :Layer 2 Tunnelling Protocol
LAN :Local Area Network
MAC :Media Access Control
MCU :Multipoint Control Unit
MIKEY :Multimedia Internet Keying
MKI :Master Key Identifier
P2P :Peer to Peer
PKI :Public Key Infrastructure
PPTP :Point to Point Tunnelling Protocol
PSTN :Public Switched Telephone Network
QoS :Quality of Servise
RAS :Registration, Admission and Status
RSA :Rivest Shamir Adleman

RTCP :Real Time Control Protocol

RTP :Real Time Protocol

SDP :Session Description Protocol

SIP :Session Initiation Protokol

SIPIT :Session Initiation Protocol Interoperability Testing

SPIT :Spam Through Internet Telephony

SRTP :Secure Real Time Protokol

SSL :Secure Socket Layer

TCP :Transmission Control Protocol

TEK :Traffic Encryption Key

TGK :TEK Generation Key

TLS :Transport Layer Security

UAC :User agent client

UAS :User agent server

UDP :User Datagram Protocol

VLAN :Virtual Local Area Network

VoIP :Voice Over Internet Protocol

VPN :Virtual Private Network

WAN :Wide Area Network

ŞEKİLLER

SAYFA NO

BÖLÜM I

GİRİŞ ve AMAÇ

I .1 GİRİŞ

Voice over IP (VoIP) bir ses iletim tekniğidir. Bu teknoloji sayesinde ses, veri paketleri halinde IP üzerinden gönderilebilmektedir. IP üzerinden sesi iletmek, internete ulaşılabilen her yerde, birkaç cihaz ve hatta yalnız yazılımlar ile sesli görüşme yapabilmek anlamına gelmektedir. Bu kullanıcıya daha ucuz, erişilebilir, kullanışlı bir sistem sağlamaktadır. Haberleşme teknolojisindeki bu gelişmeler yalnız bireysel kullanıcıların değil, kurumsal abonelerin de VoIP teknolojisine geçişini sağlamaktadır.

VoIP bu yönleriyle diğer sesli görüşme sistemlerine karşı avantaj sağlamaktadır. Ancak iletim IP üzerinden, yani internetten sağlandığı için internette oluşan sorunlardan etkilenmektedir. VoIP bazı güvenlik problemleri taşımaktadır. VoIP trafiği, diğer veri akışlarında olduğu gibi bir yönlendiriciden (router) diğerine giden trafik olarak değerlendirilebilir. Yönlendiricilere yapılacak müdahaleler, sistemin dışarıdan müdahaleye açık olduğu anlamına gelmektedir.

Sistemi tehdit eden unsurlar; kullanılan protokoller, VoIP cihazları, yazılımlar gibi farklı parametrelerden oluşur. Bununla birlikte sisteme farklı saldırı yöntemleri mevcuttur. Bunların sonucunda VoIP trafiği kötü niyetli kişiler tarafından kesilebilir, kopyalanabilir, engellenebilir, yavaşlatılabilir veya değiştirilebilir. Bu sorunlar karşısında geliştirilen sistemler, VoIP görüşmelerini daha güvenilir hale getirmeyi hedeflemektedir.

I .2 AMAÇ

İletişim altyapısında yer alan VoIP cihazları, noktalar arası ses iletiminde kullanılmaktadır. Kullanıcının iletişimde kalabilmesi için bir ağa bağlanması, internete erişebilmesi gerekir. Bununla birlikte bir arayüz kullanmalı, bazı durumlarda şifreleme işlemleri yapılmalı, duruma uygun protokol seçilmelidir. Tüm bu değişkenlerdeki hatalar sistemin güvenliğini tehdit eden unsurlardır.

İnternet güvenliği kesin olarak sağlanamamış bir konu olarak önümüzde durmaktadır. Bir VoIP sisteminde yukarıda sayılan parametreler de dahil olunca daha çok etkenin sağlıklı çalışması, VoIP güvenliği açısından son derece önemlidir. Kullanılacak protokolün zayıf noktalarından, şifreleme yapılmamasından veya kullanılan şifreleme siteminden kaynaklanan güvenlik açıkları, kullanılacak programdan kaynaklanan hatalar sistemi olumsuz yönde etkilemektedir.

VoIP teknolojisinde güvenlik açıkları temel sorunlardan biri olarak karşımıza çıkmaktadır. Bu tez ile ne tür saldırılar olduğu, bu saldırılara karşı ne tür önlemler alındığı, hangi protokollerin bu saldırılardan daha az etkilendiği ve daha güvenilir olduğu, ne tür şifreleme sistemlerinin kullanıldığı, hangi protokollerin geliştirildiği araştırılacaktır. Bu tezdeki amaç VoIP sisteminin nasıl daha güvenli hale getirileceğinin incelenmesidir.

BÖLÜM II

GENEL BİLGİLER

II.1 VOIP

VoIP teknolojisi sesin sayısal sinyallere dönüştürüldükten sonra, veri paketleri halinde IP protokolü kullanılarak gönderilmesidir. Bu teknolojide yalnız ses değil, aynı zamanda faks, video konferans gibi çoklu ortam uygulamaları da gerçek zamanlı olarak iletilmektedir. VoIP teknolojisinden önce, internet henüz yaygın değilken, etkileşimli (interaktif) iletişim sadece PSTN şebekesi üzerinden yapılabiliyordu. Veri iletimi özellikle uzun mesafeler için oldukça pahalıydı ve görüntülü iletişim mümkün değildi.

PSTN şebekelerinde kullanıcılara her çağrı için uçtan uca bir devre bağlantısı sağlamaktadır. Arayan ve aranan tarafların numarasına göre, arayan kullanıcının bağlı olduğu santralden başlayarak, aradaki santraller ve aranan kullanıcının santraline kadar bir devre kurulmaktadır. Bu santraller arasındaki sinyalleşme temel olarak çağrı kurma, çağrı yönlendirme ve çağrı sonlandırma işlemlerinden oluşmaktadır. Buna paralel olarak veri trafiği için ayrı şebekeler oluşmuştur. Doğal olarak ayrı ses ve veri şebekeleri servis sağlayıcılar için ilave yük, aboneler için de ilave ücret anlamına gelmektedir.

IP ağları üzerinden ses transferi 1995 yılında mümkün hale geldi. Uygulamalar yaygın olarak kullanılmamakla birlikte standartlaştırma çalışmaları 1995 yılında başladı. 1996'da ilk VoIP standartları kabul edildi. Aynı yıl düşük kapasiteli H.323 ağ geçitleri (gateway) geliştirildi. Ağ geçitleri birbirinden farklı PSTN ve IP ağları arasında iletişimi sağlamak için kullanılmaktadırlar. Devre anahtarlamalı PSTN ile paket anahtarlamalı IP ağları birleştirmek, konuşturmak ve birinden diğerine veri akışını sağlama işlemi ağ geçitleri tarafından gerçekleştirilir. Bu gelişmeler sonucunda, internet üzerinden telefondan telefona görüşme gerçekleştirildi.

VoIP teknolojisinden hem kurumsal şirketler, hem bireysel kullanıcılar yararlanabilmektedir. İnternette bulunan iki kullanılıcı bu teknolojiyi kullanarak telefon görüşmesi yapabilmektedir. Standart telefonlar bir gateway aracılığıyla IP

ağa bağlanabilmekte ya da PC üzerinde çalışabilen bir yazılımsal telefon (softphone) ile VoIP teknolojisi kolaylıkla kullanılabilmektedir. [1,2,3] Şekil II.1'de VoIP senaryoları görülmektedir.

Şekil II.1 VoIP Senaryoları [1]

VoIP teknolojisinin avantajları şu şekilde sıralanabilir:

• Ses ve veri hizmetlerinin bir arada verilebilmesi.

• Var olan internet altyapısı üzerine kurulabilmesi.

• İletişim yatırım maliyetlerinin çok büyük oranda düşmesi.

• Dünyanın her yerinden erişilebilir olması.

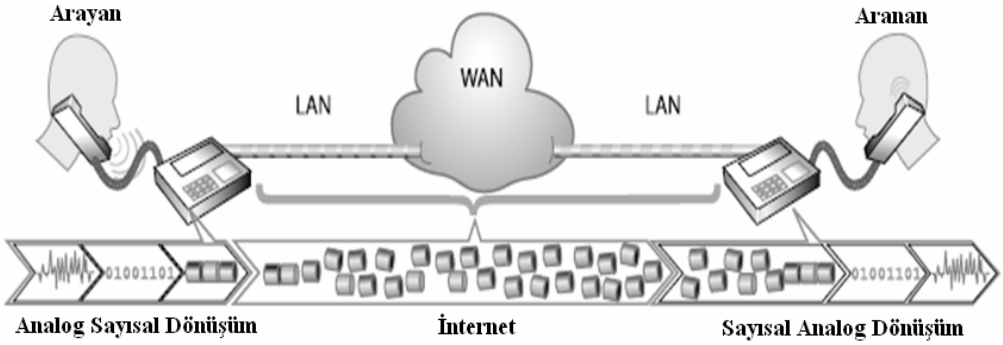
• Gelişme ve yeniliklere açıklık.

VoIP teknolojisinde IP, UDP, TCP, RTP, RTCP protokolleri kullanılarak, verinin terminaller arasında iletimi sağlanır. Bu protokoller VoIP mimarisinin temelini oluştururlar. Bu protokollerin kullanımı H.323 ve SIP olmak üzere, iki temel VoIP sinyalleşme protokolüne bağlı olarak değişir. H.323 ve SIP protokolleri, iletim protokollerinin hangi kurallara bağlı olarak, veri iletimini gerçekleştireceğini belirlerler.

II.1.1 VoIP Mimarisi

VoIP teknolojisi daha önce de belirtildiği gibi, ses paketlerinin IP ağı üzerinden iletilmesi esasına dayanmaktadır. Bu nedenle öncelikle ses verisinin sayısal paketlere dönüştürülmesi gerekmektedir. Şekil II:2'de görüldüğü gibi, IP Telefon, bilgisayar üzerinde kurulu olan bir softphone ya da gateway aracılığıyla ses verisi sayısal

paketlere dönüştürülür. Elde edilen paketler UDP, TCP, RTP protokolleri kullanılarak, veri hattı üzerinden aranan kullanıcıya iletilir. Aranan kullanıcıya ait cihaz, alınan sayısal paketleri analog forma çevirir ve bu şekilde iletişim sağlanmış olur. Ses iletimi sırasında kullanılan protokoller gerçek zamanlı veri iletimini sağlarlar.



Şekil II.2 IP Üzerinden Ses İletim Aşamaları [1]

II.1.1.1 IP (İnternet Protokolü)

IP protokolü, veri paketlerinin yönlendirilmesinden sorumludur. OSI referans modelinin ağ katmanına karşılık gelir. Bu katman, ağlar arasında veri gönderiminin gerçekleştirilmesini sağlayan protokolleri içerir. İletilecek veriler, yönlendirilmek üzere IP katmanına yollanır. Bu katman parçanın içeriğiyle ilgilenmez, yalnızca bu parçayı gideceği adrese yollamakla yükümlüdür. Bunun için, öncelikle bir yol bulur. Yolun saptanmasından sonra kendi başlığını veri paketine ekler Bu başlığın da eklenmesiyle oluşan yeni pakete "datagram" adı verilir. IP başlığının içinde gönderici ve alıcının internet adresi, protokol numarası ve sağlama toplamı vardır. Alıcının internet adresi, iletinin gönderilmek istendiği bilgisayarın adresidir. Bu adres sayesinde, aradaki yönlendiriciler ve geçit yolları bu datagramı nereye yönlendireceklerini bilir. Protokol numarası, bu datagramı TCP'ye vermesi gerektiğini söyler. Sağlama toplamı, IP başlık bilgisinin yolda bozulup bozulmadığını veya yanlış adrese gidip gitmediğini denetlemek için kullanılır. [1,4]

II.1.1.2 TCP (Transmission Control Protocol)

TCP, İletim kontrol protokolü şeklinde tanımlanır. Paket anahtarlamalı veri iletişiminde kayıpsız veri gönderimi sağlayabilmek için geliştirilmiştir. TCP, gönderilen veriler için onay (acknowledgement) mesajı gönderilir. Bu mesaj hangi paketlerin ulaştığını belirlemekte kullanılır. Eğer alıcı taraftan onay mesajı

gelmemişse, iletilemeyen veri tekrar gönderilir. Bu şekilde verinin alıcıya kayıpsız şekilde iletilmesi amaçlanır.

A bilgisayarı ile B bilgisayarı arasında TCP ile şu şekilde bağlantı kurulur:

- A bilgisayarı B bilgisayarına TCP SYNchronize mesajı yollar
- B bilgisayarı A bilgisayarının isteğini aldığına dair bir TCP SYN+ACKnowledgement mesajı yollar.
- A bilgisayarı B bilgisayarına TCP ACK mesajı yollar
- B bilgisayarı bir ACK "TCP connection is established" mesajı alır.

TCP'nin temel işlevi, üst katmandan (uygulama katmanı) gelen bilginin segmentler haline dönüştürülmesi, iletişim ortamında kaybolan bilginin tekrar yollanması ve ayrı sıralar halinde gelebilen bilginin doğru sırada sıralanmasıdır. [1,4]

II.1.1.3 UDP (User Datagram Protocol)

UDP, aktarım katmanı protokolünden birisidir. Bu protokol minimum protokol mekanizmasıyla bir uygulama programından diğerine mesaj göndermek için bir kullanılır. UDP verilerin belirli sıralara konmasının gerekli olmadığı uygulamalarda kullanılmak üzere tasarlanmıştır. Paketin teslim garantisini isteyen uygulamalar TCP protokolünü kullanılır.

Geniş alan ağlarında (WAN) ses ve görüntü aktarımı gibi gerçek zamanlı veri aktarımlarında UDP kullanılır. UDP bağlantı kurulum işlemlerini, akış kontrolü ve tekrar iletim işlemlerini yapmayarak veri iletim süresini en aza indirir. UDP güvenilir olmayan bir aktarım protokolüdür. UDP protokolü ağ üzerinden paketi gönderir ve gidip gitmediğini takip etmez ve paketin yerine ulaşıp ulaşmayacağına onay verme yetkisi yoktur.

UDP protokolü hızlı iletişim kurulması gereken yerlerde tercih edilir. TCP'de olduğu gibi UDP'de de bir başlık vardır. Ağ yazılımı bu UDP başlığını iletilecek bilginin başına koyar. Ardından UDP bu bilgiyi IP katmanına yollar. IP katmanı kendi başlık bilgisini ve protokol numarasını yerleştirir. Fakat UDP, TCP'nin yaptıklarının hepsini yapmaz. Bilgi burada datagramlara bölünmez ve yollanan paketlerin kaydı tutulmaz. UDP'nin tek sağladığı port numarasıdır. Böylece pek çok program UDP' yi kullanabilir. Daha az bilgi içerdiği için, UDP başlığı TCP başlığına göre daha kısadır. Başlık, kaynak ve varış port numaraları ile kontrol toplamını içeren bilgilerden oluşmaktadır. [1,4]

II.1.1.4 RTP (Real Time Protocol)

RTP, gecikmeye karşı duyarlı olan gerçek zamanlı ses ve görüntü verilerini paket anahtarlamalı ağlarda taşımak amacıyla geliştirilmiş bir standarttır. RTP protokolü ilk defa 1996 yılında standartlaştırılmıştır. RTP protokolü ses verilerini UDP protokolü üzerinden taşımaktadır. RTP'nin diğer bir önemli özelliği ise çoklu ortam uygulamalarında birden çok kullanıcının veri transfer işlemini gerçekleştirebilmesidir.

RTP protokolünün sağladıkları başlıca şu şekildedir:

• Sıraya sokma.

• Zaman etiketleme.

• Kaynak belirleme.

RTP, UDP gibi bağlantısız protokollere paketin alındığına dair bir takım bilgiler ekler. RTP protokolünün 'dizi numarası' ve 'zaman damgası' adlarında iki önemli bilgi biti bulunmaktadır. 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 [1,4]

II.1.1.5 RTCP (Real Time Control Protocol)

RTCP protokolü, kontrol paketlerinin zaman zaman özel bir RTP oturumuna ilişkin paylaşımcılara iletimi için kullanır. Bu kontrol paketleri paylaşımcılar hakkında bilgiler içerirler. RTCP paketlerinde bulunan en önemli bilgi ağ iletiminin kalitesidir. Yani RTCP, uç birimlerin sağlayabilecekleri ve alabilecekleri hizmet kalitesi seviyesinden haberdar olmalarını sağlamaktadır. Oturumdaki tüm paylaşımcılar birbirlerine RTCP paketleri yollarlar. RTCP'nin RTP ile sunduğu hizmetler şöyle sıralanabilir:

• Taşınan datanın türünün tanımlanması (ses/görüntü).

• Sıra numaralandırma.

• Data kalitesini (gecikme, kayıp, jitter değerleri) belirleme.

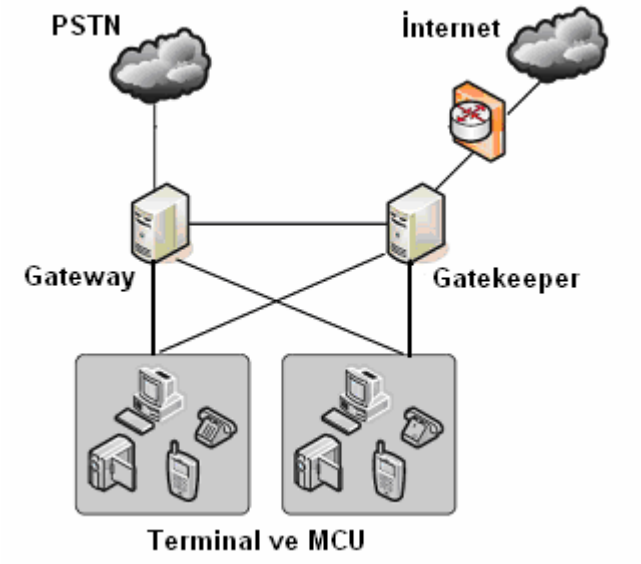
• Katılımcılar hakkında kimlik bilgisi gönderme.

• Zaman damgalama (Time-stamping).

RTCP protokolü başarım bilgisi kontrolünü istatistik raporları tutarak gerçekleştirir. Bu istatistiksel raporlarda, giden paket sayısı, gelen paket sayısı, kaybolan paket sayısı gibi bilgiler yer alır. RTCP, toplam bant genişliğinin %5'ini kullanır ve RTP'ye tuttuğu bilgilerle hizmet kalitesi (QoS-Quality of Servise) geri beslemesi yaptırabilir. [1,4]

II.1.2 H.323

H.323 protokol grubu, farklı iletişim cihazlarının birbirleriyle iletişimine imkan sağlar. H.323, IP tabanlı farklı uygulamaların, birlikte çalışmasını sağlayan ITU tarafından yayımlanan bir protokoldür. H.323 gerçek zamanlı ses, görüntü ve veri iletişimini destekler. Çoğunlukla ses iletimi için kullanılmakla beraber, opsiyonel olarak video ve veri iletimi de gerçekleştirilir. H.323 şebekesi terminal (endpoint), gateway, gatekeeper, ve MCU (multipoint kontrol ünitesi) olmak üzere dört farklı bileşenden oluşur. [5]



Şekil II.3 H.323 Bileşenleri [5]

Terminaller (Telefon, softphone, IVR, sesli mesaj, video kamera, vb.), tipik olarak son kullanıcıların etkileşimde olduğu cihazlardır. MS Netmeeting, bir H.323 terminal bir örneğidir. Terminaller ses veya verinin oluşturulmasını sağlar. Gateway, sinyalleşme ve veri iletişiminde görev alır. Bu birim ISDN, PSTN gibi şebekelerle, H.323 sistemleri arasındaki bağlantıyı sağlar, arayüz olarak hizmet verir.

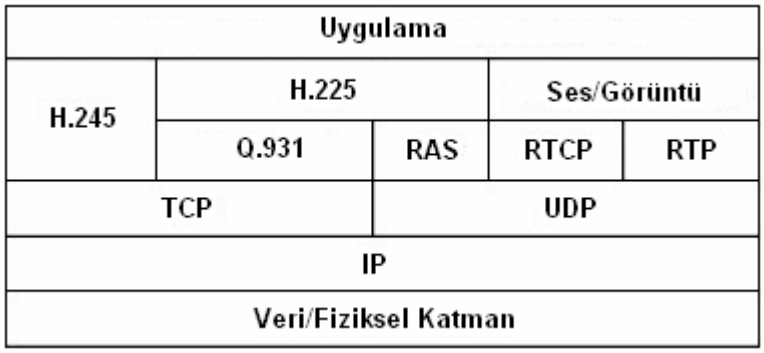
Gatekeeper, adres çözümlemesi ve H.323 sistemindeki yetkilendirme işlemlerini gerçekleştirir. En önemli görevi, simgesel adresler ile IP adresleri arasında adres çevirisidir. Gatekeeper hem görüşme yapılmasını sağlar, hem de

terminallerin servislere, ağ kaynaklarına ve ek özelliklere erişimini sağlar. Aynı zamanda servis kullanımını denetler ve bant genişliğini yönetimi gerçekleştirir. Bir H.323 sisteminde gatekeeper zorunlu değildir. Ama bir gatekeeper mevcutsa, terminaller, gatekeeper tarafından teklif edilen hizmetlerin kullanımını yapmak zorundadır.

MCU, üç veya daha çok terminal arasında multikonferans desteği sağlar. H.323 sistemlerde kullanılan bir diğer bileşen 'BES (Back end server)' olarak adlandırılır. H.323 temelli sistemlerde önemli bir ek fonksiyondur. Kullanıcı doğrulaması, servis yetkilendirme, yeni kullanıcı oluşturma, faturalandırma gibi hizmetler sunar. Basit bir şebekede bu tür hizmetleri, gatekeeper veya gateway sağlar. [5,6]

II.1.2.1 H.323 Mimarisi

H.323, farklı oturumların, cihazların birbiriyle iletişimini sağlayan bir şemsiye protokoldür. H.323, iletişimin sağlanabilmesi için farklı protokollerden yararlanır. Şekil II.4'te konuyla ilgili protokoller ve ilişkileri yer almaktadır.



Şekil II.4 H.323 Yapısı

H.323, çağrı başlangıcını ve görüşme prosedürlerine tanımlar. En önemli VoIP uygulamaları H.225, H.245, ve Q.900 sinyalleşme sisteminin üyeleridir. Gerçek zamanlı veri iletiminde kullanılan protokoller RTP ve RTCP olarak tanımlanır. Ayrıca ses kodlama tekniği olan G.700 serisi kodlama yöntemlerini de destekler.

- H.225/Q.931: Başlangıç ve bitiş sinyallerini tanımlar. Kaynak ve hedef IP adresleri, portlar, ülke kodları ve H.245 port bilgisini içerir.
- H.225/RAS: Sinyal tanımlama mesajlarıdır. Registration, admission and status (RAS) ve veri dizi bilgisini içerir. RAS, terminaller ve gateway'ler arası yönetim protokolüdür.
- H.245: Terminal görüşmesinin başlamasını sağlar. Sunucu-istemci ilişkilerini ve veri dizileri için yerel kanal bilgilerini kontrol eder.

- Real Time Protocol (RTP): Noktadan noktaya gerçek zamanlı veri iletimi sağlar.
- Real Time Control Protocol (RTCP): Noktadan noktaya veri iletimini denetler. Paket kaybı, gecikme gibi QoS (Quality of Service - Servis Kalitesi) parametreleri hakkında bilgi verir.
- Codec: VoIP için kullanılan G.700 serisi kodlar:

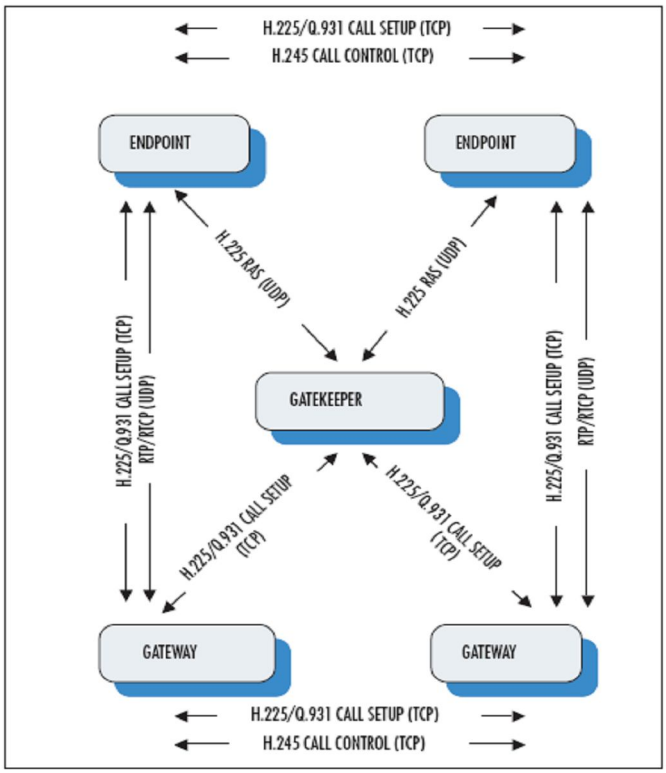
1. G.711 En eski kodlamalardan biridir., G.711 sıkıştırma yapmaz, bu nedenle ses kalitesi çok iyidir. Bu kodlama fazla bant genişliği kullanır. PSTN ve ISDN için bu kodlama kullanılır.

2. G.723.1 Bu kodlama tekniği standart telefon hatları üzerinden video konferans yapılması ve hızlı kodlama ile kod çözme yapılabilmesi için geliştirilmiştir. Orta düzeyde bir ses kalitesi vardır.

3. G.729 Bu kodlama, düşük bant genişliğine ihtiyaç duyduğundan, çoğunlukla VoIP uygulamalarında kullanılır. [5]

H.323 işaretleşmesi tipik olarak, gatekeeper yoluyla veya doğrudan gatekeeper tarafından seçilen kullanıcılar arasında gerçekleştirilir. Veri iletimi genellikle kullanıcılar arasında doğrudan iletilir. H.323 veri iletişiminde, hem TCP hem de UDP kullanılır. TCP, sinyalleşmede kullanılır. Çünkü sinyallerin düzenli olarak iletilmesi gerekir. TCP, sinyalleşmelerin ulaşmasını garanti eder. Ulaşmayan sinyaller tekrar gönderilir. Böylece veri kaybı olmaz. UDP, zamanın önemli olduğu ses ve görüntü paketleri için kullanılır. Zaman zaman oluşan paket kayıpları ihmal edilir. Sonuç olarak, H.225 çağrı işaret etme kanalı ve H.245 çağrı kontrol kanalı tipik olarak TCP üzerinde çalışır. Buna karşın ses, görüntü ve RAS sinyalleri, ulaşım için UDP'yi kullanır.

Şekil II.5'de kullanılan sinyalleşme türlerini göstermektedir. İki tür gatekeeper sinyalleşme metodu vardır. Birincisi, sinyalleşmenin terminaller arası yapıldığı doğrudan sinyalleşme, ikincisi, sinyalleşmenin gatekeeper aracılığıyla yapıldığı gatekeeper yönlendirmeli sinyalleştirmedir. [5]



Şekil II.5 H.323 Sinyalleşmesi [5]

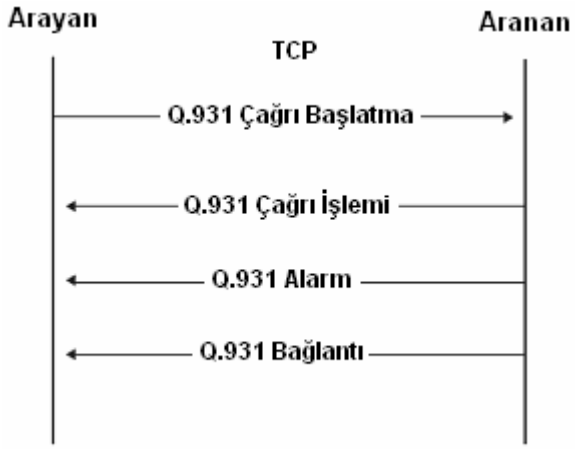
H.225 protokolü, çağrı başlatma için iki önemli standart tanımlar: Çağrı sinyalleşmesi ve RAS. Çağrı sinyalleşmesi, çağrı başlatma, kontrol ve sonlandırma işlemlerinin gerçekleşmesini sağlar. Sinyalleşme kanalı, bağlantı önceliğine göre, terminal-gateway, gateway-gateway ya da gateway-gatekeeper arasında kurulur. Eğer gateway veya gatekeeper bulunmuyorsa H.225 sinyalleşmesi doğrudan terminaller arasında kurulur.

H.225 protokolü terminal-gatekeeper ve gatekeeper-gatekeeper arası iletişimi sağlayan mesajları destekler. H.225'in bu kısmı RAS (Registration, Admissiın, Status) olarak adlandırılır ve sinyalleşme mesajından farklı olarak UDP üzerinden taşınır. RAS, kayıt, yetkilendirme kontrolü, bant genişliği durumundaki değişiklikler ve terminal ile gatekeeper arasındaki sonlandırma işlemlerini düzenlemek için kullanılır.

Bir RAS kanalı, RAS mesajlarını kullanarak sinyalleşme kanalından ayrılır. İkinci sinyalleşme kanalı eklenen kanalların bağlantı önceliğine göre terminal ile gatekeeper arasında kullanılır.

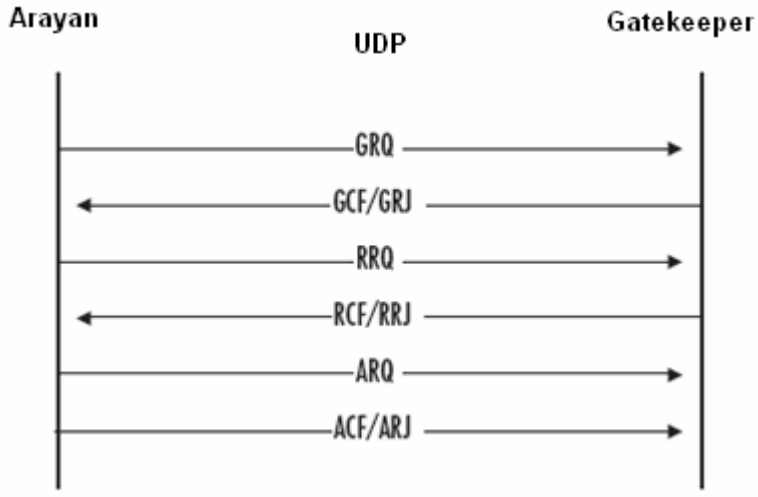
Oturumun kurulacağı birimlerin sahip olduğu niteliklere göre, İki terminal arasında bir çağrı akışı kurulur. İki terminal arasında doğrudan bağlantı oluşturmak

için, öncelikle terminaller arasında iki TCP kanalı kurulur: Biri çağrı başlangıcı (H.225/Q931) için, diğeri veri transferi ve çağrı kontrolü (H.245 mesajları) için kullanılır. Şekil II.6'da görüldüğü gibi, çağrı başlangıcı için, terminallerden biri diğerine TCP üzerinden H.225/Q931 sinyali gönderir. Aranan terminal tarafından aranan kullanıcıya alarm sesi gönderilir. Bu sinyalleşmeler, aranan terminal hattı açana dek sürer. Aranan terminalin hattı açmasıyla bağlantı gerçekleşir. Bağlantının sağlanmasının ardından H.245 sinyalleri taşınabilir.



Şekil II.6 H.225/Q931 Sinyalleşmesi

Eğer terminaller arasında bir gatekeeper varsa, H.225/RAS sinyalleşmesi, Q.931 sinyalleşmesinden önce uygulanır Şekil II.7'de gösterilen akış diyagramı oluşur.



Şekil II.7 H.225/RAS Sinyalleşmesi

Bu mesajlar bir gatekeeper'a kaydolmak ve çağrı başlatma isteğinde bulunmak için kullanılır.

- Gatekeeper Request (GRQ): GRQ mesajı, bağlantı yapılacak bir gatekeeper varlığını sorgulamak için kullanılan tek yönlü bir sinyaldir. Bu mesajla gatekeeper

IP'si kullanılarak terminal konfigürasyonları gerçekleştirilir. Konfigürasyonlar gerçekleştirilemezse, terminal isteği geri çevirir.

- Gatekeeper Confirm or Reject (GCF/GRJ): Gatekeeper'dan kayıt isteğine karşı kabul veya ret cevabıdır. Genellikle konfigürasyon hatalarından kaynaklanır.
- Registration Request (RRQ): Bir terminal veya gateway'den, gatekeeper'a yapılan kayıt isteğidir.
- Registration Confirm or Reject (RCF/RRJ): Gatekeeper'ın kayıt isteği için terminal veya gateway'e gönderdiği, kabul veya ret mesajıdır.
- Admission Request (ARQ): Bir terminal ya da gateway'den yapılan paket anahtarlamalı ağa erişim isteğidir.
- Admission Confirm or Reject (ACF/ARJ): Gatekeeper'ın paket anahtarlamalı ağa erişim için, terminal veya gateway'e gönderdiği, kabul veya ret mesajıdır. Eğer kabul edilirse, iletim adresi ve portu sinyalleşme yapılabilmesi için yanıtla birlikte gönderilir.

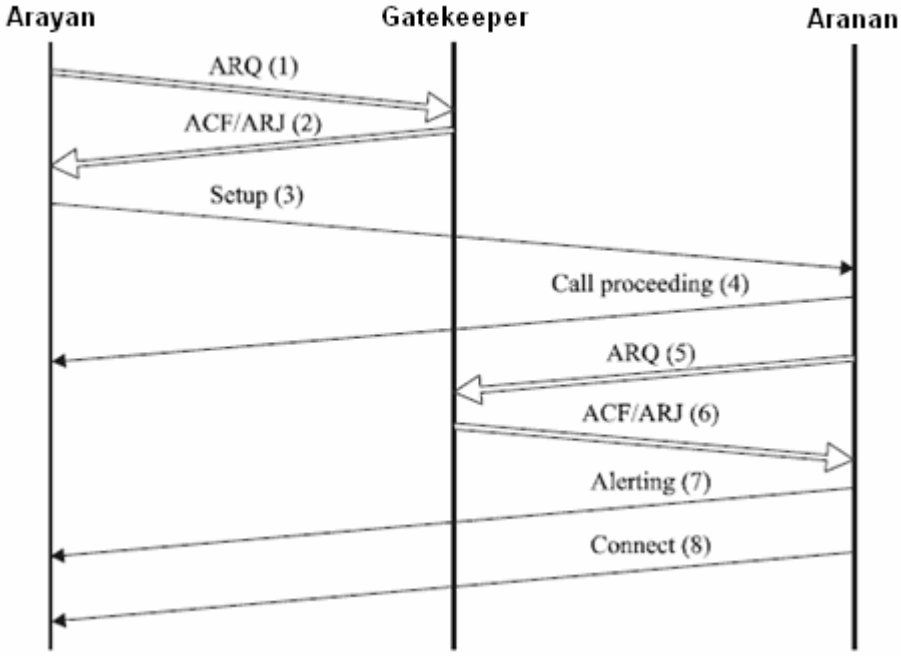
H.225/RAS sinyalinde bant genişliği tahsisinde değişiklikler hakkında istekte bulunmak, zamanlayıcıları sıfırlamak gibi bilgileri içeren mesajlar yer alır. Gatekeeper kayıt isteğini onayladıktan sonra sinyalleşme başlayabilir. [5]

II.1.2.2 Çağrı Başlatma Senaryoları

H.323 protokolünde çağrı başlatma senaryoları, H.225 sinyalleşme protokolü esasına göre gerçekleşir. Q.931 ya da RAS sinyallerinden hangilerinin kullanılacağı, terminaller arası gatekeeper olması durumuna göre belirlenir. Bunların haricinde daha önce belirtildiği gibi, doğrudan ve gatekeeper yönlendirmeli olmak üzere iki farklı sinyalleşme yöntemi vardır. Bu sinyalleşme yöntemleri ne tür bir çağrı başlatma senaryosu gerçekleşeceğini belirler.

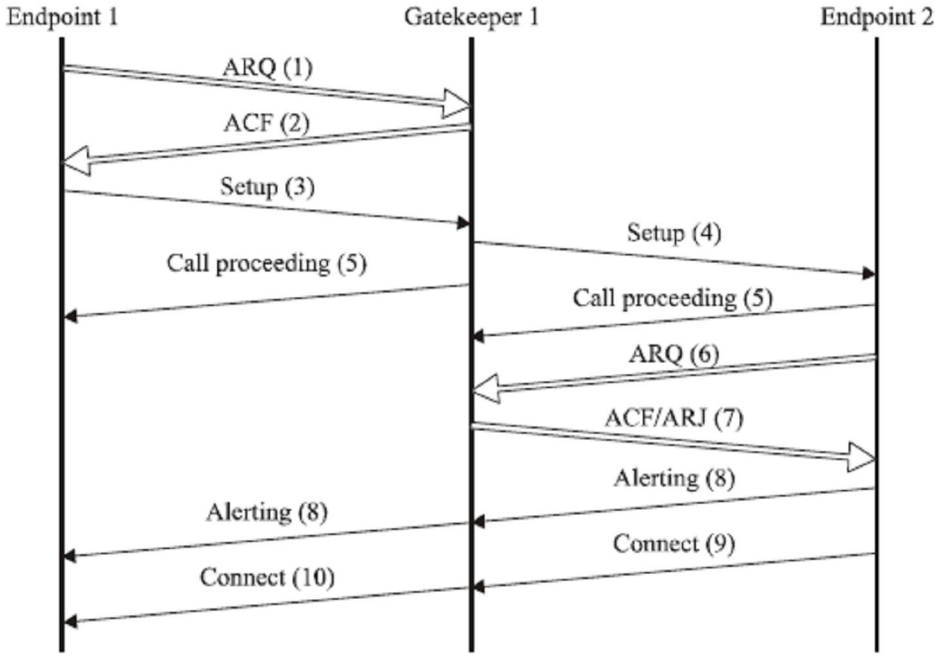
Şekil II.8'de Doğrudan yönlendirmeli bir çağrı başlatma işlemi görülmektedir. Aramayı gerçekleştiren kullanıcı gatekeeper'a başvurarak, çağrı isteğini bildirir. Bu işlem için, ağa erişmek istediğini belirten 'ARQ' mesajı gönderir. Gatekeeper bu isteği onayladığını belirten 'ACF' ya da reddettiğini belirten 'ARJ' mesajı gönderir. Gatekeeper'dan onay verilmesi durumunda. Arayan kullanıcı, aranan kullanıcıya çağrı başlatma sinyali gönderir. Aranan kullanıcı gatekeeper'a 'ARQ' mesajı göndererek, çağrıyı cevaplamak için izin ister. Gatekeeper'ın onay vermesi durumunda, aranan kullanıcıdan arayan kullanıcıya alarm sesi iletilir. Aranan

kullanıcının hattı açmasıyla birlikte veri paketlerini aktaracak ortam hazır hale gelmiştir. Bu senaryonun doğrudan yönlendirmeli olması, çağrı başlangıç ve bağlantı sinyallerinin terminaller arasında gerçekleşmesinden kaynaklanmaktadır.



Şekil II.8 Doğrudan Çağrı Sinyalleşmesi [5]

Şekil II.9'da Gatekeeper yönlendirmeli bir çağrı başlatma işlemi görülmektedir. Aramayı gerçekleştiren kullanıcı gatekeeper'a başvurarak, çağrı isteğini bildirir. Bu işlem için, ağa erişmek istediğini belirten 'ARQ' mesajı gönderir. Gatekeeper bu isteği onayladığını belirten 'ACF' ya da reddettiğini belirten 'ARJ' mesajı gönderir. Gatekeeper'dan onay verilmesi durumunda. Arayan kullanıcı, gatekeeper'a çağrı başlatma sinyali gönderir. Gatekeeper bu çağrı başlatma sinyalini aranan kullanıcıya aktarır. Aranan kullanıcı gatekeeper'a 'ARQ' mesajı göndererek, çağrıyı cevaplamak için izin ister. Gatekeeper'ın onay vermesi durumunda, aranan kullanıcıdan gatekeeper'a alarm sinyali gönderir. Gatekeeper, bu sinyali aranan kullanıcıya iletilir. Aranan kullanıcının hattı açmasıyla birlikte veri paketlerini aktaracak ortam hazır hale gelmiştir. Bu senaryonun gatekeeper yönlendirmeli olması çağrı başlangıç ve bağlantı sinyallerinin gatekeeper kontrolünde gerçekleşmesinden kaynaklanmaktadır. [5]

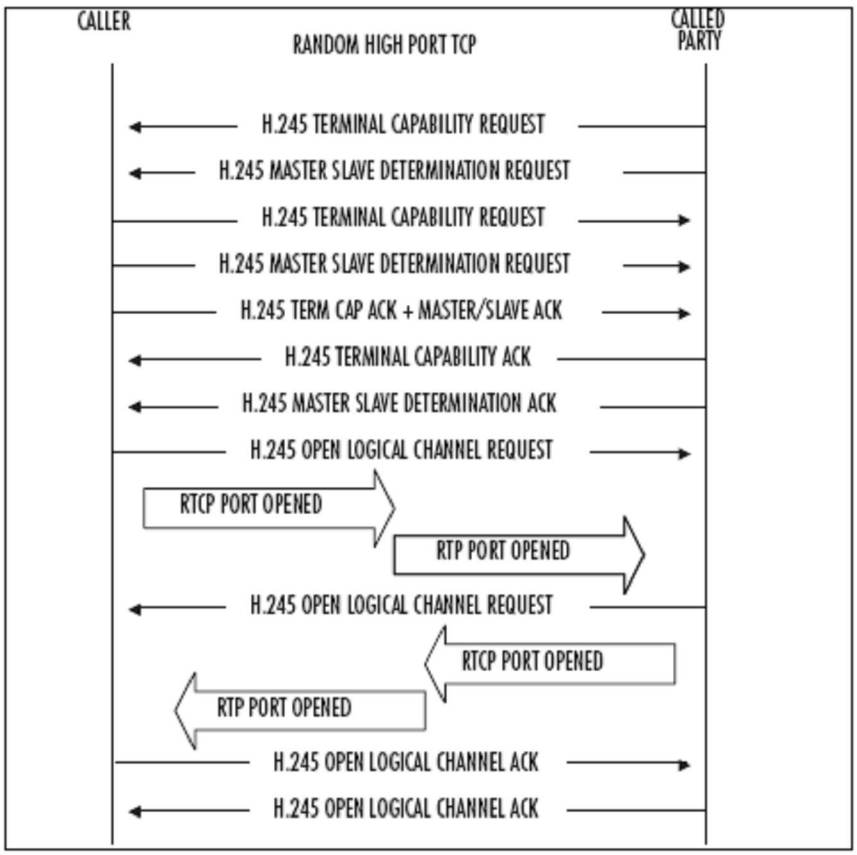


Şekil II.9 Gatekeeper yönlendirmeli çağrı sinyalleşmesi [5]

II.1.2.3 Çağrı Kontrol Mesajları

Çağrı sinyalleşme prosedürü kullanılarak bağlantı sağlandıktan sonra, H.245 mesajları kullanılarak veri tipine, terminal özelliklerine ve görüşme başlamadan önce bağlantı akış prosedürüne karar verilir. Aynı zamanda H.245 çağrı kurulumu gerçekleştikten sonra da çağrı parametrelerini kontrol eder. Mesajlar terminal özelliklerine ait bilgiyi taşır. Yerel kanallara açık ya da kapalı olacağı bilgisini aktarır. H.245 kontrol kanalı, veri kanallarından farklı olarak, sürekli açıktır.

H.245 için tanımlanmış sabit bir port yoktur. H.245 iletim adresi her zaman çağrı sinyalleşme mesajın içinden geçer. Öte yandan port bilgisi veri içerisinde H.225/Q.931 sinyalinden önce gelir. Veri kanalları da benzer şekilde tahsis edilir.



Şekil II.10 H.245 Çağrı Kontrolü [5]

Aranan terminal H225/Q.931 sinyal paketindeki port bilgisine eriştikten sonra, bağlantıyı sağlamak için TCP portunu açar. Bu işlem sırasında kodlama türü, sunucu/istemci bilgileri belirlenir. Veri kanalı görüşmeleri 'Open Logical Channel Request' mesajıyla başlar. Aranan kişi konuşmaya hazır olduğunda, dinamik port bilgisini içeren 'Open Logical Channel Ack' mesajı ile cevap verir. Dinamik potların kullanılması, güvenlik duvarları, NAT ve trafik akışında güvenlik tedbirleri almayı zorlaştırır. Bazı durumlarda, H.323 sinyalleşmesinin ve verinin güvenli geçişini sağlamak için, zararlı durumları bildirecek özel bir 'H.323 aware firewall' ya da güvenlik duvarlarının bir parçası olan 'Application Layer Gateway' kullanılır. Ardından RTP ve RTCP kanalları birlikte açılarak bağlantı sürdürülür. [5]

II.1.3 SIP

Oturum başlatma protokolü (SIP-Session Initiation Protokol) IETF tarafından IP üzerinden çoklu ortam görüşmesi yapabilmek için bir standart olarak oluşturulmuştur. RFC 2543 ile tanımlanmış ve RFC 3261 ile geliştirilip son halini almıştır. SIP iki veya daha fazla katılımcı arasındaki çoklu ortam (multimedia) oturumlarının kurulması, yürütülmesi ve sonlandırılması işlemlerini gerçekleştiren

bir sinyalleşme ve kontrol protokolüdür. SIP protokolü kullanıcılar arasındaki işaretleşme mekanizmalarını ve oturumun açılması için gerekli olan parametreleri (kodlayıcı bilgileri, lokasyon bilgileri, vb.) tanımlayarak ve gerekli ara işlemleri yaparak katılımcıların başarılı bir şekilde oturum kurmalarını sağlamaktadır.

Ses ve videonun iletilmesin ötesinde, anlık mesajlaşmayı destekler. Birçok anlık mesajlaşma programının bulunduğu uygulamalarda en sık kullanılan protokoldür. Bu özellik 'SIMPLE' olarak adlandırılır. SIMPLE, SIP'e benzer şekilde oturum başlatma görevi üstlenir. Aynı zamanda kullanıcının çevrimiçi, meşgul ya da diğer durumları hakkında bilgi verir. Bu tür metotların kullanıldığı uygulamalarda SIP tercih edilir ve bu durum SIP'in, haberleşme en çok kullanılan bileşenlerden olmasını sağlar. [1,5]

SIP protokolünün başlıca özellikleri şu şekildedir:

• Protokol HTTP protokolünden esinlenerek oluşturulmuştur. HTML'de kullanılan kodlar ufak değişikliklerle SIP protokolünde de kullanılabilmektedir.

• Düz metin (ASCII text based) yapısındadır. Dolayısıyla uygulanması ve yönetilmesi çok basittir.

• Genişleme yeteneğine sahip bir protokoldür. Zamanla yeni özellikler bu protokole kazandırılabilir.

• Büyük trafik hacimlerini karşılayabilmektedir.

• Web ile entegre olma yeteneğine sahiptir. Böylece e-posta gibi uygulamalarla ve diğer protokollerle kolayca çalışabilir.

• TCP ve UDP protokollerinin her ikisini de desteklemektedir.

II.1.3.1 SIP Fonksiyonları

SIP oluşturulurken, oturum başlatma ve sonlandırma hakkında beş temel öğeyi desteklemek üzere tasarlanmıştır. Bu beş özellik bir çağrının oluşturulması için gerekli nitelikleri sağlar. Ancak bu özelliklerin kullanılabilmesi için, diğer protokollerden faydalanılır.

II.1.3.1.1 Kullanıcı Yeri (User Location)

Kullanıcının yerinin tespit edilmesi için, kullanılan bilgisayarın kullanıcı adından güncel IP adresine ulaşılmasını sağlar. Bu önemli bir durumdur, çünkü kullanıcı farklı bilgisayarlardan bağlantı sağlayabilir ya da bir yerel ağda farklı bir IP adresiyle bağlanabilir.

Kullanılan program kullanıcının bir sunucuya kaydını gerçekleştirmek için SIP protokolünü kullanabilir. Sunucu ile kullanıcı arasında bir IP adresi ve kullanıcı adı tanımlanır. Ancak bu durumda sunucu kullanıcıyı tanır ve diğer kullanıcılar kayıt gerçekleştiren kullanıcıyla bağlantı sağlayabilir. Kullanıcılar birbirlerinin IP adresine ulaştıktan sonra sunucu üzerinden oturum açma isteğinde bulunur ve bağlantıyı kurarlar.

II.1.3.1.2 Kullanıcı Erişilebilirliği (User Availability)

Kullanıcı erişilebilirliğini belirleyen bu özellik, bağlantı kurulmuş olan kullanıcıların durumunu kontrol imkanı sağlar. Kullanıcılar kendilerini dışarıda, meşgul gibi durumlarda gösterebilir. Eğer ulaşılabilir durumdaysa diğer kullanıcılar tarafından, kullanılan programın özelliğine göre, sesli veya görüntülü konuşmaya davet edilebilir.

II.1.3.1.3 Kullanıcı Nitelikleri (User Capabilities)

Kullanıcı özellikleri, kullanılan bileşenin özelliklerine ve oturum sırasındaki görüşmelere bağlı olarak hesaplanır. SIP farklı platformlarda, farklı programlar tarafından kullanılabilir ve tekli veya çoklu görüşmeye bağlı olarak parametrelerin hesaplanması gerekir. Örneğin, bir kullanıcı arandığında, arayan terminaller görüntülü konuşmayı destekleyebilir ancak aranan terminal bu özelliği kullanamayabilir. Kullanıcı yeteneklerinin hesaplanması, kullanıcıların oturum sırasında hangi özellikleri, veri tiplerini ve parametreleri kullanacaklarını belirler.

II.1.3.1.4 Oturum Başlatma (Session Setup)

Kullanıcıların birlikte bağlandıkları kısımdır. Oturuma katılan bir kullanıcı bağlantıyı sağlayacak bir programa sahip olmalı ya da akış prosedürlerini yerine getirmelidir. Aranılan kullanıcı kabul veya ret seçeneğini kullanabilir. Eğer kabul edilirse oturum parametrelerinde uzlaşılır ve bağlantı sağlanır. Böylece iki terminal arasında, iletişim kurmalarını sağlayacak bir oturum başlamış olur.

II.1.3.1.5 Oturum Yönetimi (Session Management)

Oturum yönetimi SIP'in son özelliğidir. Oturum özelliklerinin oturum sırasında değiştirilmesini sağlar. Oturum esnasında, veri kullanıcılar arasında iletilen veri tipleri değişebilir. Örneğin, bir konuşma esnasında, kullanıcılar diğer hizmetleri

kullanarak görüntülü konuşma başlatmayı isteyebilirler. Yeni bir kullanıcının konuşmaya dahil olması veya çıkarılması, bir kullanıcının bekletilmesi, oturumun sonlandırılması gerekebilir. Tüm bu işlemler SIP'in oturum yönetimi özelliği sayesinde gerçekleştirilir.

II.1.3.2 SIP Mimarisi

SIP, çeşitli bileşenler ve protokoller olmadan bir ağ üzerinde oturum kurulması işlemini gerçekleştiremez. Kullanılacak olan bileşenler, bağlantı sırasında katılımcıların birbirleriyle iletişim kurmasını sağlar. Protokoller ise, bilgisayar ya da diğer bileşenler arasında veri taşınması görevini üstlenir. Tüm bunlar SIP mimarisini oluşturur. [5]

II.1.3.2.1 SIP Bileşenleri

SIP, diğer teknolojiler ve protokollerle birlikte çalışabilmesine rağmen, oturum başlatma protokolü ile kullanılan iki temel bileşen vardır:

- User agent (Kullanıcı, terminal), konuşmayı başlatan ve hedefteki aranan birim olarak tanımlanır. Terminaller, biri istemci, diğeri sunucu olmak üzere iki kısımdan oluşur. Kullanıcı, bir oturumu başlatmak için bir istekte bulunduğu durumda kullanıcı (UAC, User agent client), isteğe cevap veren konumunda bulunduğu durumda sunucu (UAS, User agent server) görevini üstlenir. Kullanıcı bu iki görevi değişken olarak gerçekleştirir. Kullanıcı önce bir mesaj yollayacak, ardından gelen isteğe cevap verecek, sonra tekrar istekte bulunacak ve işlemler bu sırayla devam edecektir. UAC ve UAS oturum sırasında rollerini değiştirerek veri transferini gerçekleştirirler. Kullanıcı, genellikle bilgisayarda yüklü bir yazılım, bir PDA, bilgisayara bağlı bir telefon ya da PSTN'e bağlı bir gateway olabilir. Tüm bu durumlarda, kullanıcı hem istemci, hem sunucu gibi davranarak, mesaj isteğinde bulunur ve gelen isteklere cevap verir.
- SIP server (SIP sunucu), terminallerin kullanıcı adlarını kullanarak, IP adreslerine erişir ve verinin kullanıcılar arasında iletilmesini sağlar. Böylece mesajlar bir kullanıcıdan diğerine doğru bir şekilde iletilebilir. Kullanıcılar ağ üzerindeki güncel konumlarından elde ettikleri IP adresi ve kullanıcı adıyla SIP sunucuya kayıt olurlar. Bu kullanıcıların erişilebilir durumda olduklarını gösterir ve diğer kullanıcılar tarafından bu durum fark edilerek oturuma davet edilmeleri mümkün olur. Oturuma davet edilen kullanıcının erişilebilirlik durumu, SIP sunucu tarafından

kontrol edilir. SIP sunucusu, kullanıcı adı ve IP adresini kullanarak konum belirlemesi yapar. Eğer kullanıcı farklı bir bölgede bulunuyorsa ya da farklı bir SIP sunucusuna kayıtlı ise, istek mesajı diğer sunucuya iletilir.

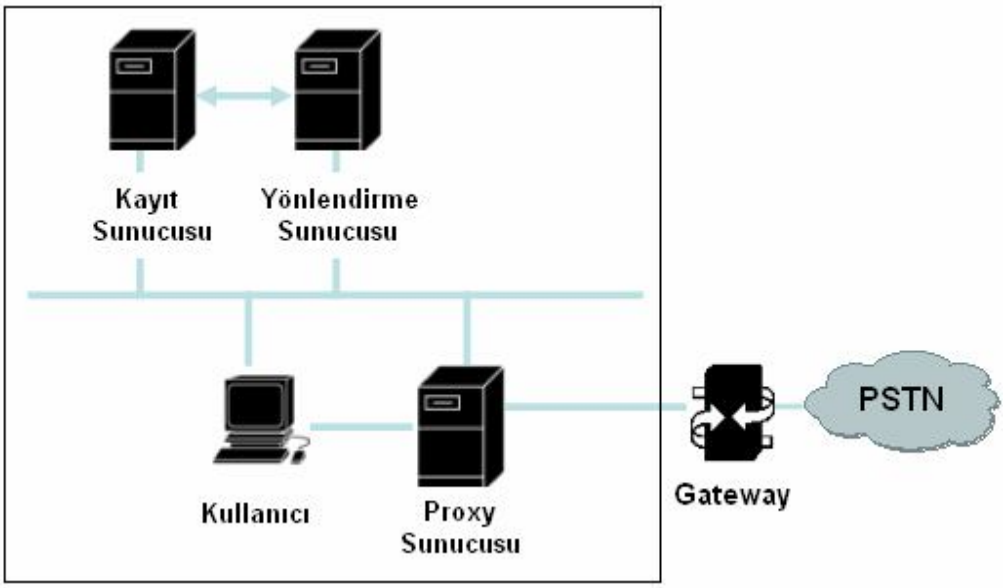
SIP sunucusu, kullanıcı mesajlarının iletimindeki bu farklı işlevleri gerçekleştirmek için farklı görevler üstlenir.

- Kayıt Sunucusu (Registrar server)
- Proxy server
- Yönlendirme Sunucusu (Redirect server)

1) Kayıt Sunucusu: Kayıt sunucuları (Registrar server), ağa kaydolan bir kullanıcının yerini kaydetmekte kullanılır. Kullanıcının IP adresini elde eder ve kullanıcı adıyla birlikte sisteme kaydeder. Bu şekilde ağa kayıtlı olan kullanıcılar ve konumları güncel bir şeklinde oluşturulur. Bir kullanıcı oturum kurmak istediği zaman, kayıt sunucusu, kayıtlı IP adreslerini kullanarak adres doğrulaması yapar ve istenen kullanıcıya ulaşır.

2) Proxy Sunucu: Proxy sunucuları, bir kullanıcıdan iletilen mesajları, onun adına diğer kullanıcılara iletmekle görevlidir. Kullanıcılara vekalet ederler. SIP sunucusu, bir kullanıcıdan aldığı mesajı başka bir SIP sunucusuna iletebilir. Eğer Proxy sunucusu kullanılıyorsa, işlemler sırasında, ağ iletişim kontrolü, güvenlik, kimlik doğrulama özellikleri kullanılabilir.

3) Yönlendirme sunucusu: Yönlendirme sunucusu (Redirect server), katılımcıların, erişilmek istenen kullanıcıya erişilmesini sağlar. Bir katılımcı bağlantı isteğinde bulunduğunda, yönlendirme sunucusu, kayıtlı kullanıcının IP adresini kullanarak cevap verir. Bu Proxy sunucusundan farklı bir durumdur. Proxy sunucusu kullanıcı yerine hareket eder, vekalet eder. Yönlendirme sucusu ise, kullanıcılara nasıl bağlanacağını söyler, yol gösterir. Yönlendirme sunucusu, bir çağrıyı aynı anda birden fazla konuma aktarabilme yeteneğine sahiptir. Bir kullanıcının arama yapması durumunda yönlendirme sunucusu bu çağrıyı farklı kullanıcılara yönlendirebilir ve tüm kullanıcılara aynı anda sinyal gönderilir. Kullanıcılardan biri yanıt verdiğinde, diğer kullanıcılara giden sinyal kesilir. [5]



Şekil II.11 SIP Bileşenleri

II.1.3.2.2 SIP İsimleri ve Adresleri

SIP protokolünde kullanıcılar SIP adresleriyle tanımlıdırlar. Bu adresler aslında e-posta adresleriyle büyük bir benzerlik göstermektedirler. Bu adresler SIP URL olarak da bilinirler. Basit bir SIP URL adresi "sip:kullanıcı_adı@servis_sağlayıcı" şeklindedir. Burada; "kullanıcı_adı" bölümü bir kullanıcıya atanmış bir isim ya da bir telefon numarası olabilirken; "servis_sağlayıcı" bölümü ise, bir alan adı ya da bir IP adresi olabilmektedir. SIP URL adreslerine aşağıda birkaç örnek verilmiştir: [2]

02124552525@system.com

voip@system.com

02124552525@192.168.0.22

II.1.3.2.3 SIP Mesajları

SIP, HTTP gibi metin-temelli bir protokoldür, sunucu ve istemciler arasında bilgi aktarımı için kullanılır. İstemci ve sunucular sırayla değişerek, istek ve cevap mesajları gönderirler. Bu mesajlaşmanın gerçekleşebilmesi için tanımlanmış, bir dizi sinyalleşme komutu mevcuttur. Bileşenler mesajlaşma sırasında, birbirlerine ait kimlik bilgilerini karşı tarafa iletirler. SDP (Session Description Protocol) tarafından gönderilen bu verilerde, kullanılan kodlama yöntemi, kullanıcı adı gibi bilgiler yer alır. Bir kullanıcı diğer kullanıcıya 'invite' mesajı gönderdiğinde, bu mesajla birlikte SDP bilgisini de gönderir. Böylece, iletişim parametrelerinde anlaşma sağlanır. SIP bileşenleri arasında iletilen mesajlar şunlardır:

- **Register:** Bir kullanıcının ilk kez erişilebilir konuma geçtiği ve SIP adresi ile IP adresini kullanarak kayıt sunucusuna kayıt isteğinde bulunması için kullanılır.
- **Invite:** Bir başka SIP kullanıcısını iletişime çağırmak için kullanılır ve ardından aralarında bir SIP oturumu kurulur.
- **Ack:** Oturum isteğini kabul etmek ve mesaj değişimini onaylamak için kullanılır.
- **Options:** Diğer kullanıcıların özelliklerini hakkında bilgi edinmek için kullanılır.
- **Subscribe:** Kullanıcıların durumunu belirlemek için kullanılır. Bu sayede kullanıcının erişilebilir, meşgul, uzakta gibi durumlardan hangisinde bulunduğu belirlenir.
- **Notify:** Kullanıcının son durumunu güncellemesi için istekte bulunulacağı durumlarda kullanılır.
- **Cancel:** Oturum sonlandırılmadan, bağlantıdan vazgeçme isteğini belirtir.
- **Bye:** Bağlantıyı bitirme isteğini belirtir. Arayan ya da aranan kullanıcı bu komutu kullanarak, oturumu sonlandırma isteğini karşı tarafa iletir.

Bir SIP sunucuya ya da bir kullanıcıya bir mesaj gönderildiğinde, iletilebilecek olası cevaplar altı kategoride toplanmıştır:

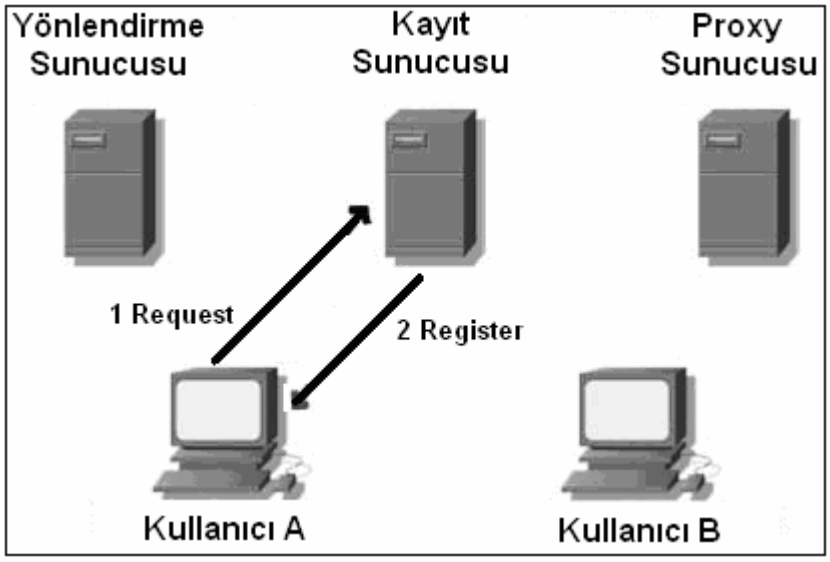
- **Bilgilendirme Mesajları (1xx):** Mesajın alındığını ve işlem aşamasında olduğunu belirtir.
- **Başarı Mesajları (2xx):** Mesajın alındığını ve kabul edildiğini belirtir.
- **Yönlendirme Mesajları (3xx):** İşlemin tamamlanamadığını ve ek işlemlerin gerektiğini belirtir.
- **Kullanıcı Hataları (4xx):** Mesajda hatalar oluştuğunu, Bu nedenle sunucunun işlemi gerçekleştiremediğini belirtir.
- **Sunucu Hataları (5xx):** Mesajın alındığını, ancak sunucunun işlemi gerçekleştiremediğini belirtir.
- **Genel Hatalar (6xx):** Genel Hataları Belirtir. [5,6]

II.1.3.2.4 SIP Çağrı Akışı

Bu bölümde, iki terminal arasındaki iletişimin nasıl gerçekleştiği incelenecektir. Bir yerel ağda veya internet üzerinde, farklı bileşenlerin nasıl birlikte çalıştığı, sinyalleşmenin nasıl gerçekleştiği belirtilecektir.

Kullanıcılar, diğer kullanıcıya ulaşmak için, farklı sunuculara mesaj gönderirler. Bir başka kullanıcı ile oturum kurulana dek, sunucu-istemci ilişkisi devam eder ve sunucu-istemci mimarisi devrededir. Arama isteğinde bulunan kullanıcı sunuculara bağlantı isteğinde bulunur ve bu isteğe cevap verilmesini bekler. İki kullanıcı arasında oturum başlamasıyla birlikte mimari değişir. Artık kullanıcı bir başka kullanıcıyla ya da bir sunucuyla oturum başlatmıştır. Bu noktada kullanıcılar arası, noktadan noktaya (peer to peer, P2P) mimari devreye girer. Bu mimaride bilgisayarlar birbirine denktir. Sunucuya aynı şekilde istekte bulunurlar. [5]

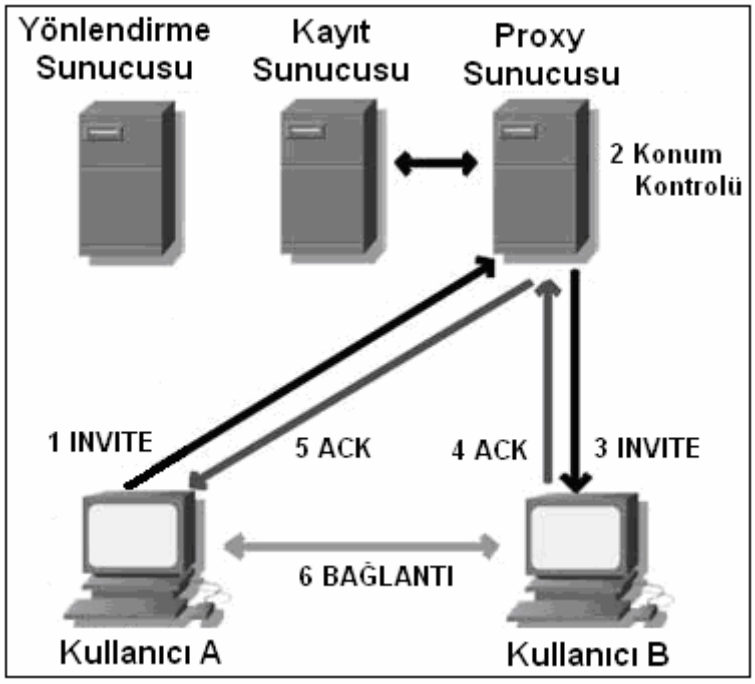
1) SIP Registration: Bir kullanıcı, başka bir kullanıcıyla iletişim kurmak için istekte bulunmadan önce, bir kayıt sucusuna bağlanmalıdır. Kullanıcı, kayıt sunucusuna bir 'Register' mesajı gönderir. Sunucu bu isteği kabul ederse, kullanıcının SIP adresini ve IP adresini konum servisine kaydeder. Konum servisi daha sonra kullanıcı adından SIP adresine ve IP adresine ulaşılmasını sağlar.



Şekil II.12 Kullanıcı Kayıt İşlemi [5]

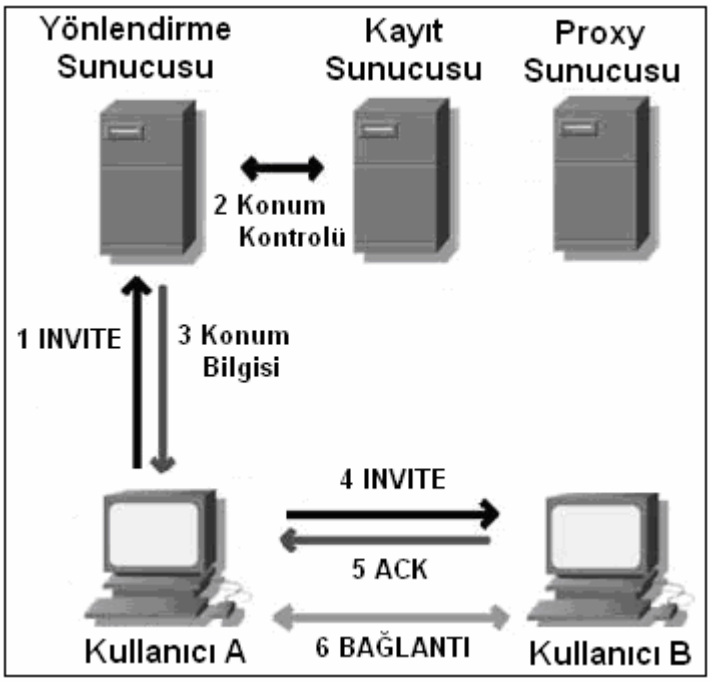
• Proxy Sunucu Aracılıyla Çağrı Kurulumu: Bir kullanıcının, proxy sunucusu kullanarak istekte bulunması ve cevap vermesi, Proxy yönlendirmeli bir bağlantı gerçekleştirildiğini gösterir. Şekil II.13'te A kullanıcısının, B kullanıcısına oturum başlatmak için, bir Proxy sunucusu üzerinden 'invite' mesajı göndermek istediği görülmektedir. Oturuma davet edilen kullanıcının IP adresi konum servisinden kontrol edilir. Proxy sunucusu oturum isteğini belirlenen adres üzerinden B kullanıcısına gönderilir. Proxy daha sonra B kullanıcısından gelen cevabı, A kullanıcısına iletir. Bu ana kadar iki kullanıcı ve Proxy sunucusu, sinyalleşmeyi SDP

üzerinden göndermişlerdir. Bu adımlar tamamlandıktan sonra, Proxy sunucusu her iki kullanıcıya da bir onay mesajı gönderir ve kullanıcılar arasında bir oturum kurulmuş olur. Bu noktadan itibaren, kullanıcılar aralarında veri transferi gerçekleştirmek için RTP kullanırlar.



Şekil II.13 Proxy Sunucu Aracılığıyla Çağrı Kurulumu [5]

- Yönlendirme Sunucusu Aracılığıyla Çağrı Kurulumu: Bir kullanıcının, yönlendirme sunucusu kullanarak istekte bulunması ve cevap vermesi, yönlendirme sunucusu yönlendirmeli bir bağlantı gerçekleştirildiğini gösterir. Şekil II.14'te A kullanıcısının, B kullanıcısına oturum başlatmak için, bir yönlendirme sunucusu üzerinden 'invite' mesajı göndermek istediği görülüyor. Oturuma davet edilen kullanıcının IP adresi, konum servisinden kontrol edilir. Yönlendirme sunucusu adres bilgisini A kullanıcısına iletir. A kullanıcısı artık bağlantıyı sağlamak için gerekli bilgiye sahiptir. A kullanıcısı, B kullanıcısına 'invite' mesajı gönderir. B kullanıcısı bu isteğe bir cevap gönderir. Bu noktaya kadar sinyalleşme SDP üzerinden gerçekleşir. İki terminal arasında oturumun kurulmasıyla birlikte, veri transferi RTP üzerinden gerçekleştirilir.

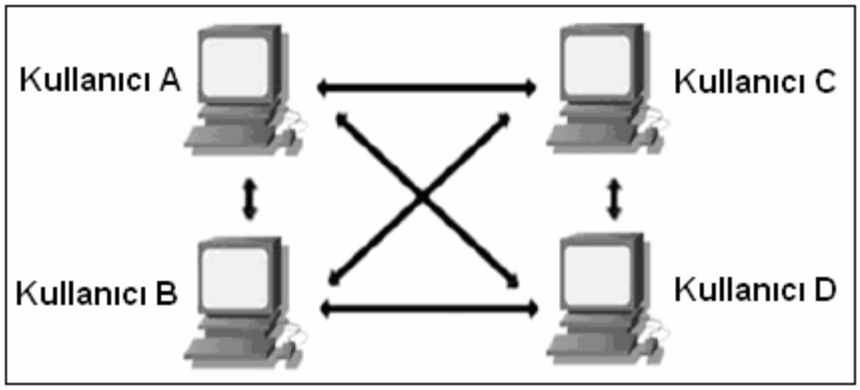


Şekil II.14 Yönlendirme Sunucusu Aracılığıyla Çağrı Kurulumu [5]

2) Peer to Peer (Noktadan Nokataya): Kullanıcılar kayıt işlemlerini tamamlayıp, sinyalleşmeleri bulundukları konumdan kendileri yapmaya başlayınca, sunucu-istemci mimarisinden, noktalar arası (P2P) mimariye geçerler. P2P mimarisinde, kullanıcılar hem istemci, hem de sunucu olarak görev yaparlar.

Bu mimaride kaynaklar tek bir sunucudan ya da küçük bir grup bilgisayardan ibaret değildir. Ağdaki her kullanıcı aynı zamanda bir kaynak hizmeti sağlar. Bir kullanıcı oturum başlatmak istediğinde, diğer kullanıcılar hem sunucu ve istemci olarak görev yapabilirler. Her kullanıcı bir başka katılımcıyı oturuma davet edebilir.

Şekil II.15'de kullanıcıların birbirleriyle sesli veya görüntülü konuşma yapabildiği gösterilmektedir. Kullanıcılardan herhangi biri oturumu sonlandırabilir. Kullanıcılardan birinde bir sorun olduğu zaman, diğer kullanıcılar bu durumdan etkilenmeden konuşmalarına devam edebilirler. Bu mimari kullanıcılar arasındaki iletişimi sürekli hale getirir ve ağda oluşacak sorunlardan en az derecede etkilenilmesini sağlar. [5]



Şekil II.15 Noktadan Noktaya Çağrı Akışı [5]

II.2 TEHDİTLER ve SALDIRILAR

İletişim şebekelerinin güvenliği, birkaç farklı açıdan analiz edilebilir. Bu bölümde VoIP teknolojisine özel saldırılara ve tehditlerde odaklanılarak, VoIP güvenliğine daha yakın bir bakış sağlanacaktır.

VoIP teknolojisinde güvenli protokoller, destekleyici servisler ve cihazlar kullanılması durumunda bile, her saldırıya karşı korunmak zordur. VoIP mimarisinde güvenlik zaafları oluşabilir ve bu durum tam bir koruma sağlanmasını önler. Alt katmanlarda sağlanacak güvenlik, sistem güvenliği için çok önemlidir. Uygulama katmanında yapılacak analizler ve uygulamalar ise, güvenli bir ağ oluşturmak için daha pratik bir çözümdür. Aşağıda VoIP mimarisinde karşılaşılan saldırıların sınıflandırması mevcuttur.

- Hizmet Karıştırma (Service disruption): VoIP servislerini, yönetimi, erişimi bozmaya yönelik saldırı türüdür. Bu kategoride bulunan saldırılar, routerlar, DNS sunucuları, proxy sunucuları gibi ağ bileşenlerini etkileyebilir. Bu tür saldırılar hedef alınan bileşenlere doğrudan erişim olmadan, uzaktan saldırı gerçekleştirebilir ve yönetebilirler. Saldırgan VoIP telefon gibi bir terminali, bir ağ bileşenini veya bir grubu hedef alabilir. SPIT (Spam Through Internet Telephony) gibi büyük sorun oluşturan saldırılar bu kategoride yer alırlar.
- Telekulak (Eavesdropping, Annoyance): Aktarılan bilgiye erişmek amacıyla yapılan saldırı türüdür. Bu durum kullanıcılar arasında yapılan korumasız sinyalleşmenin ve veri paketlerinin görüntülenmesi anlamına gelmektedir. Trafik analizleri bu kategoride incelenmektedir. Veri paketlerine erişmek, saklamak, analiz etmek mümkündür. Saldırının amacı konuşmadaki sözlü veya yazılı bilgileri elde

etmektir. Bu sayede kart numaraları ve pin numaralarına ulaşılabilir. Bağlantının analizi yapılarak, sistemin zayıf yanları tespit edilir.

- Gizlenme (Masquerading and impersonation): Bir kullanıcı veya sistem bileşeni gibi davranılarak, ağa erişimin sağlandığı saldırı türüdür. Bu şekilde bir başka kullanıcıya, servise veya bileşene erişilmesi amaçlanır. Bu önemli bir saldırı türüdür. Çünkü, çağrı dolandırıcılığı (fraud), yetkisiz sisteme girme (unauthorized access) ve hizmet engelleme (service disruption) saldırıları, bu yöntem kullanılarak gerçekleştirilebilir. Bu saldırının özelliği, sistem bileşenlerinin kimliğini taklit edebilmesidir. Saldırının hedefi bir kullanıcı, aygıt ya da ağ bileşeni olabilir. VoIP bileşenlerine izinsiz erişerek veya uzaktan bağlantı kurarak sinyalleşmeyi veya veri paketlerini kendi isteği doğrultusunda kullanabilir. Örneğin, yetkilendirme için yalnız kullanıcı adının kullanıldığı bir sistemde bilgilere kolaylıkla erişilebilir. Bu uygulama katmanında bir saldırıdır. Aynı zamanda VoIP mimarisinde yer alan, yardımcı protokollere (ARP, IP, DNS) de saldırı düzenlenebilir.
- Yetkisiz Erişim (Unauthorized Access): Bir ağ bileşenine, servise ya da özelliğe, doğru yetkilendirme olmadan erişmektir. Bu saldırı, diğer saldırı türleriyle birlikte gerçekleştirilebilir, diğer saldırılara destek sağlar. Bu saldırı türü, bileşenlerin, kaynakların ve ağ erişiminin kontrolüne imkan tanır. Yanıltma saldırılarından farkı, başka bir kullanıcının ya da bileşenin yerine geçmek zorunda olmamasıdır. Saldırı, sistemin yoğunluğundan, kullanılan ayarlardan, zayıf sinyalleşme güvenliğinden ve ağ erişimindeki zayıflıklardan yararlanılarak gerçekleştirilir. Örneğin, Proxy sunucusu aracılığıyla, yönetici niteliğine sahip bir saldırgan, sistem bilgilerini silerek, VoIP sinyalleşmesini engelleyebilir. Bu durum sunucu ve servisi devre dışı bırakır. Yine bir kullanıcı gatewaye erişerek, zararlı bir yazılım yükleyebilir. Bu yazılımla veri paketlerini kaydedebilir.
- Dolandırıcılık (Fraud): VoIP hizmetini kötüye kullanarak kişisel ya da maddi kazanç sağlamaya yönelik saldırı türüdür. Bu saldırı türü telekom taşıyıcıları ve sağlayıcıları için en tehlikeli saldırılardandır. Bu saldırı türü, sinyalleşme mesajlarının veya VoIP aygıtlarının ayarlarının değiştirilmesiyle gerçekleştirilir. Faturalandırma sistemleri, saldırının hedefleri arasındadır. Bir bağlantıdaki çağrı akışına etki ederek, VoIP uygulamalarında çeşitli dolandırıcılık senaryoları gerçekleştirilebilir. Bunun için daha karmaşık yöntemler kullanmak gerekir. [7]

II.2.1 Hizmet Karıştırma (Service Disruption)

Hizmet karıştırma saldırıları, yönetim, kontrol ve kullanıcı katmanları gibi farklı katmanları hedef alabilir. Hizmet karıştırma saldırıları, VoIP altyapısını ve ilgili hizmetlerini destekleyen bileşenlerin, herhangi birisine karşı yapılabilir. Saldırılar temel VoIP bileşenlerini (Sinyalleşme ve veri aktarını sağlayan gatewayler, mobil servisler), yönetim, yetkilendirme ve diğer hizmetleri sağlayan VoIP servislerini ve yardımcı protokolleri etkileyebilir.

Karıştırma saldırıları, sistemin özelliklerinde ve ağ kapasitesinde değişiklik yapmak için, uygun bir ağ bileşenine yönlendirilebilir. Bu saldırılarda mobil cihazlar, gateway, router gibi ağ bileşenleri, sinyalleşme ve veri gibi servis bileşenleri, yönetim, ücretlendirme gibi işletim sistemi bileşenleri hedeflenmektedir.

Hizmet karıştırma saldırıları, VoIP mimarisini alt katmanlardan itibaren etkiler. VoIP teknolojisi, gerçek zamanlı iletişim gerektirdiğinden, email servislerinden ve web tarayıcılarından farklıdır. VoIP protokollerinde sunucu-istemci modeli kullanıldığından, karıştırma saldırılarını uygulanabilir hale getirmektedir. [7]

II.2.2 Telefon Hizmetlerine Yönelik Saldırılar

Telekomünikasyon hizmetleri, yasal olarak korunmaktadır. Bu yüzden, çeşitli ulusal ve uluslararası yasalar gereği, gizlilik, güvenilirlik, ve erişilebilirlik niteliklerini sağlamalıdır. Gelişen telekomünikasyon hizmetleriyle birlikte, yeni özellikler kullanıma sunulmaktadır. Bu özelliklere bağlı olarak, VoIP hizmetinin engellemesi için yapılan saldırılar da değişiklik göstermektedir. Tehditlere açık bir sistem, gizlilik, güvenilirlik ve erişilebilirlik niteliklerini sağlayamayabilir. Aşağıda VoIP servislerine karşı oluşturulan tehditler görülmektedir.

- Voicemail (Sesli mesaj): Yetkisi olmayan insanların, kişisel seli mesajlara eriştiği saldırı türüdür. Bu seli mesajlar için iyi bir şifre kullanmayan tüm kullanıcıların karşılaşabileceği bir durumdur. Saldırgan genellikle tercih edilen şifreleri kullanarak erişmeyi dener. Saldırganın kullanıcı mesajlarına ulaşması durumunda, mesajların silinmesi, değiştirilmesi ve diğer kullanıcılara mesaj gönderilmesi gibi saldırılarda bulunabilir.
- CALLER ID (Kullanıcı Kimliği): Bir kullanıcının kullanıcı kimliğini taklit ederek, o kullanıcı gibi davranılmasına yönelik saldırı türüdür. Bankalarda kullanılan otomatik yanıt sistemlerinde, telekomünikasyon sağlayıcılarında, sigorta şirketlerinde kullanıcı adı doğrulaması yapılmaktadır. Konuşma sırasında yapılan

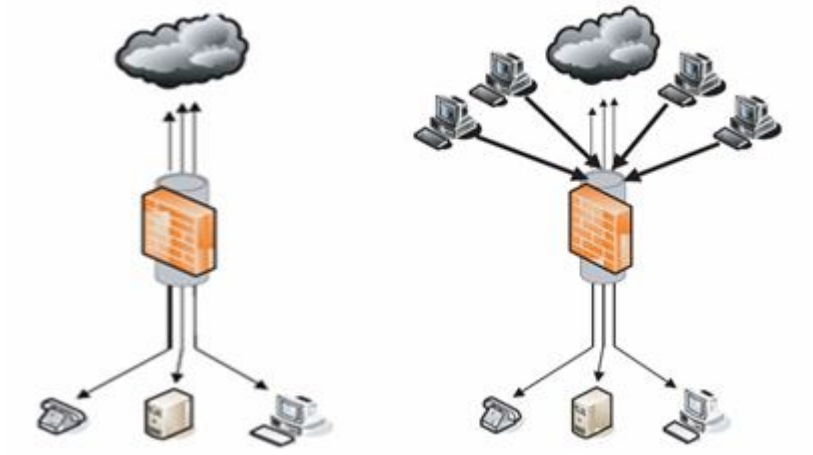
doğrulama, saldırgan için bir fırsat oluşturmaktadır. Bunun dışında sinyalleşme mesajlarına müdahale ederek kullanıcı kimliğine erişmek de mümkündür.

- Call forwarding (Çağrı Yönlendirme): Bir kullanıcıya gelen çağrıların, başka bir kullanıcıya yönlendirilmesidir. Saldırgan kullanıcıların bilgilerine ya da çağrı yönlendirmesine olanak tanıyan VoIP bileşenlerine (SIP Proxy) erişebilirse, çağrının farklı kullanıcılara yönlendirilmesini sağlayabilir. Bu saldırıyla, kötü niyetli bir kullanıcı, telefon aramalarını uluslar arası ya da ücretli (pay per call, 900) numaralara yönlendirebilir. Böylece her arama farklı numaralara yönlendirilecek ve yüksek ücretler ödenmesi gerekecektir.
- Location and presence services (Konum ve Durum Servisi): Bu birim, kullanıcıların bulunduğu konum ve durumları hakkında bilgi verir. Kullanıcılara daha iyi hizmet sağlamak için kullanılır. Kullanıcıların bilgileri, güvenlik kurallarına göre korunmaktadır. Ancak, saldırganlar sunucuya erişerek, birçok saldırı gerçekleştirebilirler. Veri trafiğini izleyebilir ve kullanıcı kimliklerine erişebilirler.
- Confidentiality (Gizlilik): Gizlilik, görüşmelerindeki en önemli niteliklerden biridir. Gizlilik, bir özellikten çok, sağlanmaya çalışılan bir beklentidir. VoIP üzerinden yapılan günlük konuşmalar, önemli bilgiler içermeyebilir. Ancak, bir bankadaki hesap miktarını öğrenmenin, bir avukatla yapılan görüşmenin, bir iş stratejisi hakkındaki konuşmanın, başkalarının bilgisi olmadan gerçekleşmesi istenir. Kullanıcılara karşı yapılan servis karıştırma saldırıları (Service Disruption), taklit etme saldırıları (Masquerading), veri şifrelemesindeki zayıflıklar, gizliliği tehdit eden saldırı türleridir.
- Emergency services (Acil Durum Aramaları): Acil durum servisleri VoIP sağlayıcıları tarafından gerçekleştirilmelidir. VoIP hizmeti veren bileşenlere yapılan saldırı, sistemin cevap verme yeteneğini etkileyebilir. Bu tür durumlarda, saldırıyı algılayacak ve acil durum servisini koruyacak, güvenlik mekanizmaları uygulanmalıdır. Bu mekanizmaların, sistem kullanıcılarını olumsuz yönde etkilememesi gerekmektedir. [7]

II.2.3 Servis Yanıltma (Denial of Service)

Servis yanıltma saldırısı (Denial of Service, DoS), IP temelli ağları hedef alır. DoS saldırıları, sistemin çalışmasına küçük etkiler oluşturabileceği gibi, sistemi tamamen kullanılamaz hale de getirebilir. Saldırılar, IP temelli şebeke hizmetini

etkileyebilir. Bu saldırıların bir türü, farklı harici kaynaklardan çok sayıda veri paketi göndererek, sistemin tüm çağrıları karşılayamaması esasına dayanır. [5]



Şekil II.16 DoS Saldırısı [5]

Şekil II.16'da DoS saldırısına maruz kalan bir sistem görülmektedir. Şeklin ilk bölümünde olağan trafik akışı görülürken, ikinci bölümde ise, saldırganlar tarafından oluşturulan trafiğin kullanıcıları etkilediği görülmektedir.

DoS saldırılarının diğer bir türü, aynı ağ içerisindeki kullanıcıların etkisiz hale getirilmesini amaçlar. Bu saldırı da benzer şekilde çok sayıda paket göndererek, kullanıcıların hizmet almasını zorlaştırır. DoS saldırılarında, servisi etkisiz hale getirmek için bant genişliği ve CPU hedef alınır.

Doğruluk kontrolleri ya da şifreleme yöntemleri bu saldırıların önüne geçemezler. DoS saldırıları, temel olarak ses paketlerinin, hedef alınan kullanıcıya gönderilmesine dayanır. Ses paketlerinin belirli bir kaynaktan gönderilmesi, bilinen bir IP adresine sahip olması ya da şifrelenmiş olması, bu saldırıyı etkileyen faktörlerden değildir.

DoS saldırılarına karşı koymak zordur. Çünkü VoIP, IP ağı üzerinden hizmet veren bir servistir ve IP üzerinden hizmet veren diğer servisler gibi DoS saldırılarından etkilenirler. Ayrıca, DoS saldırıları, özellikle VoIP gibi gerçek zamanlı veri akışının gerçekleştiği servislerde etkili olurlar. Çünkü bu servisler, ağın anlık durumuna karşı daha hassastır. Virüsler ve solucanlar bu kategoride incelenirler ve DoS saldırılarına yol açarlar. Bu zararlı yazılımlar, kendilerini kopyalayarak ve çoğaltarak, sistem trafiğinin artmasına neden olurlar.

Aşağıda DoS saldırılarının türleri görülmektedir. Bu saldırıların bazıları kısmen, bazıları tamamen sistemi hizmet dışı bırakabilir. Arama yapılmasını

engelleyen, sesli mesaj alınmasını önleyen saldırılar olduğu gibi, acil aramalara dahi izin vermeyen DoS saldırıları da mevcuttur.

- **TLS Connection Reset:** TLS genellikle, gateway ve terminaller arasında güvenli sinyalleşmeyi sağlamak için kullanılır. Bir TLS bağlantısını resetlemek zor değildir. Sisteme uygun türde bozucu bir komut (junk packet) gönderilmesi durumunda, TLS bağlantısı resetlenecektir. Bu durum, terminal ve sunucu arasındaki sinyalleşme kanalının bozulmasına neden olur.
- **VoIP Packet Replay Attack:** Veri paketlerinin yeniden gönderilmesidir. Tekrar gönderilen veri paketleri alıcı taraftaki veri sıralamasını etkiler. Bunun sonucunda, seste gecikme olur ve görüşme kalitesi düşer.
- **QoS Modification Attack:** VoIP veri paketleri içinde bulunan kontrol bilgisinin değiştirilmesidir. Bu saldırı türü çoğunlukla IP paketleri içindeki ToS (Terms of Service) bitlerinde değişikler gerçekleştirir. Ses trafiğini ikinci plana atarak, veri trafiğini ön plana çıkarır. Böylece seste gecikmeler olur ve kalite düşer.
- **VoIP Packet Injection:** VoIP paketlerinin taklit edilerek, alıcıya fazla paketler gönderilmesidir. Konuşmaya yeni kelimeler, gürültü, ya da boşluklar eklenir. Yetkilendirme yapılmayan bir sistemde, RTCP paketlerine müdahale edilerek, saldırı gerçekleştirilir.
- **DoS against Supplementary Services:** VoIP hizmetine destek veren protokole (DHCP,DNS) karşı yapılan saldırıdır. Örneğin, DHCP sunucu kullanan terminale yapılan saldırı, adresleme ve yönlendirme işlemlerini olumsuz etkileyecek ve VoIP hizmeti sağlanamayacaktır.
- **Control Packet Flood:** Yetkilendirilmemiş kontrol paketlerini kullanarak, sunucu veya terminallere yapılan saldırı türüdür. Saldırıdaki amaç cihazları, sistemi veya ağ kaynaklarını, servis kullanım dışı kalana dek yormaktır. Saldırı tüm portları hedef alarak, sistemi çağrı işlemleriyle meşgul eder.
- **Bogus Message DoS:** Sunuculara ya da terminallere geçerli ama gerçek olmayan protokol paketleri gönderilerek çağrı sonlandırma ya da meşgul durumuna geçirme işlemleri yapılan, saldırı türüdür. Saldırı terminale sahte bir mesaj göndererek, ya olağan olmayan yollardan çağrının sonlandırılmasına neden olur, ya da kullanılmak istenen hattın meşgul olduğunu belirterek, çağrının yanlış yönlendirilmesini sağlar.

- **Immature Software DoS:** PDA ve taşınabilir telefonlar ve ilk nesil VoIP telefonlarda karşılaşılan saldırı türüdür. Bu cihazlar güvenlik alanında çok gelişmemişlerdir. Kullanılan işletim sistemin zayıflıkları sistemin çalışmasını olumsuz etkiler.
- **Packet of Death DoS:** Sunucu veya terminallere rasgele TCP, UDP paketleri göndererek, işlemcinin, bant genişliğinin ve TCP oturumunun yorulmasını amaçlar. Örneğin, bir saldırgan öncelikli ve büyük boyutlu bir TCP paketini alıcıya gönderir. Alıcının işlem kapasitesini aşan trafik kapasitesi, gecikmelere veya sistemin cevap verememesine neden olur. [5]

II.2.4 SPIT (Spam over Internet Telephony)

Spam, gereksiz verileri ifade etmek için tanımlanan bir terimdir. SPIT ise, kullanıcıya sürekli bu gereksiz bilgilerin yollanması, aranmasıdır. Bu yoğun çağrı talebi, aranan kişi tarafından engellenemez. VoIP sistemlerinde, arayanın tespiti durumunda, engellenmesi mümkün olacaktır. Arayan tespit edilemezse, sistem yoğun bir trafiğe maruz kalır.

SPIT, PSTN'deki istenmeyen bilgilendirme çağrılara denk gelmektedir. Bu aramalar daha öncelikle reklam amacıyla yapılırlar. Ancak, PSTN pahalı bir tercihtir ve yüksek bant genişliği kullanılır. Bu durum PSTN için bir dezavantaj oluşturur. SPIT, daha çok, VoIP sistemlerinde ve e-mail servislerinde karşılaşılan bir problemdir. Ücretsiz ya da düşük maliyetli servisler, bu iletişim yöntemlerini kullanarak, ticari ya da siyasi içerik taşıyan mesajlar gönderirler. Basit bir saldırı, bir yazı hazırlayarak, geniş bir çağrı numarasına ya da IP adresine gönderilmesiyle gerçekleştirilir. E-mail servislerinde, bu soruna bir çözüm bulmak kolaydır. Gelen mesajların belirli konulara ya da kişilere göre engellenmesi mümkündür. E-mail servislerinde kullanılan filtreler, bu mesajların ulaşmasını engeller. SPIT, savunma sistemleri için önemli bir sorun oluşturur, çünkü çağrının ne zaman, kimden geleceği belirlenemez. Bu konuda zararlı kullanıcılar için bir kara liste oluşturmak, VoIP teknolojisinde kullanılan yöntemlerdendir. Bazı sistemlerde, zararlı olabilecek kullanıcılara karşı tedbir almak söz konusu olabilmektedir. Bir başka çözüm yöntemi ise, kullanıcıdan gelecek yanıtlara göre arayanın niyetini belirlemektir. Arayan kişiye basit bir soru sorularak, çağrı buna göre yönlendirilebilmektedir. Örneğin, 'Siyahın karşıtı olan renk nedir?' sorusuna, saldırıda bulunmak isteyen bir makine cevap veremeyecektir. Bu sayede zararlı kullanıcılar önlenmiş olacaktır.

Çağrı önceliğini değiştirmek, SPIT saldırılarından biridir. Bir kullanıcı acil arama ya da öncelikli arama yaptığında, saldırgan arama önceliğini değiştirebilir ve istenilen bir çağrıyı öncelikli hale getirebilir.

VoIP sistemlerinde sinyalleşme mesajlarının taşınmasındaki zayıflıklar, güvenliği tehdit eden saldırılara imkan tanır. Bu saldırılardan birisi, SIPIT (Session Initiation Protocol Interoperability Testing) olarak adlandırılır. Bu saldırı oturum başlatma mesajının, tüm ağa gönderilmesiyle gerçekleştirilir. Bu mesajla birlikte, tüm kullanıcılara ait telefonlar aynı anda çalmaya başlar. Arayan kullanıcı sahte bir kimlik, numara kullandığından, çağrıya cevap veren kullanıcılar bu adrese yönlendirilmiş olacaktır. SIP protokolündeki 'invite' mesajına benzer mesajlar diğer protokollerde de bulunmaktadır. Bu mesajlar yardımıyla bu tür saldırılar diğer protokollere de uygulanabilmektedir.

Benzer bir saldırı türü de, RTP paketlerinin içine bozucu mesajlar ekleyerek, bu paketleri konuşma esnasında karşı tarafa göndermektir. Paketlere eklenen bozucu mesajlar, konuşmada gürültüye sebep olarak kalitenin düşmesine neden olur. Veri paketlerinin sıra numaralarının karıştırılması, farklı kodlamaların gönderilmesi, yanlış adres veya port bilgilerinin belirtilmesi, SPIT saldırılarına diğer örnekler olarak gösterilebilir. [7]

II.2.5 Yetkisiz Erişim (Unauthorized Access)

Yetkisiz erişim, fiziksel ve uygulama katmanlarında güvenlik gerektiren bir saldırı türüdür. Şu üç şekilde gerçekleştirilir:

- Taklit etme
- Ortadaki adam saldırısı (Man in the middle attacks)
- Tam uzlaşı (Total compromise)

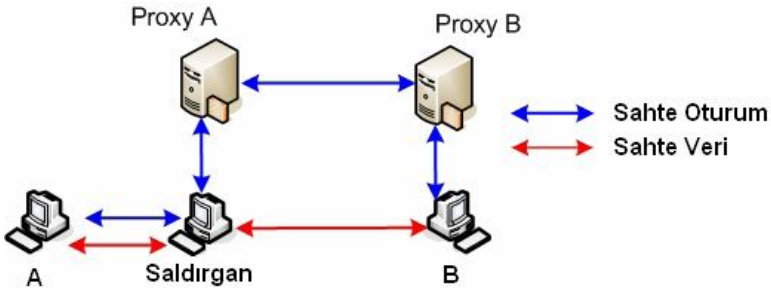
Taklit saldırıları, kullanıcının yetkilendirilmesini sağlayan kullanıcı adı ve şifre bilgilerini ele geçirmesi ile gerçekleştirilir. Bu şekilde saldırgan, kullanıcı gibi davranışlarda bulunabilir. Ortadaki adam saldırısında, sistemde tanımlı kullanıcılar bağlantıyı gerçekleştirir ve görüşmeye başlayabilir. Ancak saldırgan, konuşmayı görüntüleyebilir ve yetkilendirilme gerçekleştirildikten sonra, oturumun yönetimini ele geçirebilir. Toplam uzlaşıda, saldırgan sistemin tüm kontrolünü eline geçirir. Sistemde kullanılan servisleri kullanabilir, komutlar verebilir, kullanıcılara işlemler yaptırabilir. Örneğin, hedef kullanıcının bilgisayarına zararlı bir yazılım (worm, solucan) gönderilebilir. Kullanıcı oturum başlattığı zaman, saldırgan bu yazılım

sayesinde, kullanıcı kimliğini tespit edebilir ve yerine geçebilir. VoIP iletişiminde yetkisiz erişim, aşağıdaki alanlarda gerçekleşebilir:

- VoIP service: Saldırgan, servis sinyalleşmesindeki zayıflıkları kullanarak, VoIP ağına yetkisiz erişim sağlayabilir.
- VoIP altyapısı: VoIP ağ bileşenlerine yetkisiz erişim kazanmak için, sistemdeki zayıflıkları, saldırganın kendi amaçlarına yönelik kullanmasıdır.
- Sinyalleşme ve Veri Transferi Sağlayan VoIP Ağ Bileşenleri: DNS, proxy sunucular, kayıt sunucuları, gateway'ler ve diğer bileşenler
- VoIP terminalleri.
- Yardımcı mimari. (RTP, RTCP, UDP)
- İletim katmanı bileşenleri: router, switch
- Yönetim ve Yetkilendirme Sistemi. Saldırgan yönetim ve yetkilendirme sisteminin arayüzüne erişerek, erişimi kontrol altına alır.

Yetkisiz erişim, bir sistemdeki ya da ağdaki servislere, ağa ya da kontrole erişmek için, sistemdeki zayıflıkların kullanılmasıdır. Bu şekilde çeşitli saldırılar gerçekleştirilebilir. Zayıf güvenlik önlemleri, saldırıların olasılığını ve sisteme etkisini artırır.

Çeşitli bileşenler ve protokoller kullanılarak, gelişmiş bir VoIP yapısı oluşturulur. Ancak bu karmaşık yapısı yetkisiz erişim için saldırı fırsatları doğurabilir. Bu saldırılar, VoIP altyapısında yönetim, yetkilendirme ya da destek sağlayan yazılımlardan herhangi birine karşı gerçekleştirilebilir. Şekil II.17'de bir yetkisiz erişim türü olan, ortadaki adam saldırısı görülmektedir.



Şekil II.17 Ortadaki Adam Saldırısı [4]

Yetkisiz erişim, işletim sistemlerine yönelik bir saldırı türüdür. Ancak, aynı zamanda uygulama katmanında da saldırılar gerçekleştirilebilir. Bir saldırgan, sinyalleşme mesajlarındaki zayıflıklardan yararlanarak VoIP ağına erişebilir. Yetkisiz erişim saldırısı, ağ bileşenlerine, servislere ve uygulamalara erişimi sağlar

ve diğer saldırılara uygun ortam hazırlamak için kullanılır. [7] 2006 yılında yetkisiz erişim saldırısı kullanılarak, faklı VoIP sağlayıcılarının altyapısına erişilmiş ve yönlendirme tablolarında (routing table) değişiklikler yapılmıştır. Bu durum şirketlere 1 milyon dolar maliyet getirmiştir. [8]

II.2.6 Telekulak (Eavesdropping)

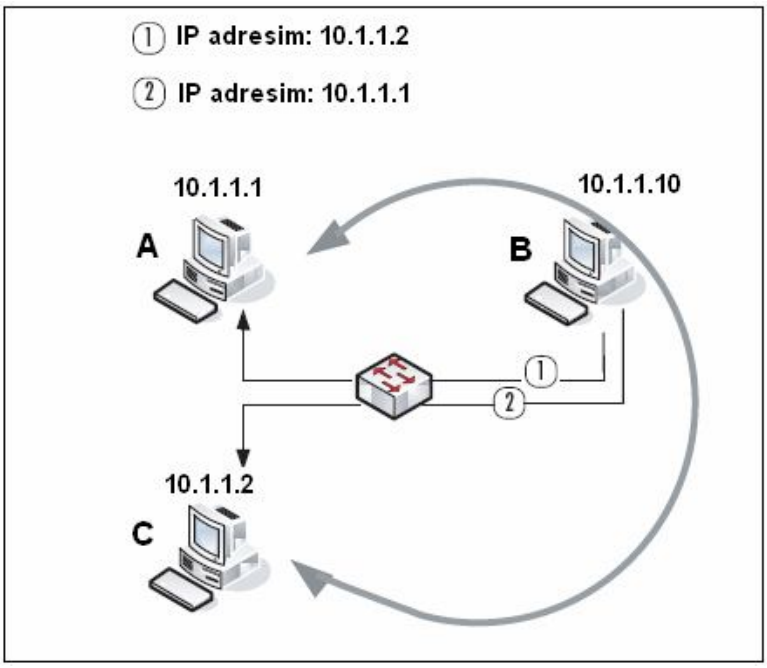
Gizlilik ve güvenilirlik, güvenliğin temel özellikleridir. VoIP uygulamalarındaki güvenliğin yasalarla sağlanmaktadır. Güvenlik için değişmez güvenlik gereksinimleri vardır. Şifreleme, gizlilik ve güvenilirlik için temel bileşenlerden biridir. Kullanılan bazı yöntemler bu güvenliği aşabilmektedirler. Telekulak (Eavesdropping, gizlice dinleme) saldırısı gerçekleştirmek için kullanılan yöntemler şunlardır:

- Trafik analizi (link, network, and transport layers)
- Sinyalleşmeyi Görüntülemek (Signaling Eavesdropping)
- Veri Görüntüleme (Eavesdropping)

Trafik analizi, şifrelemenin yapılmadığı tüm uygulamalarda kullanılabilir. Trafik analizi, kullanıcını görüşme düzeni, davranışları ve alışkanlıkları hakkında bilgi toplanmasını sağlar. Bu durum, hedef profilini algılamada yardımcı olur. Eğer şifreleme için bir ana şifre (Master key) kullanılıyorsa, bu şifre kullanılarak kaydedilmiş bilgiler açılabilir ve gizli bilginin içeriği görüntülenebilir. Bir ağ analiz programıyla VoIP paketleri incelendiğinde, kullanılan protokoller ve bağlantıya bağlı olarak çeşitli teknik veriler elde edilebilir.

İletişimde telekulak, birkaç yöntemle gerçekleştirilebilir. Bir saldırgan, protokollerde ya da VoIP bileşenlerinde kullanılan yazılımlarda bulunan zayıflıklardan faydalanabilir. Saldırgan IP ağa erişerek sinyalleşme ve veri paketlerini görüntüleyebilir ve yakalayabilir. IP ağlara erişimin kolay olması, saldırının gerçekleşmesine kolaylık tanımaktadır. IP ağlarda, tüm verilerin yayınlanmaması, telekulak saldırısına karşı bir önlem olarak düşünülebilir.

ARP bozma (ARP poisoning) saldırısı, ağ trafiğini saldırganın kullandığı sunucuya yönlendirmesini sağlar. Bu şekilde ortadaki adam saldırısı (Man in the middle) gerçekleştirilmiş olur. Bu saldırı ağda buluna sunucular arsında gerçekleştirilir. Ortadaki adam saldırısı sırasında, saldırgan kullanıcılar arsındaki görüşmeyi dinleyebilir. Kullanıcı adı ve şifre gibi, hesap bilgilerine ve veri paketlerine ulaşabilir.



Şekil II.18 Telekulak Saldırısı [5]

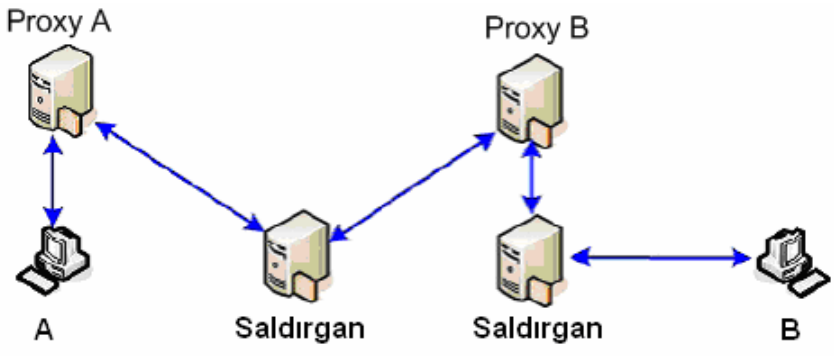
ARP (Adres çözümleme protokolü, address resolution protocol), MAC adresi ve IP adresi arasındaki dönüşümü sağlayan protokoldür. ARP bozma saldırısı, sunuculardaki bulunan ARP tablosundaki, MAC ve IP adreslerinin değiştirilmesi esasına dayanır. Şekil II.17'de A (10.1.1.1) ve C (10.1.1.2) kullanıcıları arsında bir trafik akışı görülmektedir. Saldırgan bir ARP mesajı göndererek, C kullanıcısı için yeni MAC adresinin 00:0B:95:09:68:05 (10.1.1.10) olduğunu bildirir. A kullanıcısı bundan sonraki verileri B kullanıcısı (10.1.1.10) üzerinden, C kullanıcısına (10.1.1.2) yönlendirilecektir. [5,7]

II.2.7 Gizlenme (Masquerading)

Bu saldırı türü gizlenme yöntemine dayanır. VoIP iletişiminde kullanılan protokollerin farklı katmanlarında uygulanabilir. Bir truva atı gibi, sisteme giriş için farklı yöntemler kullanılarak, kimlik gizlenir.

Saldırı yöntemlerinden biri, kullanıcıyı taklit etmek, bir kullanıcıymış gibi davranmaktır. Saldırgan, önceden sağlanan kimlik bilgilerini kullanarak ya da kullanıcı bilgilerini içeren bir bileşene erişerek, kimliği gizler. Bileşen, büyük olasılıkla, saldırganın fiziksel ya da mantıksal kontrolü altındadır. Saldırgan, bileşenin zayıf yönlerini kullanarak, uzaktan yetkisiz erişim sağlayabilir. Saldırganın, gerçek bir kimlik kullanıyor olması, sistemin saldırganı tespitini zorlaştırır.

Bir uygulama ya da servisin davranışını taklit etmek, çeşitli durumların koordinasyonunu gerektirir. Servis durumu, mesaj senkronizasyonu, bileşenler ve terminaller arsındaki olayların kopyalanması gerekmektedir. Uygulama ya da servisin bu özelliklerine bağlı olarak, bir taklit etme saldırısı düzenlenebilir. Genellikle, saldırgan, VoIP sisteminin altyapısını oluşturan bileşenlere ya da uygulamalara erişerek, sinyalleşme protokolündeki yönlendirmeyi etkiler.



Şekil II.19 Taklit Etme Saldırısı [9]

Bir diğer taklit etme saldırısı, aygıt yerine geçmektir (Device Impersonation). Saldırgan, bir telefon, sinyalleşme gateway'i, veri gateway'i, DNS sunucusu, SIP sunucusu olarak sisteme girebilir. Bu cihaz üzerinden saldırıları gerçekleştirir. Saldırının amacı veri akışını ele geçirmek ve kendi isteği doğrultusunda yönlendirmektir. Örneğin, bir saldırgan DNS sunucusu yerine geçerek, gelen çağrıların, kendi hedeflediği sunucuya yönlendirilmesini sağlayabilir. [5,9]

II.2.8 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. Bu denetimler sonucu, bir servis sağlayıcısının yıllık ortalama trafik kaybı %3-8 arasındadır. Ve yine belirlenen 200 çeşit iletişim hırsızlığı türü mevcuttur. Bu saldırı türlerinin daha da artacağı tahmin edilmektedir. [7]

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

- Teknolojinin karmaşık hale gelmesi, kararsızlık ve dikkatsizliği artırmaktadır.
- Yeni teknolojiler, beraberinde güvenlik sınırlılıklarını ve zayıflıklarını getirmektedir.
- Ürünlerin pazarlama dönemlerinde, bazı özellikleri gizli kalmakta ve daha sonra güvenlik yönlerinin geliştirilmesine ihtiyaç duyulmaktadır.

Bir saldırgan, VoIP hizmetlerinin dolandırılması için, geleneksel metotları kullanabilir. Örneğin, Bir kullanıcının kişisel bilgilerine (İsim, adres, sosyal güvenlik numarası) erişerek, iletişim sahtekarlığı gerçekleştirilebilir. Bu bilgilerle bir servis isteğinde bulunulabilir. Böylece, başka bir kullanıcı adına işlem gerçekleştirilmiş olur.

Daha fazla teknik bilgi ve beceri gerektiren saldırılar için, sistemin bir ya da birkaç zayıf noktasından faydalanarak gerçekleştirilir. VoIP altyapısında kullanılan bileşenlerden (SIP Proxy, H323 gateway), güvensiz yazılım uygulamalarından ve protokol sınırlılıklarından kaynaklanan, güvenlik zaafları oluşmaktadır.

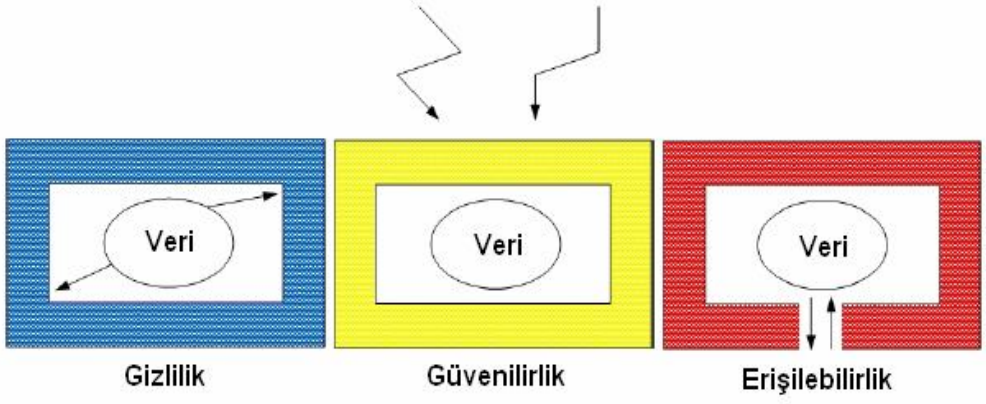
VoIP sağlayıcıları, yeni tip sahtekarlık saldırılarının geleceğini beklemektedirler. Bunların bir kısmı bilinen yöntemler üzerinden gerçekleştirilecektir. Ancak bir kısmı yeni bir yöntem kullanacaktır. Bu saldırılar, yeni bir algılama ve önleme mekanizması gerektirecektir. [7]

II.3 GÜVENLİK ÖNLEMLERİ

VoIP teknolojisi, iletişim sırasında internet altyapısını kullanır. Veriler, IP paketleri olarak terminaller arasında iletilir. Bu nedenle, VoIP güvenliği ile internet güvenliği doğru orantılı olarak etkilenir. Önceki bölümde anlatılan saldırı yöntemlerine karşı geliştirilmiş, birçok güvenlik mekanizması bulunmaktadır. Bu bölümde VoIP güvenliğinde kullanılan güvenlik önlemleri incelenecektir. Bu güvenlik önlemleri, iletim katmanından uygulama katmanına kadar, her katmanda güvenliği sağlamayı amaçlar.

Bir sistemin güvenli olabilmesi için, üç niteliği barındırması gerekir. Bunlar;

- Gizlilik (Confidentially): İletilen veriye yalnız yetkili kullanıcıların erişebilmesi anlamına gelir.
- Güvenilirlik (Integrity): Verinin dış etkenlere karşı korunması, veri bütünlüğünün sağlanması, veriyi yalnız yetkili kullanıcıların değiştirmesi anlamına gelmektedir.
- Erişilebilirlik (Availability): Sistemde tanımlı kullanıcıların, servis isteğinde bulundukları zaman, hizmet alabilmeleri olarak tanımlanmaktadır.



Şekil II.20 Güvenlik Kriterleri [9]

Bir sistemde iletilen verilere, istenmeyen kişiler tarafından erişilmesinin engellenmesi, güvenliğin temellerindendir. Bu amaç için birçok yöntem geliştirilmiştir. Ancak bu yöntemler, sistem kaynaklarına erişimi zorlaştırmamalıdır. Güvenlik önlemleri üst düzeyde olan, ancak hizmet kalitesi düşük bir sistem, güvenlik kriterlerini yerine getirmiş sayılmamaktadır. [9]

VoIP teknolojisinde güvenliği sağlamak için, çeşitli yöntemler geliştirilmiştir. Bu yöntemler farklı katmanlarda görev yapan teknolojilerden oluşmaktadır. VoIP teknolojisindeki güvenlik önlemleri; şifreleme yöntemleri, TLS, IPsec, MIKEY, SRTP, Firewall, VLAN, VPN olarak sıralanabilir.

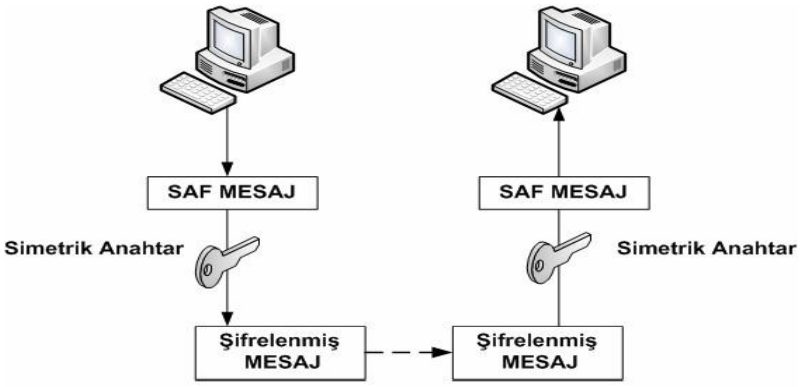
II.3.1 Şifreleme Yöntemleri

Şifreleme, iletilecek veriyi gizleme ve çözme işlemidir. Şifreleme, iletilecek verinin, hedef haricindeki şahısların erişmesini engeller. Şifreleme sistemleri, şifreleme ve şifre çözme olmak üzere iki bölümden oluşur. Gönderilmek istenen orijinal mesaj açık metin (plain text) ve bu mesajın şifrelenmiş hali şifreli metin (ciphered text) olarak adlandırılır. Açık metinden şifreli metine geçme işlemi "şifreleme"; şifreli metinden açık metne geçme işlemi ise "şifre çözme" olarak

adlandırılır. Herkesin ulaşabileceği bir açık metin şifrelenerek, içeriğinin gizlenmesi hedeflenir. Şifreleme teknikleri simetrik ve asimetrik olmak üzere ikiye ayrılır.

II.3.1.1 Simetrik Şifreleme Yöntemleri

Simetrik şifreleme yönteminde, şifreleme ve şifre çözme için tek bir anahtar kullanılır. Bu yöntemde, şifreleme işleminde kullanılan anahtar, yalnız gönderici ve alıcı tarafından bilinir. Bu şifreleme tekniğini kullanan algoritmalara örnek olarak; DES, 3DES, IDEA, RC2, RC4, RC5 ve blowfish algoritmaları verilebilir.



Şekil II.21 Simetrik Şifreleme Yöntemi [10]

- Bilgi Şifreleme Standardı (DES-Data Encryption Standard): DES algoritması en yaygın olarak kullanılan simetrik şifreleme metodudur. DES 64 bit'lik bir blok boyutuna sahiptir. 64 bit'lik düzyazı blokları 56 bit'lik anahtarlar kullanılarak 64 bit'lik şifreli yazı bloklarına çevrilir. Şifreleme işlemi 16 döngü sonucunda gerçekleştirilir. DES orta seviye kaynakları olan saldırganlara karşı sınırlı bir koruma sağlar. 56 bit'lik kısa anahtar boyutuna sahip olması ve teknoloji ve işlem gücündeki gelişmeler nedeniyle DES, güçlü işlemcilerin saldırılarına karşı artık yetersiz kalmaktadır.

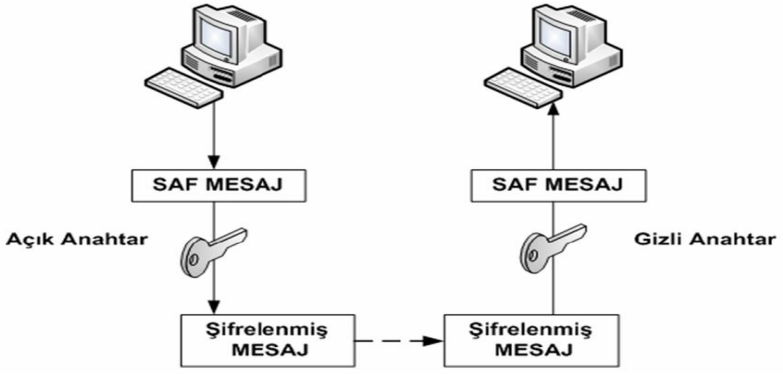
- Gelişmiş Şifreleme Sistemi (AES-Advanced Encryption System): AES, simetrik algoritmalar içerisinde en güçlü algoritmalardan biridir. AES algoritması 128 bit veri bloklarını 128, 192, 256 bit anahtar seçenekleri ile şifreleyen bir algoritmadır. Döngü sayısı anahtar genişliğine göre değişmektedir. 128 bit anahtar için 10 döngüde şifreleme yapılırken 192 ve 256 bit anahtarlar için sırasıyla 12 ve 14 döngüde şifreleme yapılmaktadır.

- 3DES (Triple-DES) Algoritması: DES`in daha çok güvenlik sağlayan bir çeşididir. Bu metot şifreleme anahtarındaki bit'leri 3 katına çıkaran yani, DES`in 3 kez kullanımına dayanan bir metottur.

- Uluslararası Bilgi Şifreleme Algoritması (IDEA-International Data Encryption Algorithm): 64 bit bloklar üzerinde 128 bit anahtar kullanan bir simetrik şifreleme metodudur.
- RC5 (Rone's Code 5) Algoritması: RSA Laboratories tarafından geliştirilen RC5 algoritması değişken-uzunluklu anahtarlar ile çalışır. İhracat kısıtlamaları yüzünden farklı anahtar uzunluklarına ihtiyaç duyan uygulamalar için oldukça uygundur.
- RC2 (Rone's Code 2) Algoritması: RC2, DES`e alternatif bir metot olarak geliştirildi. RC2 için giriş anahtarı 1 ile 1024 bit arası bir uzunlukta olabilir. Şifreleme anahtarı bir bit`den 1024 bit`e kadar değerler alabilir.
- RC4 (Rone's Code 4) Algoritması: RC4 1 ile 2048 bit arası uzunluklarda anahtarları destekler. DES ile karşılaştırıldığında RC4 beş kat daha hızlıdır. RC4`ü çalıştırmada kullanılan kod DES algoritmasının onda biri kadardır.
- Blowfish Algoritması: 32 bit mikro işlemciler ile 1 byte data 18 işlemci döngüsünde şifrelenir. 5 KB'tan daha az bir hafızaya ihtiyaç duyar. Uygulaması kolaydır ve farklı uzunlukta kripto anahtarları seçilerek farklı güvenlik seviyeleri elde edilebilir. [10-13]

II.3.1.2 Asimetrik Şifreleme Yöntemi

Asimetrik şifreleme yönteminde, iki farklı anahtar kullanılmaktadır. Bu sistemde şifreleme işlemi herkes tarafından bilinen açık anahtarla yapılır. Şifre çözme işlemi ise her kullanıcıda bulunan gizli anahtarla yapılır. Böylece, şifreleme ve şifre çözme işlemlerinde farklı anahtarlar kullanılmış olmaktadır. Asimetrik şifreleme algoritmalarına örnek olarak; Diffie-Helman, RSA, gösterilebilir.



Şekil II.22 Asimetrik Şifreleme Yöntemi[10]

- Diffie-Helman: Algoritmanın amacı, iki kullanıcının bir anahtarı güvenli şekilde birbirlerine iletmelerini ve daha sonra bu anahtar yardımı ile şifreli mesajları birbirlerine gönderebilmelerini sağlamaktır. Algoritma anahtar değişimi ile sınırlıdır. Diffie-Hellman takas sistemiyle her iki taraf bazı genel sayısal değerler konusunda anlaşarak bir anahtar oluşturur. Ardından anahtarların matematiksel dönüşümlerini takas ederek oturum anahtarı adı verilen üçüncü bir anahtarı hesaplarlar. Oturum anahtarı her oturum için ayrı ayrı hesaplanmaktadır.
- RSA (Rivest Shamir Adleman): Bu yöntem, iki ayrı anahtar kullanılarak şifreleme yapılması esasına dayanır. Anahtarlardan birisi kamuya açık, birisi de gizlidir. Herkes açık anahtarını yayınlar ve kendisine şifreli bir mesaj göndermek isteyen birisi bu anahtarı kullanarak mesajı şifreler ve gönderir. Gizli anahtar sahibi, mesaja erişerek, şifreyi çözebilir. [10-13]

II.3.2 TLS (Transport Layer Security)

TLS (Transport Layer Security), ulaşım katmanı güvenlik protokolü anlamına gelmektedir. RFC 2246 tarafından tanımlanan bir güvenlik protokolüdür. TLS, web uygulamalarında güvenliği sağlamak için kullanılan SSL 3.0 (Secure Socket Layer version 3.0) protokolüne dayanılarak modellenmiştir. Bu nedenle TLS, SSL 3.0 protokolünün geliştirilmiş bir hali olarak düşünülebilir. Bu protokol bağlantı yönelimli ve güvenilir iletim protokolü gerektirdiğinden dolayı UDP protokolünü kullanan sistemler ile çalışmaz.

Bir VoIP ağında TLS protokolü istemci-sunucu uygulamalarında mesaj gizliliğini, katılımcıların doğrulanmasını ve mesaj bütünlüğünü sağlamaktadır. Genellikle http güvenliği için kullanılmakla birlikte, TLS bağımsız bir protokoldür. TCP gibi bağlantı yönelimli ve güvenilir transmisyon protokolü kullanan farklı uygulamalar için kullanılabilmektedir.

TLS, güvenliği sağlama işini Kayıt Protokolü (Record Protocol) ve El-Sıkışma Protokolü (Handshake Protocol) olmak üzere iki katmanı sayesinde gerçekleştirmektedir El sıkışma protokolü katılımcıların doğruluğunu saptamak amacıyla güvenlik anlaşması sağlarken, kayıt protokolü gizlilik ve veri bütünlüğünü sağlamaktadır. [4,14,15]

II.3.2.1 El Sıkışma Protokolü

TLS iletişiminin ilk fazı el sıkışma işlemiyle yürütülmektedir. El sıkışma protokolünün iki temel görevi vardır.

1. Katılımcıların birbirlerini doğrulamasını sağlamaktadır. Katılımcılar açık anahtar altyapısı (PKI- Public Key Infrastructure) sayesinde birbirlerini doğrulamaktadırlar.

2. Veri iletiminden önce kullanılacak olan şifreleme algoritmaları ve şifrelemeyle ilgili anahtarlar konusunda katılımcıların anlaşmasını sağlamaktadır.

TLS protokolü el sıkışma protokolü sayesinde, şifreleme öncesinde kendi anahtar yönetimini ve doğrulamasını gerçekleştirmektedir. Başarılı bir şifreleme anlaşmasından sonra her iki katılımcı da birbirlerini doğrulamak için hazırlardır. Bu doğrulama mekanizması X.509 sertifikalarının takası temeline dayanmaktadır. Yani açık anahtar altyapısı kullanılmaktadır. TLS'de istemci ve sunucu arasında karşılıklı olarak bir doğrulama mekanizması gerçekleşir.

II.3.2.2 Kayıt Protokolü

Kayıt protokolünün iki temel görevi vardır:

1) Katılımcılar arasındaki verinin, simetrik ya da asimetrik şifreleme metotları ile şifrelenerek gizliliğini sağlamaktadır.

2) Özetleme fonksiyonları sayesinde mesaj bütünlüğünün korunmasını sağlamaktadır. TLS 1.0 ve SSL 3.0 protokollerinin her ikisi de güvenli bir TCP/IP bağlantısı kurmayı ve sürdürmeyi sağlayan güvenlik servislerini uygulamak için şifreleme mekanizmaları kullanmaktadır. Bu güvenli bağlantı sayesinde gizli dinleme, mesaj değiştirme, mesaj sahteciliği gibi saldırılar engellenmektedir.

Şifreleme metotları sayesinde veriler şifrelenerek herhangi bir saldırganın araya girerek mesajları ele geçirmesi engellenir. Saldırgan mesajları ele geçirse bile mesajlar şifrelendiği için hiçbir şey anlamayacaktır.

Tek yönlü özetleme fonksiyonları sayesinde ise mesaj bütünlüğü sağlanmaktadır. Mesaj bütünlüğü, 'Mesaj Doğrulama Kodu (MAC-Message Authentication Code)' adı verilen bir başlık bilgisi sayesinde kontrol edilmektedir. Bu bilgi orijinal mesajla birlikte gönderilmektedir ve alıcının orijinal verinin bütünlüğünün değiştirilmediğini anlamasını sağlamaktadır. Özetleme fonksiyonları mesajın MAC bilgisinin hesaplamasında kullanılmaktadır. Veri gönderilmeden önce özetleme fonksiyonu ile MAC bilgisini oluşturur ve alıcıya ondan sonra iletir.

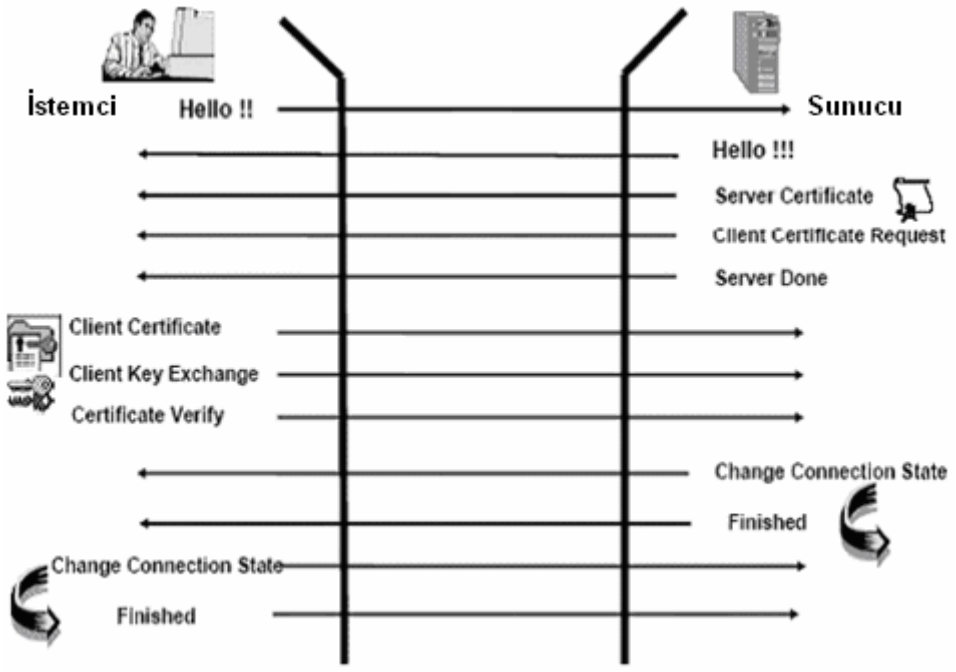
Eğer katılımcılar arasında kullanılacak olan şifreleme mekanizması simetrik bir şifreleme metodu ise bu metodun uygulanabilmesi için paylaşılmış 48 byte'lık ortak bir anahtar (şifre) gerekmektedir. Bu anahtarın üretilmesi için bir rasgele numara üreticisi ve anahtarın güvenli olarak takasını sağlamak için de ön paylaşımlı anahtar anlaşma metodu kullanılmaktadır.

Ancak eğer katılımcılar arasında kullanılacak olan şifreleme mekanizması asimetrik bir şifreleme metodu ise bu durumda katılımcıların her birinde iki ayrı anahtar bulunmaktadır. Anahtarlardan birisi kamuya açık, birisi de gizlidir. Bu açık anahtarın sahibiyle haberleşmek isteyen herkes tarafından görülebilir ve kullanılabilir olması için açık anahtar altyapısı kullanılması gerekmektedir.

TLS protokolünde birçok şifreleme metodu kullanılmaktadır. Gizliliği sağlamak için kullanılan simetrik şifreleme metotları; IDEA, DES, 3DES, AES, asimetrik şifreleme metotları ise; RSA, Diffie Helman (DH) olarak tanımlanabilir.

II.3.2.3 TLS Mesajlaşma Yapısı

Katılımcılar güvenli bir TLS bağlantısı kurmak için karşılıklı olarak birbirlerine belirli mesajlar gönderip alırlar. Bu mesajların gönderimi ve alımı bittikten sonra katılımcılar arasında güvenli bir oturum kurulmuş olur.



Şekil II.23 TLS Protokolü Mesaj Akış Şeması[4]

Client Hello: 'Client Hello' mesajı iki katılımcı arasındaki TLS haberleşmesini başlatır. Bu mesajla istemci sunucuya güvenlik servisleri konusunda anlaşmaya varmak için başvuruda bulunur. Yani, katılımcıların TLS protokolünü konuşabilmeleri için gerekli güvenlik parametrelerinin karşılıklı olarak anlaşmaya varılması için gönderilen ilk mesajdır. Bu güvenlik servislerinin içeriği şu şekildedir:

- Versiyon (Version): İstemcinin desteklediği TLS protokolünün versiyonunu içerir.
- Rasgele Sayı (Random Number): Şifreleme hesaplamasında kullanılan, istemci tarafından rasgele üretilen 32 byte'lık bir numaradır.
- Oturum Kimliği (Session ID): Belirli bir TLS oturumunu ifade etmektedir.
- Şifreleme Grubu (Cipher Suites): İstemcinin desteklediği tüm şifreleme algoritmalarını içermektedir. Bu algoritmalar DES, AES gibi simetrik şifreleme metotları, RSA ya da DH gibi asimetrik şifreleme metotları ya da MD5, SHA gibi özetleme fonksiyonları olabilmektedir.

Server Hello: Sunucu istemciden 'Client Hello' mesajını alır almaz istemciye 'Server Hello' mesajını göndermektedir. Server Hello mesajının içeriği 'Client Hello' mesajının içeriğine benzemektedir. İstemci 'Client Hello' mesajı ile sunucuya desteklediği protokoller ve parametreler konusunda bir öneride bulunur. Sunucu ise istemcinin mesajını inceler ve istemciye gönderdiği 'Server Hello' mesajı ile TLS konuşması sırasında kullanılacak protokoller ve parametreler konusunda son kararını istemciye bildirir.

Server Certificate: 'Server Hello' mesajındaki Şifreleme Grubu alanı içerisinde kullanılacak olan şifreleme algoritmaları belirtilmektedir. Bu mesajla birlikte ise sertifika bilgisi gönderilmektedir. Yani, kullanılacak olan açık anahtar algoritmasına bağlı olarak (RSA ya da DH) kullanılacak olan açık anahtarların alımı ve gönderimiyle ilgili X.509 sertifika bilgileri gönderilir. Bu mesajı alan istemci sertifika bilgisi sayesinde sunucunun açık anahtarını elde eder. İstemci bu anahtarı sunucuya göndereceği mesajları şifrelemede kullanmaktadır. Sunucuda istemciden gelen bu şifreli mesajları kendi özel anahtarı ile çözmektedir. 'Server Certificate' mesajı opsiyonel bir mesajdır. Bu mesaj 'Hello' mesajları neticesinde kullanılacak olan şifreleme metodu eğer asimetrik bir şifreleme metodu ise kullanılmaktadır. Simetrik bir şifreleme metodu tercih edilmesi durumunda, bu mesaj iletilmeyecektir.

Client Certificate Request: Sunucu istemciye kendi sertifika bilgilerini gönderdikten sonra istemciden de kendi sertifika bilgilerini göndermesini istemektedir.

Server Done: Son olarak sunucu istemciye kendisinin anlaşma mesajlarının bittiğini belirtir. Bu mesajla birlikte artık istemci sunucuya kendi bilgilerini göndermeye başlayacaktır.

Client Certificate: Sunucunun sertifika bilgilerini alan istemci, bu sefer kendi sertifika bilgilerini sunucuya göndermektedir.

Client Key Exchange: Bu mesaj istemcinin sunucu ile sertifika bilgilerini takas etmek için kullandığı 'Client Certificate' mesajının yeterli veri içermemesi durumunda istemci tarafından gönderilir. Bazı durumlarda kullanılacak anahtar takas algoritmasına (RSA ya da DH) ilişkin sertifika tipi sunucunun istemcinin açık anahtarını elde etmesinde yeterli bilgiyi içermeyebilmektedir. Bu durumda istemci Client Key Exchange mesajıyla sunucuya daha ayrıntılı bilgi vermektedir.

Certificate Verify: Bu mesaj sertifika bilgisinin kesin olarak doğrulandığı bilgisini vermektedir.

Change Connection State: 'Certificate Verify' mesajı istemci ve sunucu arasındaki müzakerelerin bittiğini göstermektedir. Yani, katılımcılar arasındaki el sıkışma işlemi bitmiştir. Bundan sonrası için artık müzakere edilen protokoller vasıtasıyla güvenlik servislerinin uygulanması için kayıt protokolü devreye girecektir. 'Change Connection State' mesajı güvenlik servislerinin artık işleme alınabileceğini göstermektedir. Yani, artık istemci ve sunucu arasındaki mesajlaşmalar ilgili şifreleme protokolleri kullanılarak gidip gelmeye başlamıştır.

Finished: Katılımcılar arasındaki güvenli TLS oturumunun başarılı bir şekilde kurulduğunu ifade etmektedir. [4,14,15]

II.3.3 IPsec

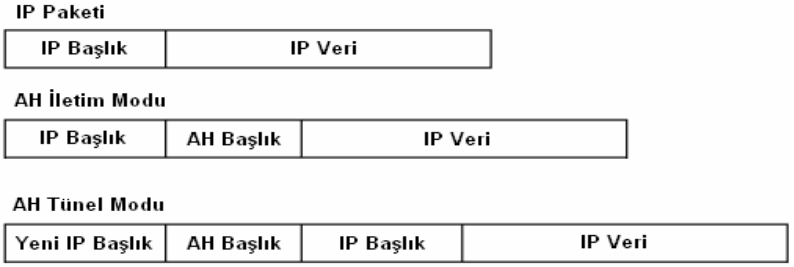
IPsec (Internet Protocol Security) standardı, IP protokolünün ihtiyaç duyduğu güvenlik ihtiyaçlarını karşılamak için geliştirilmiştir. IPsec mimarisi, RFC2401 belgesinde tanımlanmıştır. IPsec, IPv4 ve IPv6'ya uygulanabilir. IPsec protokolü, iletişimin doğruluğunu kanıtlamak, bütünlük ve gizliliğinden emin olmak için kullanılır.

IPsec gerçekleştirmek için iki farklı metot kullanılmaktadır. İletim ve tünel modu veri aktarımının hangi formatta gerçekleşeceğini belirler. İletim metodu

internet güvenliğini sağlamak için kullanıcılar arası (peer to peer) iletişimde kullanılır. IP başlığı değişmediğinden standartları destekleyen herhangi bir donanım veya yazılım ile okunabilir. Tünel modunda ise, IP verisi IPsec protokolünü kullanarak yeni bir IP başlığı tarafından tamamen kapsüllenir. Tünel metodu uzak erişim ve VPN bağlantılarında kullanılır. Paket kapsüle edilerek yeni bir paket oluşturulur ve korunan ağın topolojisi gizlenir. IPsec gerçekleştirmek için iki farklı protokol kullanılır: AH, ESP

II.3.3.1 Authentication Header (AH)

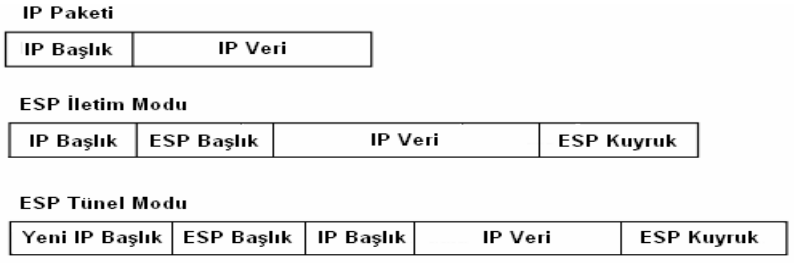
IP doğrulama başlığı anlamına gelen AH protokolü, IP datagramının bütünlüğünü korur. AH iletim metodunda, şifre doğrulama bilgisi IP başlığı (Header) ve veri arasına yerleştirilir. Bu gerekli şifre doğrulama verisini ve güvenli parametre endeksini sağlar.



II.24 AH Paket Yapısı [16]

II.3.3.2 Encapsulating Security Payload (ESP)

ESP protokolü IP kapsülleme anlamına gelmektedir. Bu protokol, hem paketin bütünlüğünü hem de şifreleme kullanarak paketin gizliğini garanti eder. ESP iletim metodunda, ESP bilgisi IP başlığı ile veri arasında yerleştirilir. ESP kuyruğu ve MAC adresi paketin sonuna eklenir. ESP tünel metodunda ise, tüm paket şifrelenir ve yeni bir ESP ve IP başlık oluşturulur, şifreleme bilgisi olarak pakete ilave bir kuyruk eklenir.



II.25 ESP Paket Yapısı [16]

IPsec protokolleri IP datagramlarının gizliliğini korumak için standart simetrik şifreleme algoritmalarını kullanır. Genellikle 3DES, AES ve Blowfish gibi güçlü algoritmalar kullanılmaktadır.

IPsec protokolleri, DoS ataklarına karşı korunmak için kayan pencere yapısı kullanırlar. Buna göre, her paketin ardışık bir numarası vardır ve bir paket sadece numarasının pencerede olması veya daha yeni olması durumunda kabul edilir. Eski paketler devre dışı kalırlar. Böylece saldırganın orjinal paketleri kaydedip daha sonra yanıtlamasıyla yapılan cevaplama saldırılarına karşı koruma sağlanmış olur.

IPsec paketlerini karşılıklı olarak kapsülleyip açabilen eşlerin gizli anahtarı, algoritmaları ve iletişimde izin verilen IP adreslerini saklamak için bir yönteme ihtiyaçları vardır. IP datagramlarının korunması için ihtiyaç duyulan bütün bu parametreler bir güvenlik anlaşmasında (security association) (SA) saklanır. Güvenlik anlaşmaları sırayla güvenlik anlaşmaları veritabanında (SAD) saklanırlar.

Her bir güvenlik anlaşması aşağıdaki parametreleri tanımlar:

- Oluşan IPsec başlığının hedef ve kaynak IP adresleri.
- IPsec protokolü (AH veya ESP)
- IPsec protokolünün kullandığı gizli anahtar ve protokol.
- Güvenlik Parametre Dizini (Security Parameter Index - SPI). Bu güvenlik anlaşmasını belirleyen 32-bit bir sayıdır.

Bazı güvenlik anlaşmalarında farklı parametreler de kullanılmaktadır:

- IPsec modu (tünel veya taşıma)
- Cevap ataklarına karşı koruma sağlayan kayan pencerenin büyüklüğü.
- Güvenlik anlaşmasının geçerlilik süresi.

Güvenlik anlaşması kaynak ve hedef IP adreslerini tanımladığından çift yönlü IPsec iletişiminde sadece bir yöndeki trafikte koruma sağlayabilir. IPsec her iki yönde de koruma sağlamak için iki adet tek yönlü güvenlik anlaşmasına ihtiyaç duyar.

Güvenlik anlaşmaları sadece IPsec'in trafiği nasıl koruyacağını belirlerler. Hangi trafiğin ne zaman korunacağını tanımlamak için ilave bilgiye ihtiyaç duyulur. Bu bilgi güvenlik anlaşması veritabanında bulundurulan güvenlik politikasında (SP) saklanır. IPsec, IPv6 ile zorunlu hale gelecektir. Bu durum internet ve VoIP güvenliğinin artacağı anlamına gelmektedir. [16-18]

II.3.4 MIKEY (Multimedia Internet Keying)

MIKEY, güvenli çoklu ortam oturumlarının kurulmasını sağlayan gereksinimleri karşılamak için tasarlanmış bir protokoldür. Bu protokolün başlıca özellikleri şu şekildedir:

• Güvenlik amaçlı kullanılan parametreler çift yönlü (gidiş-dönüş) olarak değiştirilebilmektedir.

• Basit yapıdadır.

• SDP gibi oturum kurma protokollerinde uygulanabilmektedir.

• Noktadan noktaya güvenliği sağlayabilmektedir (end-to-end security).

• Düşük bant genişliği tüketimi ve düşük iş gücü gereksinimi sağlamaktadır.

MIKEY protokolü, gerçek zamanlı çoklu ortam uygulamaları için geliştirilmiş bir anahtar yönetim protokolüdür. MIKEY özellikle SRTP protokolü ile birlikte kullanılmaktadır. MIKEY protokolünün en önemli özelliklerinden biri SIP protokolünde mesaj bilgilerini içeren SDP (Session Description Protocol) gibi oturum kurma protokolleriyle uyumlu şekilde çalışabilmesidir. MIKEY protokolü sayesinde oluşturulan ve SRTP gibi güvenlik protokollerinde kullanılacak olan anahtara "Trafik Şifreleme Anahtarı (TEK-Traffic Encryption Key)" adı verilmektedir. Katılımcılar arasında kullanılacak olan TEK anahtarlarının üretimini sağlayan anahtara da "TEK Üretim Anahtarı (TGK-TEK Generation Key)" adı verilmektedir. Bu anahtar gerekli olan TEK'lerin üretilmesinde kullanılır. [4,6]

MIKEY protokolünde şu bileşenler bulunmaktadır:

Güvenlik Protokolü (Security Protocol): Gerçek veri trafiğini korumak için kullanılan protokol (ör: SRTP, IPsec).

Veri Güvenlik İlişkisi (Data SA - Data Security Association): Güvenlik protokolü için gerekli olan bilgiyi ifade etmektedir. Birtakım parametreleri ve bir TEK anahtarını içermektedir.

Gizli Oturum (CS - Crypto Session): Çift ya da tek yönlü güvenli veri akışlarını ifade etmektedir. Güvenlik protokolü katılımcıları güvenli bir şekilde haberleştirirken bu oturumları kullanır.

Gizli Oturum Yığını (CSB - Crypto Session Bundle): Bir ya da daha fazla gizli oturumdan oluşmaktadır.

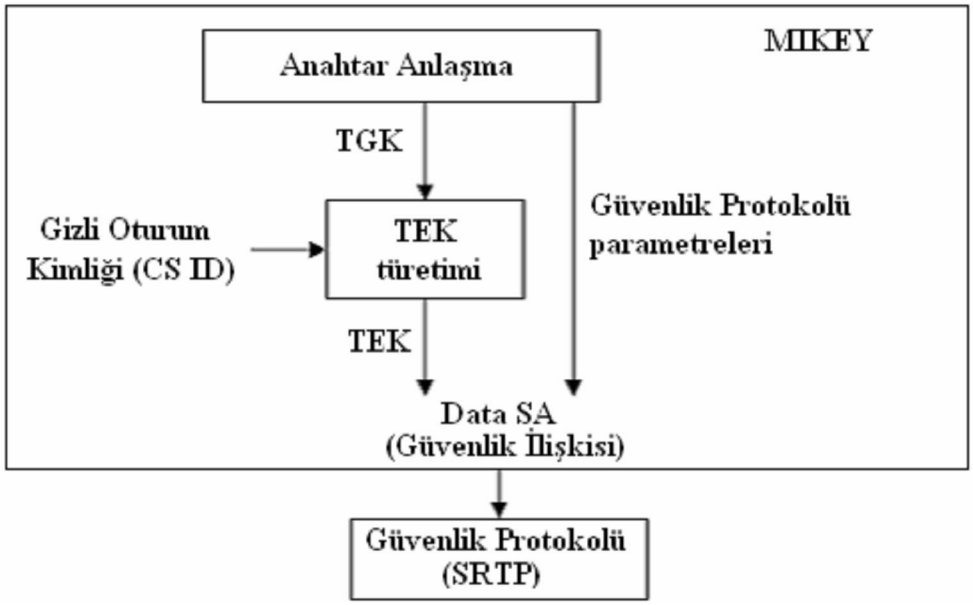
Gizli Oturum Kimliği (CS ID - Crypto Session Identifier): Bir CSB içerisindeki CS'yi tanımlama için kullanılan kimlik bilgisidir.

TEK Üretim Anahtarı (TGK-TEK Generation Key): İki ya da daha fazla katılımcının kendi aralarında anlaşmaya vardıkları bir anahtardır. TEK anahtarlarının üretilmesinde kullanılır.

Trafik Şifreleme Anahtarı (TEK-Traffic Encryption Key): Güvenlik protokolünün gizli oturumları korumak için kullandığı anahtarı ifade etmektedir. Bu anahtar doğrudan güvenlik protokolü tarafından kullanılmaktadır.

MIKEY Protokolü Çalışma Prensibi: Başlangıçta MIKEY protokolü rasgele bir TGK anahtarı üretir. Bu anahtar vasıtasıyla güvenlik protokolünün kullanacağı anahtar olan TEK anahtarı bir gizli oturum ile ilişkilendirilerek oluşturulur. Her bir veri akışı için, farklı bir oturum ve farklı bir TEK anahtarı oluşturulmaktadır. Bu farklı oturumlar birbirinden CS ID ile ayrılmaktadır.

Bir CSB birden fazla gizli oturum içermektedir. Her bir oturum aynı ortak parametreleri içerirken her biri farklı TEK anahtarlarını içermektedirler. Yani, bir SRTP akışının içerdiği parametreler bir önceki SRTP akışının içerdiğiyle aynı olurken içerdikleri TEK anahtarları ve CS 'ler farklı olmaktadır.



Şekil II.26 MIKEY Anahtar Yönetim Protokolü [4]

MIKEY anahtar yönetim protokolü sayesinde SRTP gibi güvenlik protokollerinin katılımcılar arasında güvenli oturumlar kurulmasını sağlayan trafik anahtarları (TEK) üretilir. Anahtar üretim işleminden sonra bu anahtarların katılımcılar arasında güvenli bir şekilde takas edilebilmesi için anahtar takas metotları kullanılmaktadır. [4,6,7]

II.3.5 SRTP (Secure Real Time Protokol)

SRTP, Güvenli Gerçek Zamanlı Taşıma Protokolü olarak tanımlanmaktadır. SRTP protokolü IETF tarafından 2004 yılının Mart ayında yayınlanmıştır. Ses ve görüntü uygulamaları gerçek zamanlı iletilmelidir. Bunun anlamı, verinin iki terminal arasında, en az gecikme ile ve bozulmadan iletilebilmesidir. Böylece alıcı alınan veriden doğru mesajı çıkarabilmeli ve dinamik etkileşimi bozmadan yanıt verebilmelidir.

Gerçek-zamanlı taşıma protokolü (RTP), bir IP ağında UDP portları üzerinden veri taşımak için geliştirilmiştir. RTP protokolü ses ve video gibi gerçek zamanlı verilerin iletimi için kullanılmaktadır. RTP, alıcı tarafta alınan paketleri bir tampon bellekte depolar. RTP içinde bulunan paket numaralarına ve zaman damgalarına göre veri düzenlenerek, iletişim gerçek zamanlı gerçekleştirilmesi amaçlanır. İletim sırasında veri paketlerin 150–200 ms'den fazla beklenmesi, etkileşimli veri (ses veya video) için mümkün değildir. Böyle bir durumda, konuşmanın dinamik etkileşimlilik özelliği kaybolmakta ve sağlıklı iletişim kurulamamaktadır. Bu nedenle gerçek zamanlı bir servis için terminaller arsı gecikme süresi aşılmamalıdır. Bu nedenle, RTP protokolü veri transferi sırasında hata kontrolü, hataların düzeltilmesi, doğrulama gibi yürütülmesi zaman alan güvenlik konularıyla ilgilenmez. SRTP protokolü ise RTP protokolünün güvenli bir profilidir.

SRTP gizlilik, mesaj doğrulama gibi güvenlik işlemlerini sağlamaktadır. SRTP'nin anahtar üretim mekanizması ve şifreleme algoritması içeren bir formatı bulunmaktadır. Anahtar üretim mekanizması MIKEY ana anahtar yapısına ihtiyaç duymaktadır.

SRTP; RTP ve RTCP paketleri için şifreleme ve mesaj doğrulama işlemlerini gerçekleştiren bir yapıya sahiptir. SRTP belirli bir RTP yığın uygulamasından ve belirli bir anahtar yönetim standardından bağımsızdır. MIKEY, SRTP ile birlikte çalışması için tasarlanan özel bir protokoldür. RTP protokolünün güvenlik eksikleri düşünüldüğünde SRTP'nin birçok önemli özelliği ve avantajı bulunmaktadır. Bunlardan bazıları şu şekildedir: [4]

- RTP ve RTCP paketlerinin şifrelemesini gerçekleştirerek gizlilik sağlamaktadır.
- Tüm RTP ve RTCP paketlerinin bütünlüğünü sağlayarak alıcı tarafa sorunsuz olarak iletilmesini garanti altına almaktadır.

- Oturum anahtarlarını belirli periyotlarda yenileyerek şifrelenmiş verilere gerçekleştirilebilecek saldırılara karşı büyük bir savunma sağlamaktadır.
- Yeni şifreleme algoritmalarını benimseyebilecek güncellenebilir bir yapıya sahiptir.
- Her iki terminalde de rasgele oturum anahtar üretim fonksiyonunu gerçekleştiren güvenli bir yapısı bulunmaktadır. Bu rasgele oluşturulan anahtarlar ön hesaplama ataklarına karşı bir koruma sağlamaktadır.
- Önceden tanımlanmış algoritmalar sayesinde düşük bir maliyet gerektirmektedir.
- Düşük bant genişliklerinde bile yüksek veri oranı sağlamaktadır.
- Anahtarlama bilgisi ve doğrulama işlemleri için gerekli olan veri belleği az yer kaplamaktadır.
- SRTP protokolü RTP protokolünün bir profili olarak tanımlanmıştır. Bu nedenle var olan RTP yığınları içerisine kolaylıkla entegre edilebilmektedir.
- SRTP, oturum katmanında şifreleme sağlamaktadır. Yani, SRTP protokolü RTP tarafından kullanılan önde gelen katmanlardan olan ulaşım, ağ ve fiziksel katmanlardan bağımsızdır.
- SRTP, anahtar yönetiminin sebep olduğu yükü hafifletmektedir. Çünkü gizlilik, bütünlüğü sağlama gibi anahtarlama işlevlerini tek bir ana anahtar hem SRTP akışları hem de buna ilişkin SRTCP akışları için gerçekleştirmektedir. Özel durumlarda tek bir ana anahtar, birden fazla SRTP akışını koruyabilmektedir.

Bir RTP profili olarak tanımlanmasından dolayı SRTP, mevcut çoklu ortam standartları ile kullanılabilmektedir. H.323 protokolü için SRTP desteği H.235 ile tanımlanmıştır. SIP protokolü için ise SRTP için gerekli anahtar yönetim mekanizmalarının desteklenmesi için Oturum Tanımlama Protokolü (SDP-Session Description Protocol) geliştirmeleri tanımlanmıştır. Böylece, SRTP ve MIKEY birlikte kullanılarak, H.323 ve SIP gibi farklı çoklu ortam standartları arasında uçtan uca şifreleme sağlamaktadır.

Şekil II.27 SRTP Paket Yapısı [4]

SRTP güvenli olmayan RTP paketlerini güvenli hale getiren bir RTP profili ve uzantısıdır. SRTP paket yapısı sabit RTP paketini (RTP Payload) belli bir şifreleme

metodu kullanarak şifreler ve RTP paketi alıcıya şifrelenmiş olarak gönderilir. SRTP, RTP paketinin şifrelenmesinde Gelişmiş Şifreleme Sistemini (AES-Advanced Encryption System) kullanmaktadır.

Bununla birlikte SRTP protokolü, Ana Anahtar Kimliği (MKI-Master Key Identifier) ve Mesaj Doğrulama Etiketi (Authentication Tag) adı verilen iki alanı daha içermektedir. Opsiyonel olan ana anahtar kimliği alıcı tarafa hangi anahtarın kullanılacağını belirtirken; kullanılması tavsiye edilen doğrulama etiketi ise mesaj doğrulama verisini taşımak için kullanılmaktadır.

Doğrulama etiketi sabit RTP Başlık (RTP Header) bilgisiyle şifrelenmiş RTP Paketinin (RTP Verisi) toplam boyutunu içermektedir. Alıcı taraf paketi aldıktan sonra doğrulama etiketinde yazan değer ile kendisine ulaşan RTP Başlık bilgisiyle şifrelenmiş RTP Paketinin toplam boyutunu karşılaştırır ve paketin doğru bir paket olup olmadığı bilgisine ulaşır.

SRTP protokolü anahtar takası için Çoklu Ortam Internet Anahtarlama (MIKEY- Multimedia Internet KEYing) protokolünü kullanmaktadır. MIKEY anahtarların ve güvenlik parametrelerinin takası için kullanılmaktadır. SRTP'de MIKEY protokolü gizlilik ve veri bütünlüğü gibi güvenlik işlevlerini gerçekleştirmek için tek bir "Ana Anahtar (Master Key)" kullanmaktadır. Bu ana anahtarla ilgili bilgi Ana Anahtar Kimliği (MKI-Master Key Identifier) alanı tarafından tanımlanmaktadır. [4,6,7]

II.3.6 Firewall

Güvenlik duvarı (Firewall), yerel ağlar üzerindeki kaynakları diğer ağlar üzerinden gelecek saldırılara karsı koruyan, iç ve dış ağlar arası ağ trafiğini tanımlanan kurallara göre denetleyen bir ağ geçidi çözümüdür. Güvenlik duvarları ağın içinden veya dışından gelen yetkisiz erişimleri engelleyen, süzen ve izin denetimi sağlayan yazılımlar veya donanımlardır. Kullanıcılarına internet erişim hakkı vermiş olan bir kurum, yerel ağındaki kaynakları korumak ve dış ağlardaki kaynaklara kullanıcılarının erişim hakkını belirlemek için yazılım veya donanım tabanlı güvenlik duvarları kullanırlar.

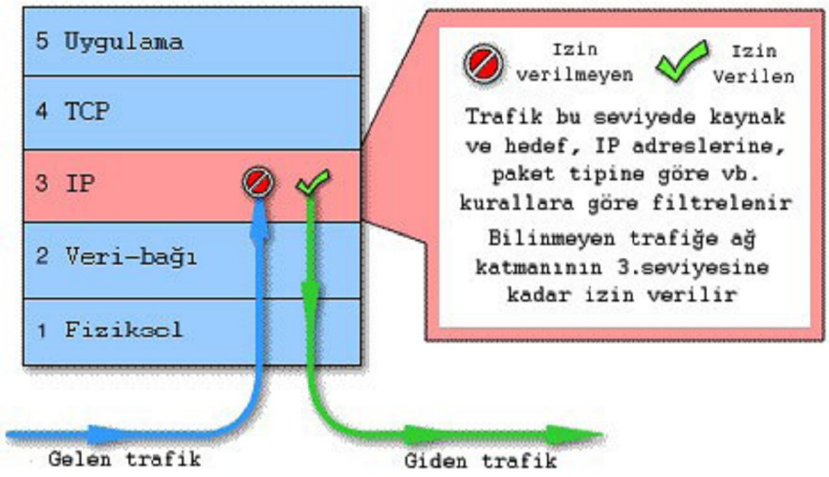
Temel olarak bir firewall, network üzerinde kendisine gelen paketleri, tanımlanan kurallar doğrultusunda geçirip geçirmeyeceğine karar verir. Güvenlik duvarları, genel olarak ağdaki diğer makinelerden farklı bir makinenin üstüne

kurulurlar. Bunun sebebi, dışarıdan gelen isteklerin direkt olarak yerel ağ kaynaklarına ulaşmasını engellemektir.

Güvenlik duvarlarının birçok denetleme metodu vardır. En basit perdeleme metotlarından biri, daha önceden belirlenmiş alanlardan ve IP adreslerinden gelen paketleri kabul edip diğer istekleri reddetmektir. Mobil kullanıcılar, güvenlik duvarları aracılığı uzaktan erişim hizmetini kullanabilirler. Bunu için özel ağlara güvenli bağlanma prosedürleri ve tanılama metotları kullanılır. Güvenlik duvarları mimarilerine göre; statik paket filtrelemeli, dinamik paket filtrelemeli ve Proxy destekli olmak üzere üç kısımda incelenirler. [4-6,19]

II.3.6.1 Statik Paket Filtrelemeli Firewall

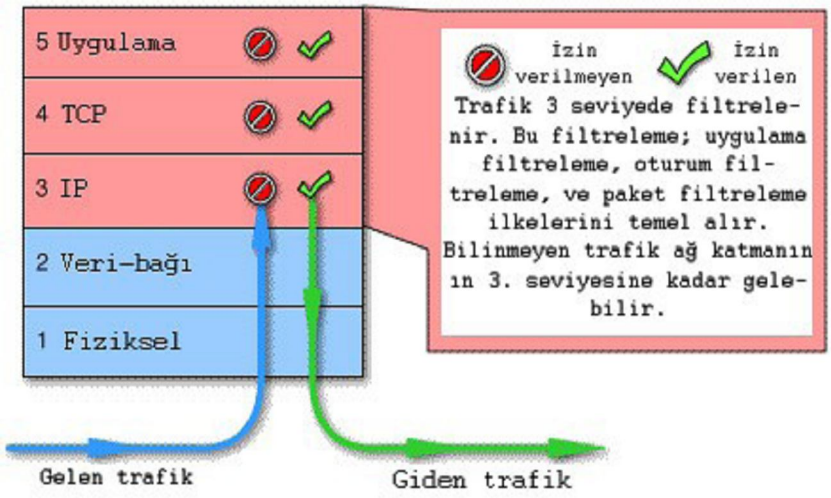
Bu mimari eskimiş olmasına rağmen halen bazı sistemlerde kullanılmaktadır. Bu güvenlik duvarları, trafikte akan verinin başlık kısmına bakar ve bu kısımdaki bilgileri okuyarak analiz eder. Bu bilgiler; kaynak adresi, hedef adresi, paketin erişmek istediği port, kullanacağı protokol gibi verileri içerir. Elde edilen sonuca ve önceden tanımlanmış yetkilere göre paketin geçişine izin verir ya da paketi engeller. Bu mimarinin en büyük dezavantajı paketi ilk gönderen sistemin yani paketin oturumunu açan sistemin bazen tespit edilemiyor olmasıdır. Bu tür güvenlik duvarları, ağ katmanında çalışırlar.



II.28 Statik Paket Filtrelemeli Firewall [19]

II.3.6.2 Dinamik Paket Filtrelemeli Firewall

Bu mimari statik paket filtre güvenlik duvarlarının yetersiz kalması üzerine tasarlanmıştır. Durum denetimi için paketler ağ katmanında yüksek performans açısından statik paket filtre güvenlik duvarlarında olduğu gibi filtrelenir. Daha sonra verinin geldiği bütün katmanlara erişilir ve bu katmanlar yüksek güvenliği sağlamak için denetlenir. Yani veri kaynaktan hedefe kadar takip edilir. Güvenlik duvarları, sadece paketin başlığını incelemekle kalmaz aynı zamanda paketin içeriğini de kontrol ederek, paket hakkında daha fazla bilgi elde eder. Ek güvenlik önlemi olarak bu güvenlik duvarları, bütün portları kapalı tutar ve bu durum port taramalarının önüne geçer. Sadece port için bir istek geldiği zaman, tanımlanmış kurallara uygun bir istek olması koşuluyla portu açar. Bu mimari günümüzde yaygın olarak kullanılmaktadır.

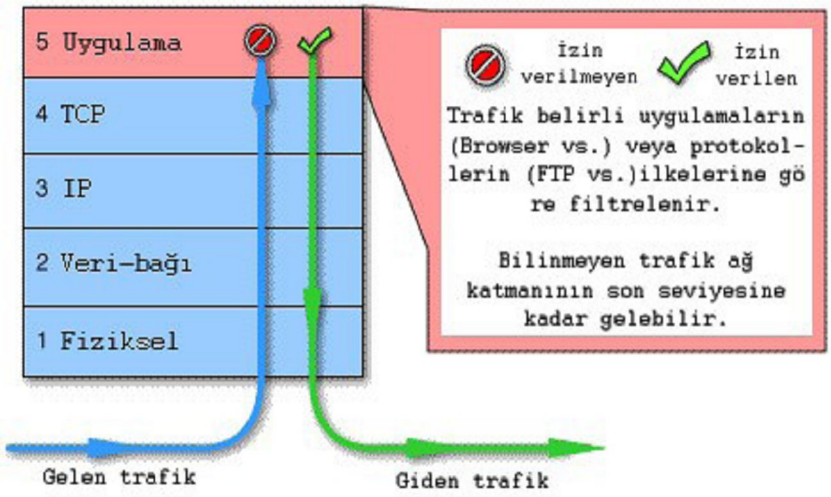


II.29 Dinamik Paket Filtrelemeli Firewall [19]

II.3.6.3 Proxy Destekli Firewall

Bu güvenlik duvarları uygulama seviyesinde çalışırlar. Proxy destekli güvenlik duvarlarının özelliği oturumu kendisinin başlatmasıdır. Yani kaynak oturum açmak istediğinde, bu isteğini güvenlik duvarına gönderir. Güvenlik duvarları da isteği hedefe iletir. Oturum açıldıktan sonra da işleyiş aynen devam eder. Proxy destekli güvenlik duvarları hedef ile kaynak arasında yalıtım görevi görür. Bu güvenlik duvarlarının paket içeriğini kontrol edebilmeleri en büyük avantajlarıdır. Bu tür güvenlik duvarları, dinamik paket filtrelemeli güvenlik duvarları gibi oturumu takip etmezler. Çünkü oturumu zaten kendileri başlatırlar. Hedef ile kaynak arasına girdiği

ve paketleri kendisi ilettiği için özellikle veri trafiğinin yoğun olduğu alanlarda performans kayıplarına neden olmaktadır.



II.30 Proxy Destekli Firewall [19]

II.3.7 VLAN

VLAN (Virtual Local Area Network), sanal yerel ağ anlamına gelmektedir. IEEE tarafından geliştirilmiştir. VLAN teknolojisi kullanılarak, bu teknolojiyi destekleyen cihazlar üzerinde mantıksal ağlar oluşturulur.

Sanal yerel alan ağı (VLAN), bir yerel alan ağı (LAN) üzerindeki ağ kullanıcılarının ve kaynakların mantıksal olarak gruplandırılması ve switch (Anahtarlama cihazları) üzerinde portlara atanmasıyla oluşturulur. Sanal ağ kullanılmasıyla, her sanal ağ sadece kendisine ait yayınları (broadcast) alabilir. Bu sayede yayın trafiği azaltılarak bant genişliği artırılmış olur. VLAN tanımlamaları, bulunulan yere, bölüme, kişilere ya da hatta kullanılan uygulamaya ya da protokole göre tanımlanabilir.

VLAN tanımlaması gerçekleştirilirken, kullanılan hatlara özel tanımlamalar mevcuttur. Sanal ağlarda kullanılan hatlar terminallere veri iletimi sağlayan, access link (Erişim hatları) ve tüm sanal ağlara hizmet verebilen trunk link (Ana hatlar) olmak üzere iki kısma ayrılır.

Erişim hatları; sadece bir sanal ağa ait olan bağlantıdır. Erişim hattı üzerine bağlanan cihaz, sanal ağlar arası ilişkilerden, fiziksel ağdan bağımsız olarak bir yayın grubuna bağlı olarak çalışır. Anahtarlama cihazları, erişim hatlarına bağlı cihaza göndermeden önce paket üzerindeki VLAN başlığını kaldırır. Erişim hatları üzerindeki cihazların gönderdiği paketler, bir router (Yönlendirici) yönlendirilmediği sürece kendi sanal ağları dışındaki cihazlarla konuşamazlar. Ana hatlar, üzerinde

birden çok sanal ağ taşıyabilirler. Ana hatlar, bir anahtarlama cihazından başka bir anahtarlama cihazına, bir yönlendiriciye ya da bir sunucuya yapılabilir.

Sanal ağlar sistem üzerinde uygulanarak, anahtarlama cihazlarından kaynaklanan birçok problem ortadan kaldırılır. Bunları temel olarak üç başlık altında toplanabilir. [20]

II.3.7.1 Broadcast Kontrol

Broadcast her protokol tarafından üretilir. Ancak yoğunluğu protokole, uygulamaya ve servisin kullanımına göre değişir. Sanal ağ uygulanmamış anahtarlama cihazlarında, gelen yayın paketi terminallerin ihtiyacına bakılmaksızın, her porta gönderilir. Ağ üzerindeki cihaz sayısının fazla olması demek, yayının katlanarak artmasına ve bu paketlerin ağ üzerindeki her cihaza gönderilmesine neden olur.

İyi tasarlanmış bir ağ, ölçütlere göre bölümlere ayrılmalıdır. Bunu yapmanın en uygun yolu anahtarlama (Switching) ve yönlendirmeden (Routing) geçer. Bu durum sanal ağlar arasındaki yayın trafiğini engeller.

II.3.7.2 Güvenlik

VLAN oluşturulmamış bir ağın dezavantajlarından biri güvenliktir. Switch kullanılmayan bir ağ üzerinde, iki kullanıcı arasındaki veri akışı, ağa bağlı tüm cihazlara da iletilmektedir (collision). Bu durum, trafik sorununa yol açtığı gibi, ağ üzerinden geçen tüm paketleri dinleyen ve veri paketlerini çözebilen yazılımlar ve donanımlar sebebiyle güvensizdir. Dağıtım cihazı olarak switch kullanıldığında her portun kendi yayın bölümüne ayrılması ile portlar arasındaki bu güvenlik açığı engellenebilmektedir. Ancak sanal ağ kullanılmayan switch topolojisinde yayının tüm portlara gönderiliyor olması, ağ üzerindeki tüm cihazların birbirinin yayınladığı trafiği aldığı anlamına gelmektedir. Bu ağ üzerinde diğerleri ile ağ ilişkisi olmayacak kullanıcı gruplarına, diğer cihazlarca erişim sağlanmakta, yayın paketleri gönderilmektedir. Switch üzerindeki terminaller sanal ağlara ayrıldığında bu tür güvenlik açıkları ortadan kalkacaktır. Bu sayede bir kullanıcının ağ üzerinde herhangi bir uca bağlanarak tüm ağı dinleme ve bilgiyi ele geçirme durumu ortadan kalkacaktır. Ancak bağlanacağı sanal ağ üzerinde işlem yapabilecektir.

II.3.7.3 Esneklik

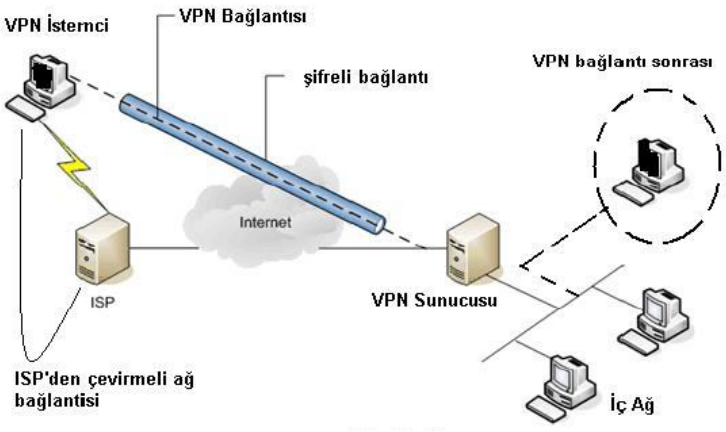
Sanal ağlar ile oluşturulmuş bir ağ, üzerinde yayın grupları oluşturulmuş bir çok ağ anlamına gelmektedir. Kullanıcıların fiziksel konumu önemli olmaksızın, istenilen sanal ağa atama gerçekleştirilebilir. Aynı şekilde zaman içerisinde büyüyen bir VLAN, yeni oluşturulan sanal ağlara aktarılabilir. Bu işlem switch üzerinde yapılacak yeni bir port tanımlamasıyla mümkün olmaktadır. Aynı işlem VLAN desteğini kullanmadan yapılmak istendiğinde merkezi yönlendirici ile yeni oluşturulacak alt ağlar arasında fiziksel bağlantı sağlanmalıdır.

II.3.8 VPN

VPN, (Virtual Private Network), sanal özel ağ anlamına gelmektedir. VPN ile internet gibi halka açık ağlar üzerinden güvenli bir şekilde kullanıcıların kendi kurum kaynaklarına erişmeleri sağlanmaktadır.

VPN ile üç farklı güvenlik tekniği sağlanır. Kimlik sorgulaması (Authentication), sadece yetkili kullanıcıların VPN hizmetini alabilmesini sağlarken, şifreleme (encryption), iletişimin yabancı kullanıcılar tarafından dinlemesini, veri bütünlüğü (data integrity) ise, kötü niyetli kullanıcıların iletilen paketlerin içeriğini değiştirmesini engeller. Kiralık hat, Frame Relay, ISDN gibi teknolojiler kullanılarak çeşitli birimler, özel bir hat vasıtasıyla birbirine bağlanabilirler. Bu şekilde verilerin çalınması veya değiştirilmesi mümkün olmamaktadır. Ancak internet üzerinden verilerin taşınması söz konusu olduğunda verilerin güvenlik amacıyla şifrelenmesi gerekmektedir. VPN teknolojileri buna imkan tanır. VPN kullanılmasının temel nedeni, düşük maliyeti ve kolay yapılandırılabilmesidir

VPN sayesinde şirketlerin ofislerini birbirine ya da mobil kullanıcılarını merkeze bağlamak için kendi ağ omurgalarını kurmasına gerek kalmaz. VPN ile her birim, diğer birimlerle arasındaki bağlantıyı internet üzerinden kesintisiz ve yüksek hızla gerçekleştirir. VPN, birimlerin internet omurgasını kendi omurgaları gibi kullanmalarına imkân vermektedir.

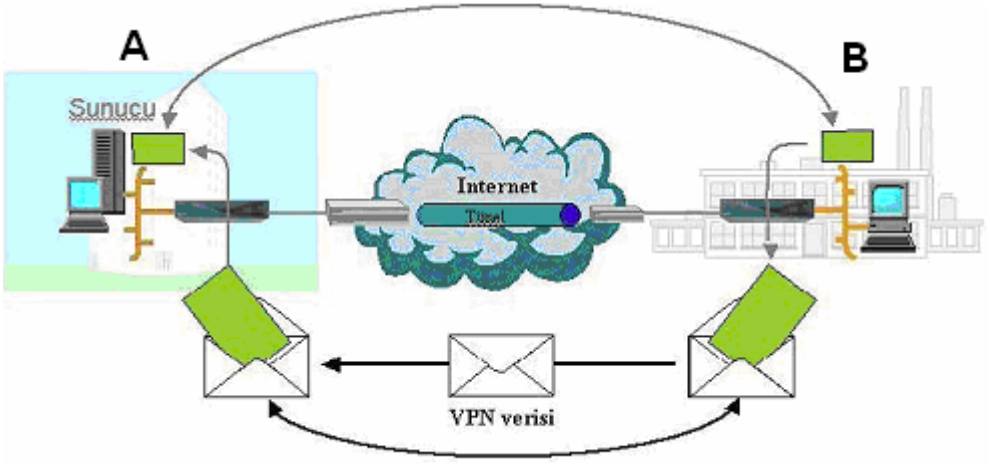


II.31 VPN Yapısı [21]

II.3.8.1 VPN Tünel Mimarisi

VPN'de iki bilgisayar arasındaki iletişim VPN tünelleriyle gerçekleşir. Tünel oluşturma, iletim sırasında veri bütünlüğünün ve gizliliğinin korunması için paketleri diğer paketlerin içine kapsülleme işlemidir. Tünellemenin, şifreleme, kimlik sorgulama, paket iletme ve özel IP adresini gizleme gibi görevleri vardır. Tünel, iki bilgisayar arasındaki özel bir bağlantı gibi görev yapmaktadır. Bu bağlantı her kullanıcının erişebileceği internet üzerinden gerçekleştirilir ancak iletilen verilere, yalnız gerekli yetkiye sahip olanlar erişebilir.

VPN iletişiminde veri kapsüllenerek VPN tüneli üzerinden gönderilir. Şekil II.32'de görülen B kullanıcısında bulunan veri şifrelenir, sonra VPN üzerinden gönderilmek üzere kapsüllenir. Bu kapsülleme sırasında, mesaj bir "zarf" içine yerleştirilir ve A kullanıcısına internet üzerinden gönderilir. A kullanıcısı veriyi kapsülden çıkarır, şifre çözme işleminin ardından, veriye ulaşır.



Şekil II.32 VPN Veri Kapsülleme [21]

II.3.8.2 VPN Tünel Protokolleri

VPN tüneller kurulumunda iki protokol kullanılmaktadır. Bu protokoller şifreleme sistemlerine göre, değişiklik gösterirler.

- PPTP (Point to Point Tunnelling Protocol): IETF tarafından geliştirilmiştir. PPTP, IP tabanlı veri ağları boyunca VPN bağlantısı oluşturarak, uzaktaki bir bilgisayardan özel bir sunucuya güvenli veri aktarımı yapılmasını sağlar. PPTP, kimlik sorgulaması ve kriptolama servislerini sağlar. Bu protokolün şifreleme sistemi zayıftır.

- L2TP (Layer 2 Tunnelling Protocol): PPTP'den sonra geliştirilmiştir ve aynı görevi görür. L2TP, IPSec tabanlı doğrulama/onaylama ve kriptolamayı desteklemesi nedeniyle PPTP'nin bir adım ötesine geçer. IPSec'in sağladığı temel özellik ve üstünlükler şunlardır:

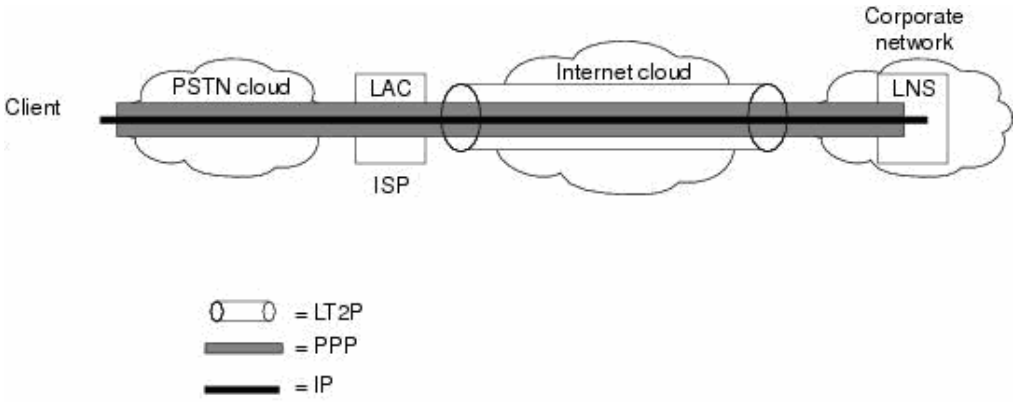
· IETF tarafından geliştirilmiştir.

· PPTP'den daha güçlü bir şifreleme ve doğrulama sağlar.

· Büyük ağlar için, PPTP'den daha iyi ölçeklenmektedir.

· VPN üreticilerince kullanılmaktadır.

VPN protokollerinin yapısı Şekil II.32'de görülmektedir.



Şekil II.33 Tünel Protokolleri Yapısı [21]

II.3.8.3 VPN Güvenliği

VPN güvenliği altı altı adımda sağlanmaktadır.

- Yetkilendirme (Authorization): VPN bağlantıları, terminallerin yetkili olduğu durumda gerçekleştirilir. VPN bağlantılarının yetkilendirilmesi, kullanıcı hesabındaki bağlantı özellikleri ve uzaktan erişim talimatları ile kesinleştirilir. Eğer kullanıcı veya router bağlantı için yetkili değilse değilse, VPN server bunları devre dışı bırakır.

- Kimlik Sorgulama (Authentication): Güvenlik için önemli bir yöntemdir. İki adımda gerçekleştirilir.

a) Makine Tabanlı Kimlik Sorgulama (Machine-level authentication): Bu özellik, IPSec protokolü kullanıldığı zaman görev yapar. Birimler arasındaki IPsec yarlarının kontrolünü sağlar.

b) Kullanıcı Tabanlı Kimlik Sorgulama (User-level authentication): Veri, PPTP veya L2TP tüneline gönderilmeden önce, kullanıcı kimliğini doğrulamak zorundadır. Bu da PPP kimlik doğrulama metodu kullanılarak yapılmaktadır.

- Şifreleme (Data Encryption): Bu yöntem, şifrelenmiş verinin iletileceği VPN bağlantı türünü oluşturur. VPN bağlantıları için uç birimler arası güvenlik garanti edilemez. Bağlantı istemci ve VPN server arasında sağlanır. Kullanıcılar arası güvenli bağlantı oluşturmak için, VPN bağlantısı kurulurken IPsec protokolü kullanılmalıdır.
- Paket Filtreleme (Packet Filtering): VPN sunucunun güvenliğini artırmak için paket filtreleme yöntemi kullanılır. VPN sunucunun arayüzüne filtreler yerleştirilerek güvenliğin artırılması amaçlanır.
- Güvenlik Duvarı (Firewall): Özel ağ ve internet arasında güçlü bir duvar oluşturur. Hangi türde paketlerin geçtiğine, hangi protokollerin izinli olduğuna ve açık portların sayısına göre firewall ayarlanabilir.
- IPSec (Internet Protocol Security): En iyi şifreleme algoritmaları ve çok kapsamlı kimlik sorgulama gibi güvenlik özelliklerini geliştirmeyi sağlar. Bu protokolün avantajlarından sadece IPSec uyumlu sistemler yararlanabilir. Bütün cihazlar ortak bir anahtar kullanmalı ve ağlardaki firewall'lar benzer güvenlik ilkelerine sahip olmalıdır. [21-23]

II.4 VoIP GÜVENLİĞİ ALANINDA YAPILAN ÇALIŞMALAR

VoIP güvenliği hakkında yapılmış birçok akademik çalışma mevcuttur. Bu çalışmalar çoğunlukla, tehditlerin tanımlanması, güvenlik önlemlerinin belirlenmesi ve bu güvenlik önlemlerinin tespitine yönelik testlerden oluşmaktadır. [24-37] VoIP teknolojisi, yaygın olarak kullanılan, sürekli gelişen ve yaygınlaşan bir teknoloji olduğu için, VoIP hizmeti veren birçok servis sağlayıcısı da bu konuda çalışmalar yapmaktadırlar. VoIP güvenliği tez çalışmalarına konu olmuştur. [4,9,29,38]

VoIP güvenliğine tehdit oluşturan durumlar, en çok araştırılan konuların başında gelmektedir. [24-28] Güvenlik saldırılarına önlemler alabilmek için, öncelikle bu tehditlerin tanımlanması gerekmektedir. VoIP mimarisinden, kullanılan protokollerden, sinyalleşme zayıflıklarından, bileşenlerin yönlendirme ve sonlandırma problemlerinden kaynaklanan güvenlik açıkları, çalışmaların temelini oluşturmaktadır. Tespit edilen güvenlik tehditlerinin sınıflandırması bir başka önemli konudur. Güvenlik tehditlerinin doğru tespit edilebilmesi ve iyi bir sınıflandırma, güvenlik tehditlerine karşı etkili önlemler almakta önemli bir adım oluşturmaktadır.

Güvenlik tehditlerinin tespitinden sonra, bunlara karşı getirilen çözüm önerileri bir diğer araştırma konusudur. [3,25-33] Bu konudaki çalışmalar, protokol güvenliği, iletim hattı güvenliği, güvenlik protokolleri alanlarında yoğunlaşmıştır. VoIP güvenliğini sağlamak için kullanılan yöntemler tespit edilmiş ve güvenilirliği değerlendirilmiştir. Akademik çalışmalar haricinde çeşitli VoIP sağlayıcıları da bu konuda çalışmalar yapmıştır. [32-37]

VoIP güvenliği ile ilgili gerçekleştirilen akademik çalışmalarda, testler ve simülasyonlar gerçekleştirilmiştir. Testler ve simülasyonlar için güvenlik araçları ve simülasyon programları kullanılmıştır. Güvenlik açıklarının tespiti için wireshark, cain&abel, protos, sivus, sipscan, nessus gibi programlar kullanılmıştır. Bu programlardan bir kısmı, sistem sinyallerini bozmaya yönelik olup, bir kısmı güvenlik açıklarını tespit etmekte kullanılır. Bu şekilde güvenlik testleri gerçekleştirilerek, VoIP güvenliği hakkında değerlendirmeler yapılmıştır. [26,27,32] Bazı çalışmalarda, sistem simülasyonları gerçekleştirilmiştir. Bu çalışmalarda, opnet, omnet, asterisk, snort programları kullanılmıştır. Bu programlardan asterisk bir açık kodlu santral olarak kullanılmaktadır. Opnet, ise bir simülasyon programı olup, akademik çalışmalarda çokça tercih edilen ve üniversiteler tarafından kullanılan bir programdır. [38-51]

VoIP güvenliği ile ilgili birçok kitap yayınlanmıştır. [1,5-7,48,49] Birçok internet sitesinde, VoIP güvenliği ile ilgili bilgiler yer almakta, test amaçlı güvenlik araçları bulunmaktadır. [50,51] Servis sağlayıcıları, VoIP hizmeti sağlayan ürünler üretmekte ve bu ürünlerde güvenlik önlemlerini artırmaktadır. Servis sağlayıcıları, araştırmacılar işbirliği gerçekleştirerek, VoIP güvenliğini sağlamaya yönelik çalışmalar, projeler gerçekleştirmektedirler. [52] Tüm bu çalışmalarla birlikte, VoIP güvenliğini artırıcı önlemler geliştirilmekte, ancak buna karşın yeni tehditler ortaya çıkmaktadır.

BÖLÜM III

ÇALIŞMALAR

Bu tez çalışmasında opnet programı kullanılarak güvenlik simülasyonları gerçekleştirilmiş ve 'Avaya IP Office 406' santrali kullanılarak gerçek ortamda, VoIP saldırıları düzenlenmiştir. Elde edilen sonuçlar analiz edilmiş ve güvenli bir VoIP sistemi oluşturulabilmesi için gerekli kriterler ortaya konmuştur.

III.1 Opnet Simülasyonları

Opnet, IT teknolojilerini modelleme yoluyla analiz eden bir simülasyon programıdır. Opnet, ağ teknolojileri, uygulamalar, çeşitli bileşenlerle oluşturulmuş bir sanal ortamdır. Dünya üzerinde binlerce ticari ve ulusal kuruluş ve beş yüzü aşkın üniversite opnet yazılımını kullanmaktadır. [53] Türkiye'de Boğaziçi Üniversitesi Netlab Laboratuarı, Anadolu Üniversitesi Elektrik Elektronik Mühendisliği Bilgisayar Laboratuarı, Sabancı Üniversitesi ve Sakarya Üniversitesi Teknik Eğitim Fakültesi'nde kullanılmaktadır. [54-56] Opnet programı kullanılarak birçok akademik çalışma gerçekleştirilmiştir. Bilimsel makalelerde ve tez çalışmalarında sıkça kullanılmaktadır.

Opnet, istenilen boyuttaki alanlarda simülasyon yapmaya olanak sağlar. Opnet ile ofis boyutunda bir proje oluşturmak mümkün olduğu gibi, kıtalararası bir proje gerçekleştirmek de mümkündür. Ayrıca projenin simülasyon süresi, birkaç saniye ile birkaç hafta arası değiştirilebilir. Bu durum, opnet programının gerçeğe uygun simülasyonlar gerçekleştirdiğinin bir göstergesidir.

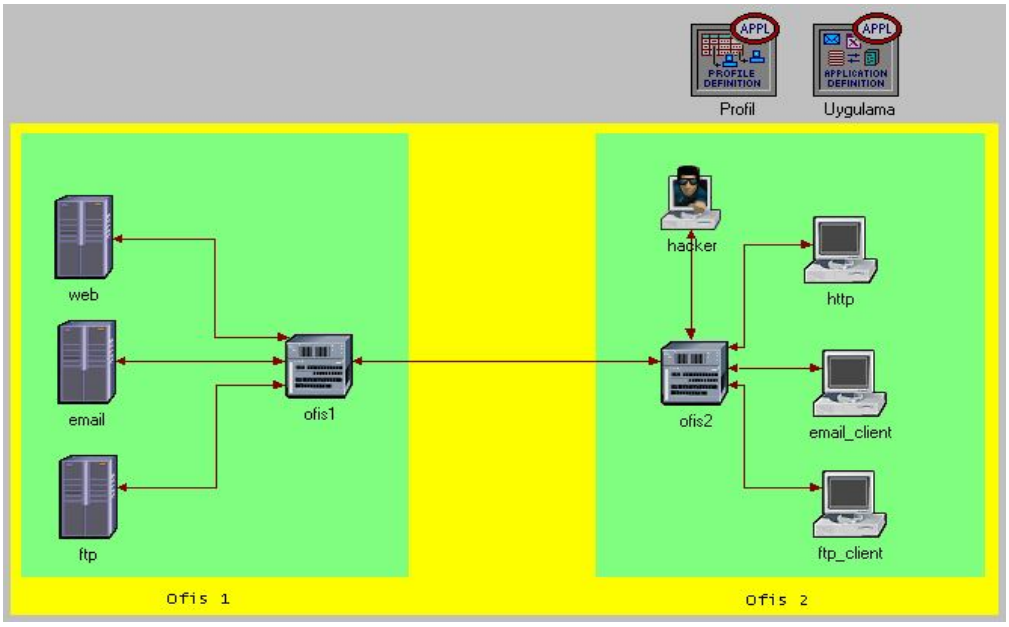
III.1 Opnet İşlem Akışı

Opnet, belirlenen boyutlarda projeler tanımlamaya ve bu projeler içinde senaryolar oluşturulması esasına dayanır. Her proje, alt senaryolara ayrılarak, farklı koşullardaki sistem performansları, elde edilen veriler, güvenlik kriterleri gibi birçok veri elde edilebilir. Proje tanımlamasında kullanılacak uygulamalar ve profiller tasarımcı tarafından belirlenir. Simülasyon sonucunda elde edilecek veriler seçilerek, simülasyon gerçekleştirilir. Sonuçlar grafik olarak görüntülenir.

Opnet programı kullanılarak, birçok akademik çalışma yapılmıştır. Özellikle yurtdışı birçok makale yayınında opnet simülasyonları kullanılmıştır. Bunun yanında birçok tez çalışması opnet temeline dayandırılarak gerçekleştirilmiştir. [38-46]

III.1.1 DoS Saldırısı

DoS saldırısı, kullanıcının hattını meşgul edecek çok sayıda sinyal gönderilmesi esasına dayanır. Bu sinyaller bir http sunucu için sayfaya bağlanma isteği, ftp sunucu için download isteği, email sunucu için mesaj gönderme isteği, bir voip sistemi için çağrı isteği olabilir. Şekil III.2'deki senaryoda, sunucuların bulunduğu bir ofis ile kullanıcıların bulunduğu diğer bir ofisin, switchler aracılığıyla haberleştiği bir sistem görülmektedir. Bu saldırıda hacker sisteme bir kullanıcı gibi bağlanır ve sistem kaynaklarını kullanır. Böylece, sistem kaynaklarının kullanım oranı (utilization) artar. Bunun sonucunda diğer kullanıcıların sistemden yararlanma hızları düşer. Hacker tarafından gönderilen sinyallerin artması durumunda, sistem kapasitesi aşılarak, kullanıcıların hizmet alması engellenmiş olur.



Şekil III.2 DoS Saldırısı Senaryosu

III.1.1.1 Sistem Tasarımı

Bu projede, iki farklı senaryo kurgulanmıştır. Birinci senaryoda; 'web', 'email' ve 'ftp' olmak üzere üç sunucunun bulunduğu bir ofis ile, 'http', 'email_client', ve 'ftp_client' adlı kullanıcıların bulunduğu başka bir ofis arasındaki trafik incelenmiştir. Bu senaryoda bulunan sunucular ve kullanıcılar isimlerinde belirtilen uygulamaları desteklemektedirler. Her kullanıcı aynı zamanda, kendi aralarında sesli görüşme yapabilecekleri bir voip uygulamasını desteklemektedir.

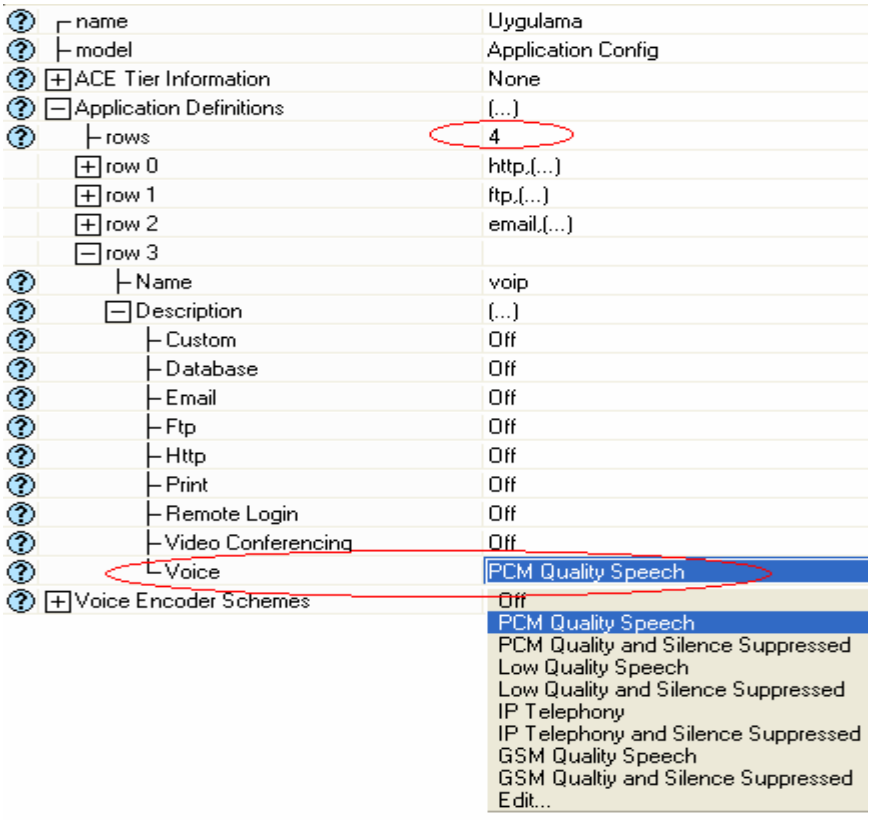
İkinci senaryoda ise, ilk senaryodan farklı olarak, kullanıcıların bulunduğu ofise bir hacker bağlanmıştır. Bu hacker, tüm sunucuların hizmetlerinden faydalanmakta ve tüm kullanıcılarla sesli görüşme yapabilmektedir. Bu sayede, hacker sistem kaynaklarını kullanacak ve diğer kullanıcıların hizmet almalarını etkileyecektir.

Sistem tasarımında; 2 adet ethernet16_switch, 3 adet ethernet_server, 3 adet ethernet workstation ve bileşenler arası bağlantıyı sağlamak için 10BaseT_LAN bağlantı kablosu kullanılmıştır. Bu hat 10Mb veri hızını desteklemektedir. Bu kısımda sistem ayarları için 'Application Config' ve 'Profile Config' bileşenleri de seçilmiştir. Bu bileşenler kullanılarak sistem tasarımı gerçekleştirilmiştir. Bu aşamadan sonra yapılacak işlem, sistemde gerçekleştirilecek uygulamaların tanımlanması ve hangi bileşenlerin hangi uygulamalar için kullanılacağının belirlenmesidir.

III.1.1.2 Sistem Ayarları

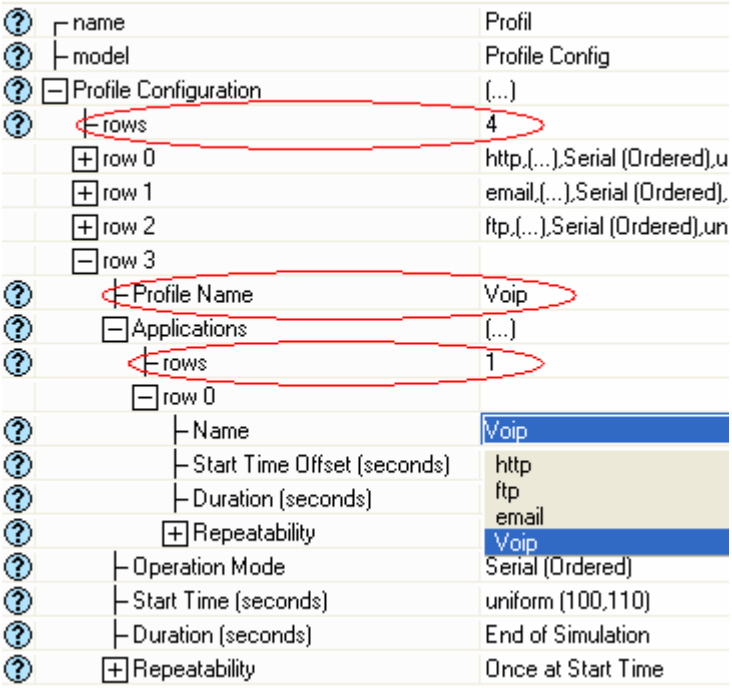
Bu sistemde üç farklı sunucu ve üç farklı kullanıcı olacaktır. Bunların dışında sisteme dışarıdan dahil olan bir hacker mevcuttur. Kullanılan sunucular ftp, http ve email sunucular olacaktır. Her bir kullanıcı bu hizmetlerden yalnız birine erişebilecek, hacker ise, tüm hizmetlerden faydalanabilecektir. Bu özelliklere göre uygulama ve profil ayarları tanımlanmalıdır.

Sistemde kullanılacak uygulamalar 'Application Config' simgesi kullanılarak belirlenmiştir. Bu projede ftp, http, email ve voice olmak üzere dört uygulama gerçekleştirilmiştir. Şekil III.3'de uygulama ayarları görülmektedir. Uygulamamızda; http için 'Heavy Browsing', ftp için 'High Load', email için 'High Load' ve voip için 'PCM Quality Speech' özellikleri seçilmiştir.



Şekil III.3 DoS Saldırısı Uygulama Ayarları

'Profile Config', bileşenlerin hangi uygulamayı destekleyeceklerinin belirlendiği kısımdır. Bu sistem için, http, ftp, email ve voip olmak üzere dört profil tanımlanmıştır. Her profil yalnız, adında belirtilen uygulamayı destekleyecek şekilde profil tanımlamaları gerçekleştirilmiştir. Tanımlamalar Şekil III.4'te görülmektedir.



Şekil III.4 DoS Saldırısı Profil Ayarları

III.1.1.3 Bileşen Ayarları

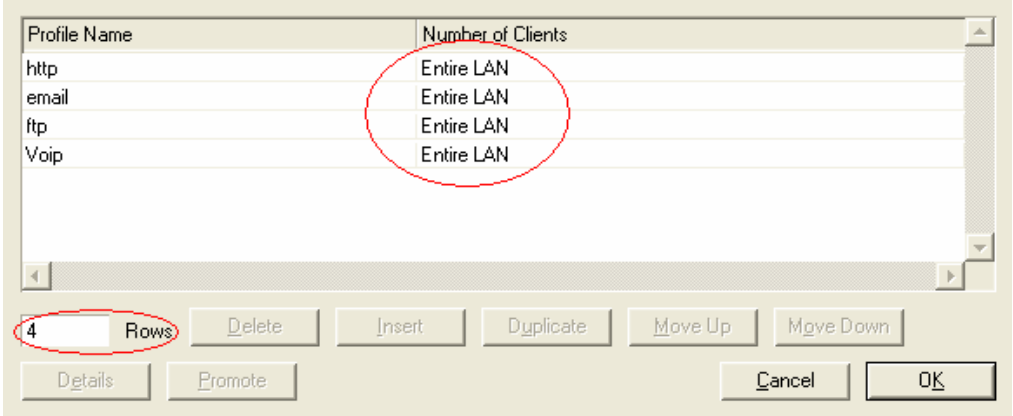
Senaryodaki uygulama ve profil tanımlamalarını tamamladıktan sonra, bileşen tanımlarını gerçekleştirmek gerekir. Bu işlem, her bileşenin hangi görevi yapacağını belirlemek anlamına gelir. Senaryoda tanımlanacak bileşenler sunucu ve kullanıcılar olmak üzere iki kısımda incelenebilir.

- Sunucu Ayarları: Senaryoda web sunucu için http, ftp sunucu için ftp, email sunucu için email uygulamaları tanımlanmıştır. Bu tanımlamalar bileşen özelliklerine girilerek gerçekleştirilmiştir.
- Kullanıcı (Workstation) Ayarları: Kullanıcı ayarları için, profil tanımlamaları kullanılır. Kullanıcıların özelliklerine girilerek; her kullanıcı, isminde belirtilen profilde tanımlanmıştır.

Ses ve görüntü uygulamaları için, diğer uygulamalardan farklı bir durum söz konusudur. Bu uygulamalarda, haberleşme kullanıcılar arasında gerçekleşmekte ve bir sunucuya ihtiyaç olmamaktadır. Bu nedenle uygulama tanımlamaları kullanıcılar üzerinde yapılır. Bu senaryo için, her kullanıcı; hem voip sunucu, hem de voip istemci olarak görev yapacak şekilde tasarlanmıştır. Bu işlem kullanıcıların profil özelliklerine voip eklenmiş ve uygulama özellikleri voip olarak seçilmiştir.

Bu işlemlerin ardından ilk senaryo tamamlanmıştır. Ardından senaryo kopyalanmış ve ikinci senaryo oluşturulmuştur. Bu senaryodaki tek fark sisteme bir hacker bağlanmış olmasıdır.

Sistem tasarlanırken birçok bilgisayardan oluşan bir ağ hacker olarak tasarlanmıştır. Hacker birçok bilgisayardan oluşan bir ağ olarak tasarlandığı için, ağdaki bilgisayar sayısı değiştirilebilir. Biz projemizdeki hacker kullanıcı sayısını '20' olarak belirledik. Şekil III.5'de görüldüğü gibi, hacker için dört profil de tanımlanmıştır. Bu sayede, hacker tüm sistem kaynaklarına erişebilecektir.

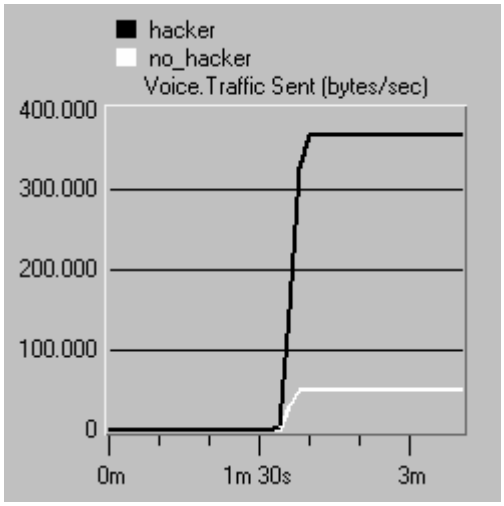


Şekil III.5 Hacker Profili

III.1.1.4 Simülasyon ve Analiz

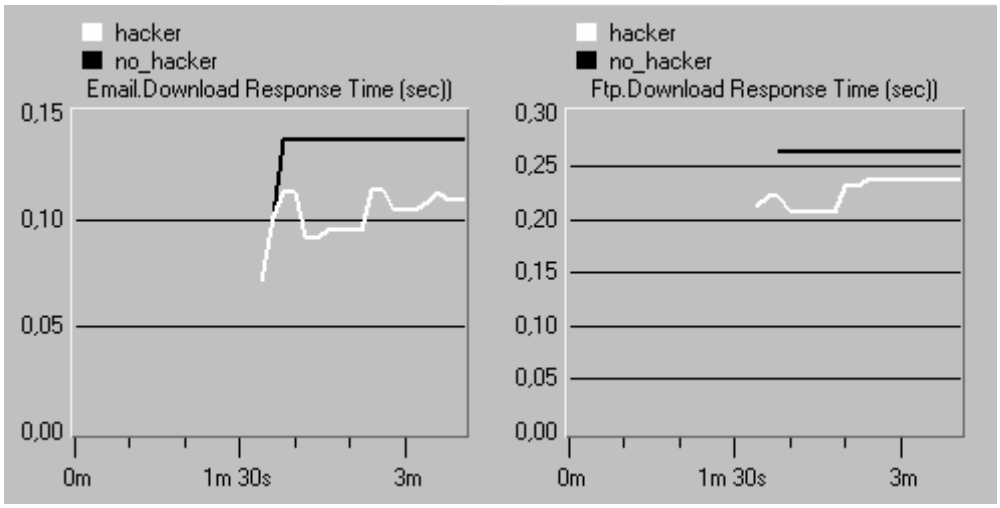
Simülasyon işlemine başlamadan önce hangi verilerin elde edilmek istendiği belirtilmelidir. Bunun için 'simulation' menüsünden hangi istenilen veriler seçilir. Projemizde email, ftp, http, voice, IP, CPU, UDP verileri incelenmiştir. İstenilen veriler seçildikten sonra simülasyon süresi bir saat ayarlanarak, simülasyon işlemine başlanmıştır.

Simülasyon işlemi tamamlandıktan sonra elde edilen veriler görüntülenir. Aşağıdaki şekillerde, projede bulunan iki senaryodan elde edilen veriler analiz edilmiştir.



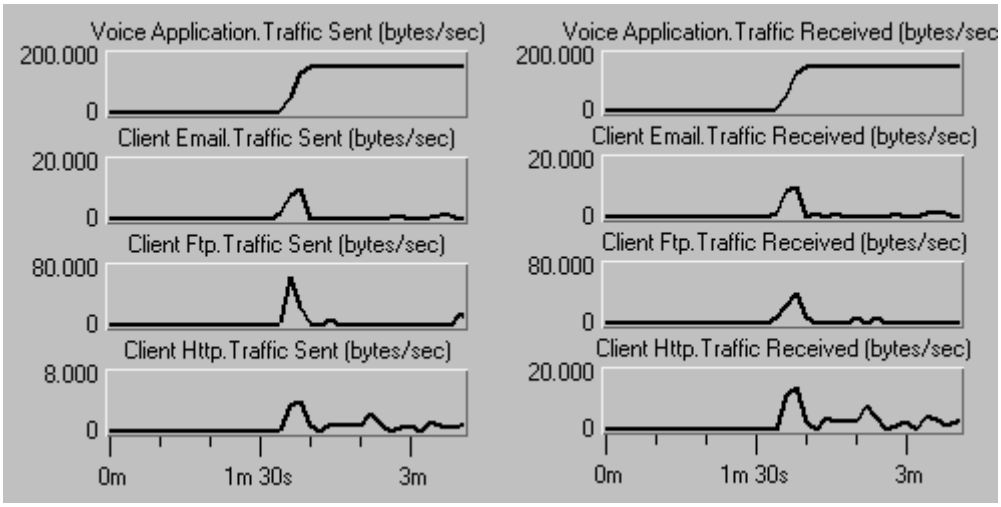
Şekil III.6 Voice Trafiği

Şekil III.6'da voice uygulaması için trafik değişimi görülmektedir. Grafikte, senaryolardaki voice trafiği saniyede gönderilen byte cinsinden ifade edilmiştir. Bu grafikten, sisteme bir hacker dahil olmasıyla, voice trafiğinin arttığı anlaşılmaktadır. Bunun sebebi, hacker'ın profil tanımlamasını gerçekleştirirken, voip hizmetinden yararlanabileceğini belirtmiş olmamızdır. Bu durum, voice trafiğinin yüksek değerlere ulaşmasına neden olmuştur. Hacker sistemdeki diğer uygulamalardan da yararlanabildiği için, tüm uygulamalarda trafik artışı görülecektir.



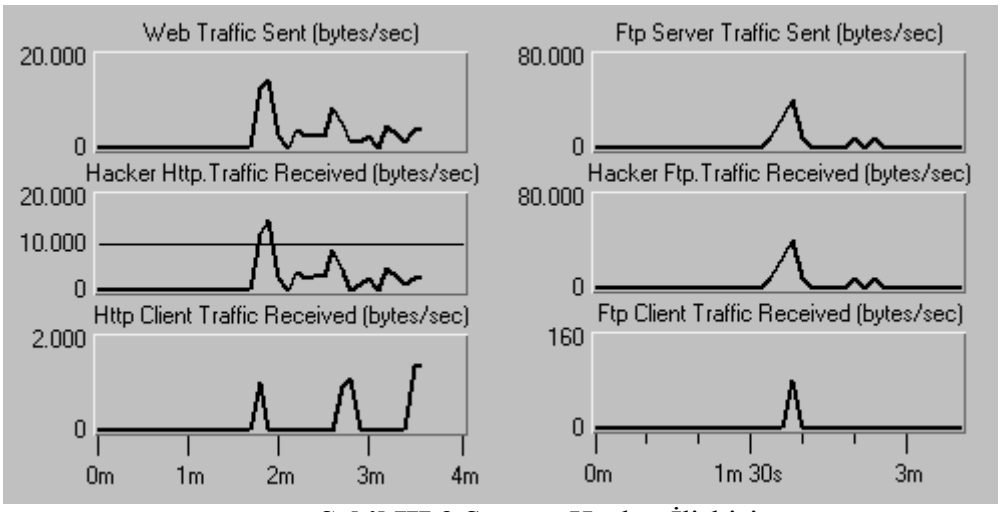
Şekil III.7 Email ve Ftp Yanıt Süreleri

Şekil III.7'de email ve ftp uygulamalarında download işlemi için yanıt sürelerinin arttığı görülmektedir. Bu durum, kullanıcılar tarafından sistemin yavaşladığı şeklinde algılanır. Bu durumun sebebi, sisteme bir hacker'ın bağlanmış olması ve DoS saldırısı düzenlenmiş olmasıdır. Sisteme etki eden hacker sayısı artması durumunda, yanıt süresi daha yüksek değerlere ulaşacaktır.



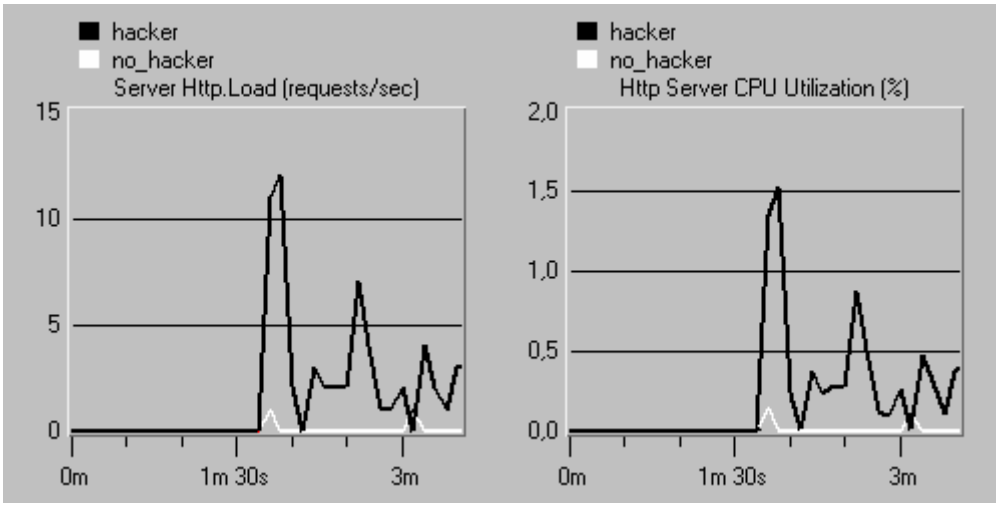
Şekil III.8 Hacker Trafiği

Şekil III.8'de hacker tarafından kullanılan uygulamalar byte cinsinden görülmektedir. Grafikte; voice, email, ftp, http uygulamaları ile yapılan veri transferi gösterilmektedir. Elde edilen verilere göre, hacker ile sunucular ve voip kullanıcıları arasında her saniye binlerce byte veri transferi olmaktadır. Bu durum sistem veriminin düşmesine neden olur.



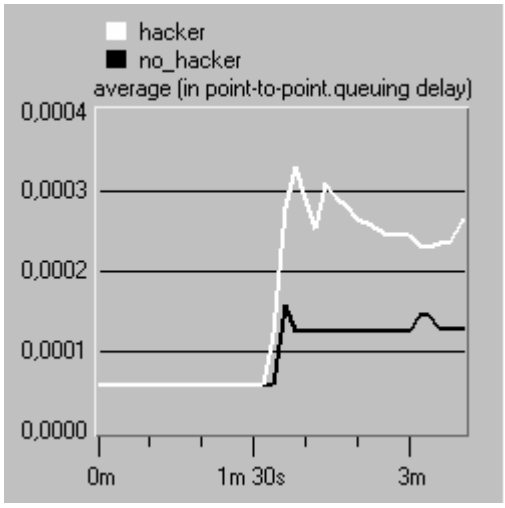
Şekil III.9 Sunucu-Hacker İlişkisi

Şekil III.9'da web sunucu ile ftp sunucu ve kullanıcılar arasındaki ilişki görülüyor. Soldaki grafikte web server, hacker ve http kullanıcısının verileri görülmektedir. Grafikte web sunucu için gönderilen (send), hacker ve http kullanıcısı için alınan (received) sinyaller incelenmiştir. Grafikte görüldüğü gibi, web sunucudan çıkan sinyallerin büyük bir bölümü, hacker tarafından alınmıştır. Aynı durum ftp sunucu içinde geçerlidir. Bu durum, sunucuların işlem yükünün hacker sebebiyle arttığını göstermektedir. Hacker'ın sistem üzerindeki olumsuz etkisi bu grafiklerde açık olarak görülmektedir.



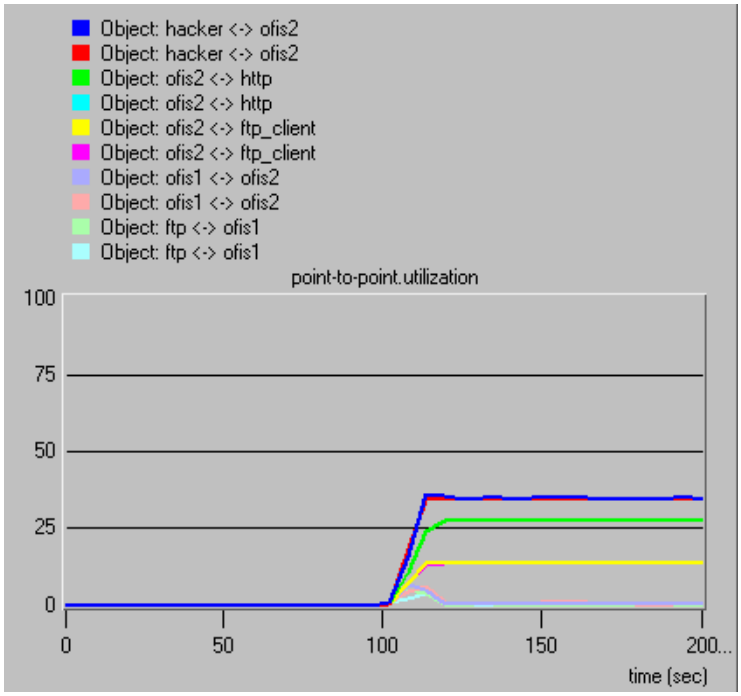
Şekil III.10 Web sunucusu hizmet değişimi

Şekil III.10'da web sunucunun farklı senaryolardaki hizmet değişimi görülmektedir. İlk grafikte sisteme hacker dahil olmasıyla, sunucuya iletilen hizmet talebindeki artış görülmektedir. İkinci grafikte ise, sunucunun kullanım oranı artmıştır. DoS saldırılarının, sistem üzerindeki olumsuz etkilerinden biri işlemci hızını yükseltmesidir. İkinci grafikte bu durum ortaya konmuştur.



Şekil III.11 Queuing Delay

Veriler hat üzerinden noktalar arasında iletilirken, iletilme süreleri değişebilir. Bu durumu hattın kapasitesi, veri hızı, kullanım oranı belirler. Noktadan noktaya gerçekleşen bu işlem sırasında geçen süre 'queuing delay' olarak tanımlanır. Şekil III.11'de bu değişim görülmektedir. Hacker hat üzerindeki paketlerin iletilme sürelerinin uzamasına sebep olmuştur.



Şekil III.12 Utilization

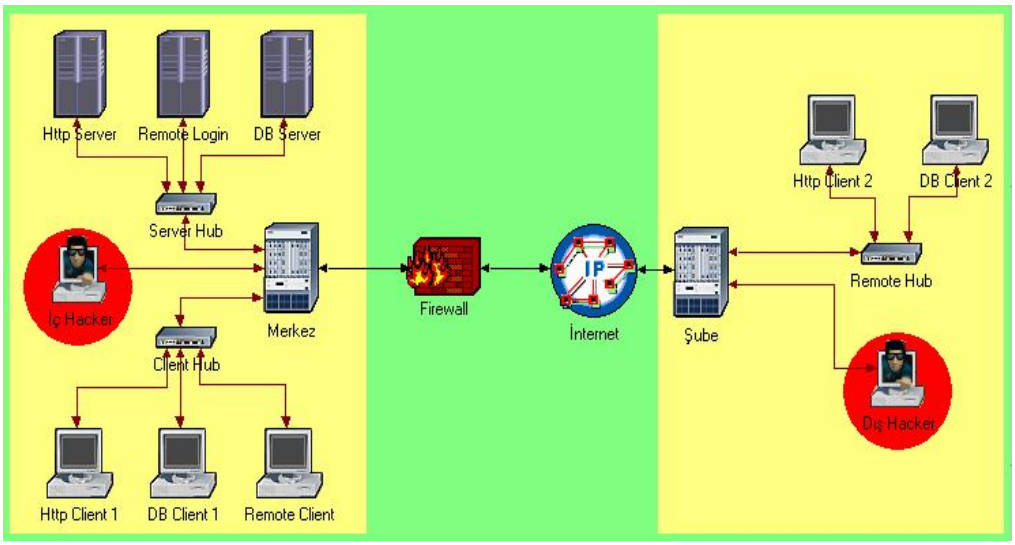
Şekil III.12'de projede bulunan iletim yollarının karşılaştırması görülmektedir. Grafikte görüldüğü gibi, hacker ile ofis2 adlı switch arasındaki hattın kullanım oranı %36'ya ulaşmıştır. Hacker'ın sisteme gönderdiği paket sayısındaki artışa göre, bu oran artabilir ve %100'ü geçmesi durumunda, bazı kullanıcılar hizmet alamayacaktır.

III.1.2 Firewall

Güvenlik saldırılarından korunmanın birçok yöntemi mevcuttur. Temel savunma yöntemlerinden biri, firewall yani güvenlik duvarı kullanımıdır. Firewall, yetkisiz erişimleri engelleyen, süzen ve izin denetimi sağlayan bileşenlerdir. Bu bileşen sayesinde, IP, port, web ve içerik filtreleme gibi çeşitli filtreleme özellikleri kullanılabilir. Bu sayede sisteme gelen ve giden paketler kontrol altında tutulabilir.

Bu projede bir merkez ve bu merkeze bağlı bir şube arasındaki veri trafiği incelendi. Proje altında iki farklı senaryo oluşturuldu. Bunlardan birinci senaryoda, firewall kullanılmamış olup, 'no firewall' adı verilmiştir. 'Firewall' adlı ikinci senaryoda, sisteme bir firewall dahil edilmiş ve diğer tüm özellikler korunmuştur.

III.1.2.1 Sistem Tasarımı



Şekil III.13 Firewall Senaryosu

Yukarıda görülen topoloji ikinci senaryoya aittir. Bu projede dört farklı uygulama kullanıldı. Projede tasarımında, biri merkezde, diğeri şubede bulunan iki hacker tasarlandı. Yapılan analizler sonucu güvenlik duvarının hacker'lar üzerindeki etkisi incelendi.

Projede 3 sunucu, 2 router, 2 hub, 1 internet bulutu, bir firewall ve ikisi hacker olmak üzere 7 workstation kullanılmıştır. Bu bileşenler kullanılarak sistemin donanımsal kurulumu senaryoda görüldüğü gibi gerçekleştirilmiştir.

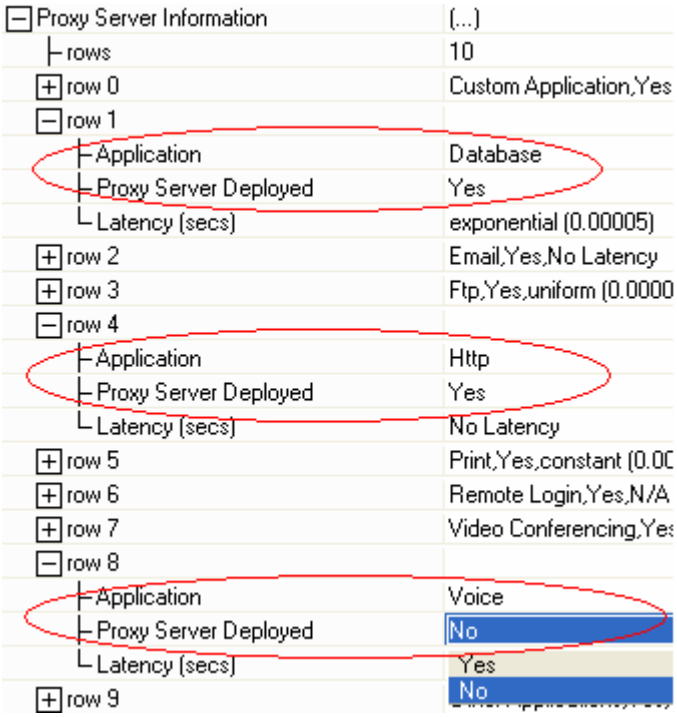
III.1.2.2 Sistem Ayarları

Projede; voip, http, remote login ve database uygulamaları kullanıldı. Bu uygulamalar için dört uygulama, dört profil tanımlaması yapılmıştır. Projedeki uygulamalarda; http, remote login ve database için 'low load', voice 'PCM quality speech' seçenekleri seçilmiştir. Profil ayarları, her profil yalnız bir uygulamayı destekleyecek şekilde düzenlenmiştir. 'Http Client', 'Remote Login Client', 'Database Client' ve 'voip' olmak üzere dört profil oluşturulmuştur.

III.1.2.3 Bileşen Ayarları

Uygulamada her bileşen adında belirtilen uygulamayı destekleyecek şekilde ayarlanmıştır. Örneğin; http server, http uygulamasını destekleyecek, DB server database uygulamasını destekleyecektir. Ayrıca http client 2' ve 'DB Client 2' hariç tüm kullanıcılar, voice uygulamasına destek verecek şekilde ayarlanmıştır. İç ve dış hacker ise; yalnız voice uygulamasını destekleyecek şekilde ayarlanmıştır.

- Firewall Ayarları: Daha önce de belirtildiği gibi proje iki farklı senaryodan oluşmaktadır. Birinci senaryoda yukarıda belirtilen tanımlamalar gerçekleştirilmiştir. Bu işlemler tamamlandıktan sonra 'no firewall' adlı senaryo tamamlanmış oldu. İkinci senaryoyu oluşturmak için, 'no firewall' adlı senaryo kopyalanmış ve 'firewall' adlı ikinci senaryo oluşturulmuştur. Seçilen firewall, 'Merkez' adlı router ve 'İnternet' adlı internet bulutu arasına yerleştirilmiştir. Ardından, firewall özelliklerine girilerek hangi uygulamalara izin verileceği ve hangi uygulamaların engelleneceği belirlenmiştir. Projede tanımlı olan dış hacker, voip profilini kullanmaktadır. Bu nedenle voip uygulaması firewall tarafından engellenmiştir. Bu durum firewall üzerinden geçen ve voip uygulamasına ait olan paketlerin engellenmesi, firewall arkasına geçememesi anlamına gelmektedir. Öte yandan projedeki, 'şube' kısmında bulunan 'Http Client 2' ve 'DB Client 2' kullanıcılarının veri iletişiminin sağlanması için, bu bileşenlerin kullandığı http ve database uygulamalarına izin verilmiştir. Şekil III.14'de bu işlem için gerekli firewall ayarları görülmektedir.

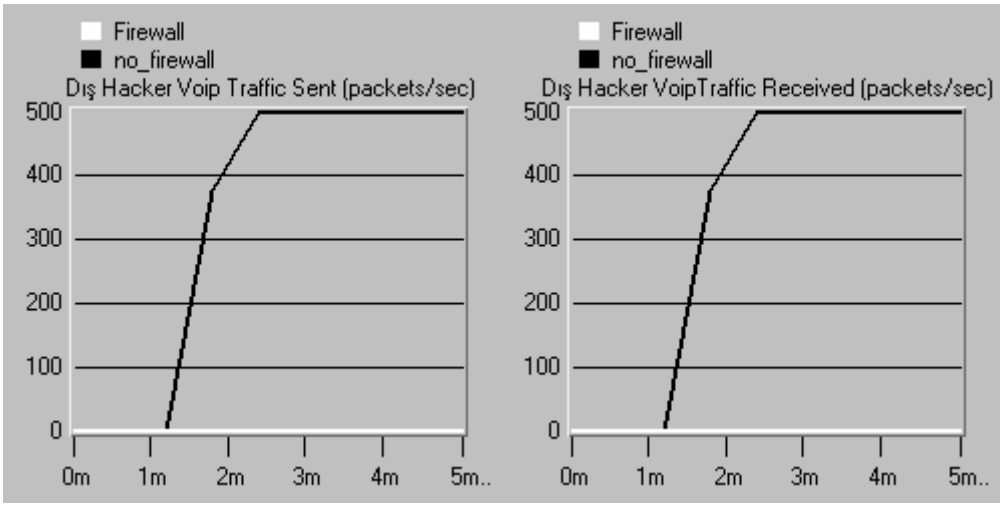


Şekil III.14 Firewall Ayarları

III.1.2.4 Simülasyon ve Analiz

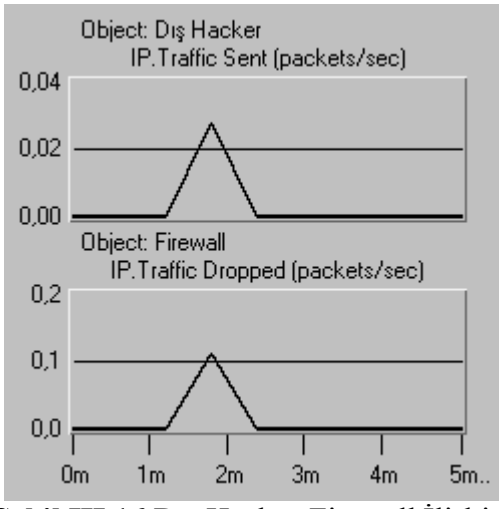
Simülasyon işlemi için, öncelikle elde edilecek verileri belirlenmelidir. Bu uygulamada Voice, DB Query, http, Remote Login ve IP, değerleri seçilmiştir ve ardından simülasyon gerçekleştirilmiştir.

Projede bulunan iki senaryonun simülasyonu tamamlandıktan sonra elde elden sonuçlar analiz edildi. Aşağıda analiz sonuçları yer almaktadır.



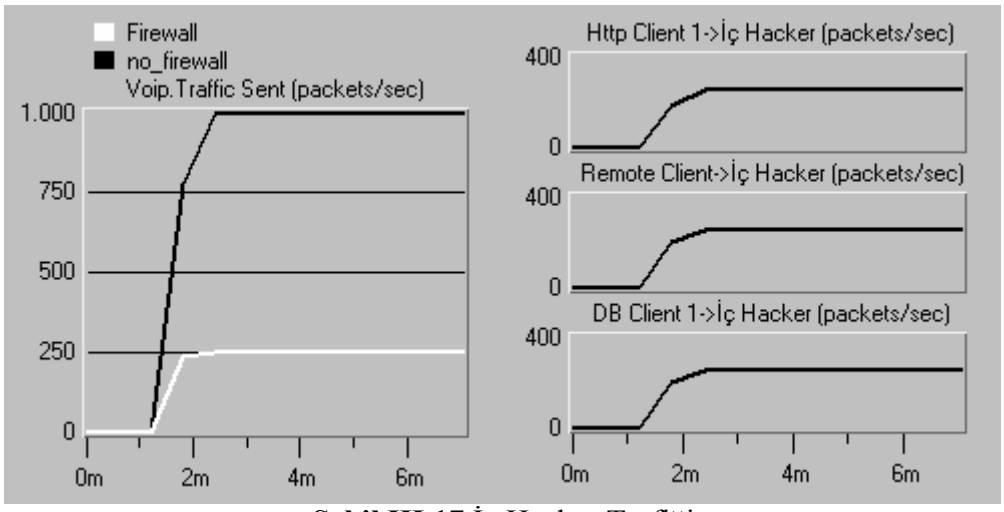
Şekil III.15 Dış Hacker Trafiği

Şekil III.15'de Dış Hacker'ın iki senaryodaki veri trafiği görülüyor. Buna göre; 'no firewall' isimli senaryoda Dış Hacker'ın diğer kullanıcılarla voip uygulaması gerçekleştirdiği görülür. Bu kullanıcılar merkez ofiste bulunmaktadırlar. Yani 'Dış Hacker' veri paketlerini, firewall üzerinden gönderebilmiştir. İkinci senaryoda ise, firewall ayarlarından voice uygulamaları engellendiği için, saldırılar engellenmiş, 'Dış Hacker'dan gelen veriler, firewall ötesine geçememiştir.



Şekil III.16 Dış Hacker-Firewall İlişkisi

Şekil III.16'da görüldüğü üzere, dış hacker tarafından gönderilen IP paketleri, firewall tarafından düşürülmüştür. Böylece, 'Dış Hacker'ın sisteme saldırı düzenlemesi engellenmiş olur.



Şekil III.17 İç Hacker Trafiği

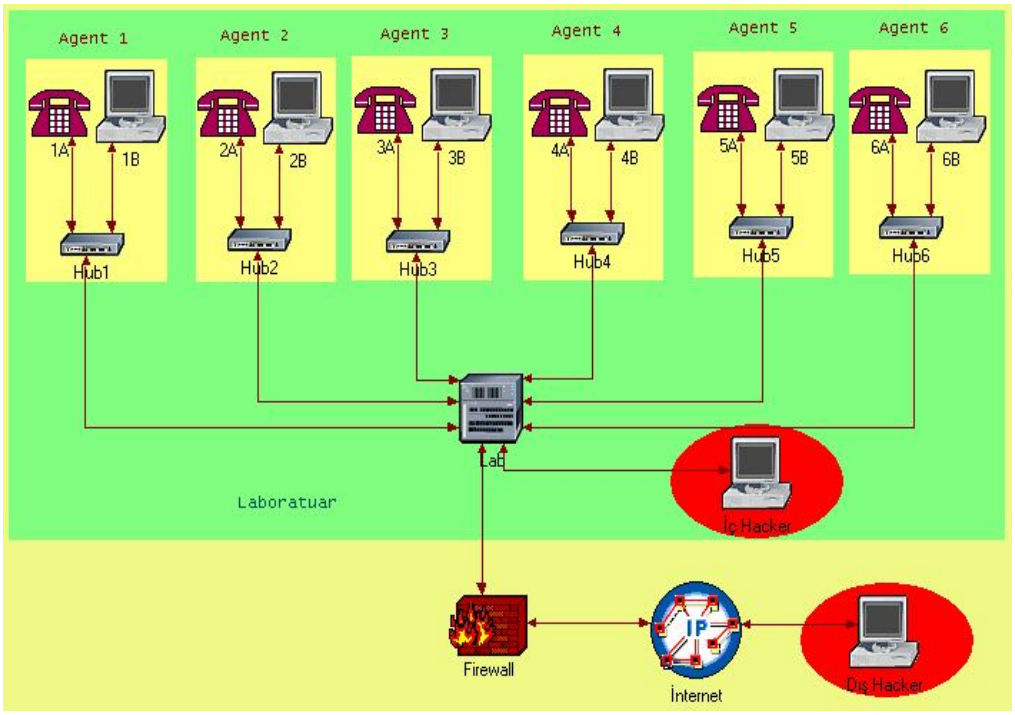
Şekilde III.17'de, ilk grafikte, 'İç Hacker'ın her iki senaryoda da veri alışverişi yapabildiği görülmektedir. Bu durum, ikinci grafikte saniyede iletilen paket cinsinden belirtilmiştir. Bunun sebebi 'İç Hacker' ve diğer voip kullanıcılarının aynı

bölüm içinde bulunmasıdır. Bu iki bileşen arasında iletilen veriler firewall üzerinden geçmediği için, firewall 'İç Hacker' sinyallerin engelleyemez. Bu durum, firewall güvenliğinin, iç saldırganlara karşı etkisiz olduğu, koruma sağlamadığının bir göstergesidir.

III.1.3 VLAN

VLAN (Virtual Local Area Network), switch üzerinde yapılan ayarlamalar ile gerçekleştirilen bir teknolojidir. Aşağıdaki simülasyonda bir VLAN sistemi tasarlanmıştır.

III.1.3.1 Sistem Tasarımı



Şekil III.18 VLAN Senaryosu

VLAN senaryosunda 6 kullanıcı bulunmaktadır. Her kullanıcı için bir IP telefon ve bir pc (softphone) mevcuttur. Kullanıcılara ait pc ve IP telefonlar birer hub vasıtasıyla merkezi switch'e bağlanır. Switch bir firewall aracılığıyla internete açılır. Merkezi switch'e bir hacker (iç hacker) bağlanmış olup, sistem kaynaklarını kullanmaya yönelik saldırılar düzenlemektedir. Ayrıca başka bir hacker (dış hacker) internet üzerinden laboratuara erişmeye çalışmaktadır. Bu projede, switch üzerinde vlan kurulu olması ve olmaması durumları ayrı ayrı incelenmiş ve sonuçlar analiz edilmiştir.

III.1.3.2 Sistem Ayarları

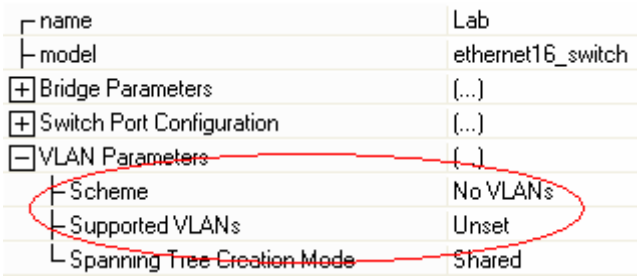
Proje kapsamında ‘Vlan’ ve ‘no_vlan’ adlı iki senaryo oluşturulmuştur. Projede yalnız ‘voice’ uygulaması gerçekleştirilmiştir. Bu kapsamda bir uygulama ve bir profil oluşturulmuştur. Her bileşen ‘voice’ uygulamasını destekleyecek şekilde yapılandırılmıştır.

III.1.3.3 Bileşen Ayarları

Projede, 6 IP telefon, 8 workstation, 6 hub, 1 switch, 1 IP bulutu ve bir firewall kullanılmıştır. Diğer projelerden farklı olarak, bu projede sunucu bulunmamaktadır. Bunun sebebi, projede yalnız voice uygulamasının gerçekleştirilmiş olmasıdır. Projede bulunan bileşenler hem voip uygulamasını, hem de voip profilini destekleyecek şekilde tanımlanmışlardır.

- Firewall Ayarları: Projede bulunan ‘Dış Hacker’ sisteme internet üzerinden bağlanmaya çalışmaktadır. ‘vlan’ ve ‘firewall’ projeleri arasında sağlıklı bir analiz yapabilmek için, sisteme bir firewall eklenmiştir. ‘Dış Hacker’ voice uygulaması için sisteme bağlanmak istemektedir. Bu nedenle firewall ayarlarından bu özellik devre dışı bırakılmıştır.
- Switch Ayarları: VLAN tanımlamaları switch üzerinde gerçekleştirilmiştir. Bu tanımlamalar aşağıda belirtildiği gibi yapılandırılmıştır.

1) no vlan: İlk senaryoda ‘vlan’ özelliği kullanılmamıştır ve bu senaryoya ‘no_vlan’ adı verilmiştir. Yapılan ayarlar Şekil III.19’da gösterilmiştir.

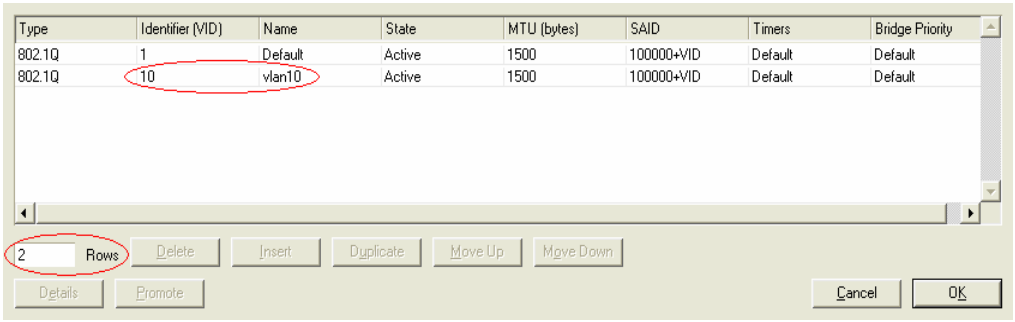


Şekil III.19 Switch Ayarları

2) vlan: Bu işlemlerden sonra ‘no vlan’ isimli ilk senaryo tamamlanmış ve bu senaryo kopyalanarak ‘vlan’ adı verilen ikinci bir senaryo oluşturulmuştur. Bu senaryoda switch ayarları değiştirilerek bir VLAN oluşturulmuştur.

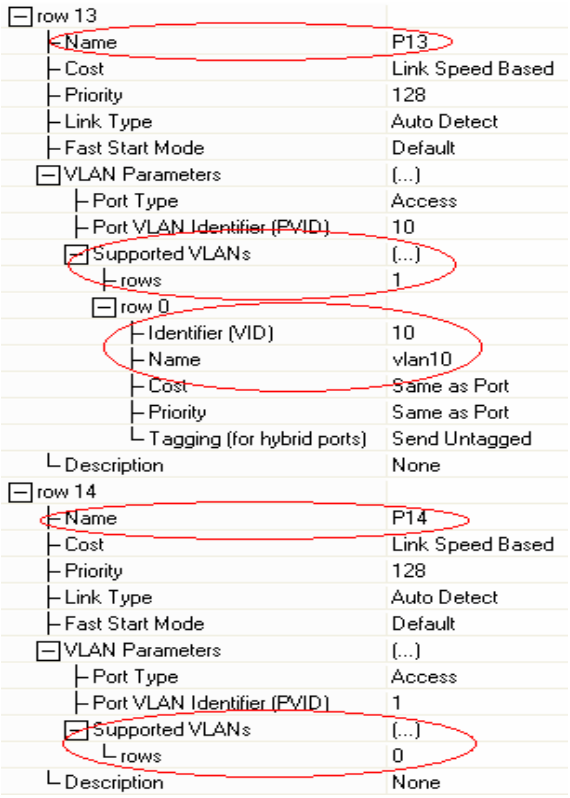
Vlan ayarlarının yapılacağı ekranda kimlik bilgisi (identifier), ‘1’ olan bir vlan tanımaması çıkar. Bu tanımlama default değer olup, tanımlayacağımız sanal ağlara ait olmayan portlar tarafından kullanılacaktır.

Tanımladığımız sanal ağ için ‘identifier’ değerini ‘10’, ‘name’ değerini ‘vlan10’ olarak belirlenmiştir.



Şekil III.20 VLAN Ayarları

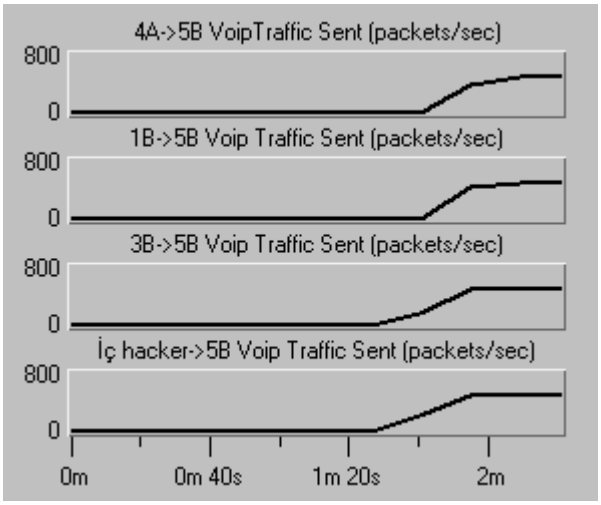
Bu işlemlerin ardından tanımlanan sanal ağların, hangi portlar tarafından destekleneceği belirlenmiştir. Projemizde ‘İç Hacker’a ait port on dördüncü porttur. Bu port için ‘vlan10’ desteği olmamalıdır. Bunun için, bu porta ait ‘PVID’ değeri ‘1’ seçilmiştir. Bu şekilde bu porta bağlı olan kullanıcının sanal ağa erişimi engellenmesi sağlanmıştır. Port tarafından desteklenen sanal ağlar kısmı boş bırakılarak, bu porta erişim engellenmiştir. On üçüncü port ise, Hub1 ile bağlantılıdır ve bu porta kullanıcıların görüşme yapabilmesi için, bu porta izin verilmiştir. Şekil III.21’de bu yapılandırma görülmektedir.



Şekil III.21 Port Ayarları

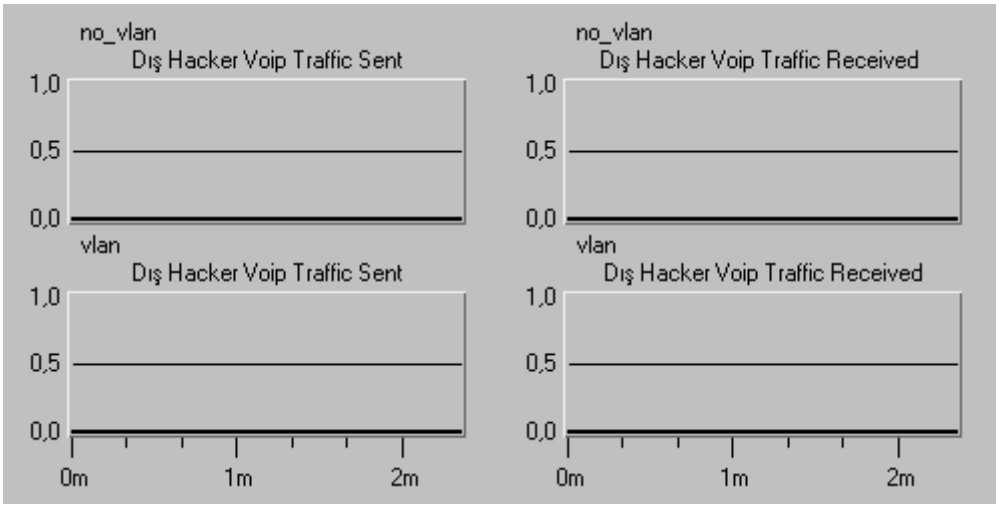
III.1.3.4 Simülasyon ve Analiz

Simülasyon için vlan ve voice, voice application, voice called party, voice calling party ve IP değerleri seçilmiştir. Simülasyon işlemi tamamlandıktan sonra, sistem bileşenlerinden elde edilen veriler analiz edilmiştir.



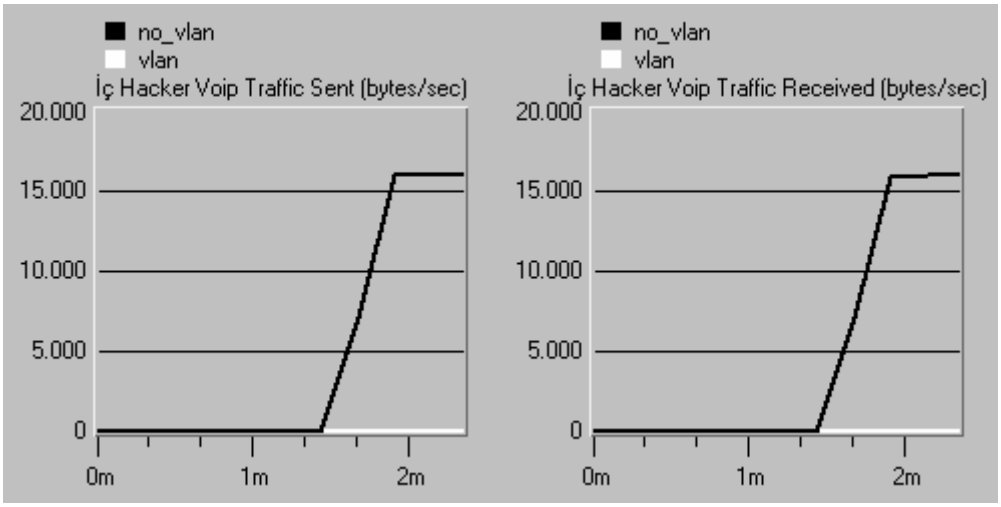
Şekil III.22 Kullanıcı Trafiği

Şekil III.22'de '5B' isimli kullanıcının, 'no vlan' senaryosundaki voice trafiği görülmektedir. En altta bulunan grafikte, 5B kullanıcısı ile iç hacker arasındaki trafik görülmektedir. Bu saldırganın sisteme girdiği anlamına gelmektedir.



Şekil III.23 Dış Hacker Trafiği **(**VLAN)

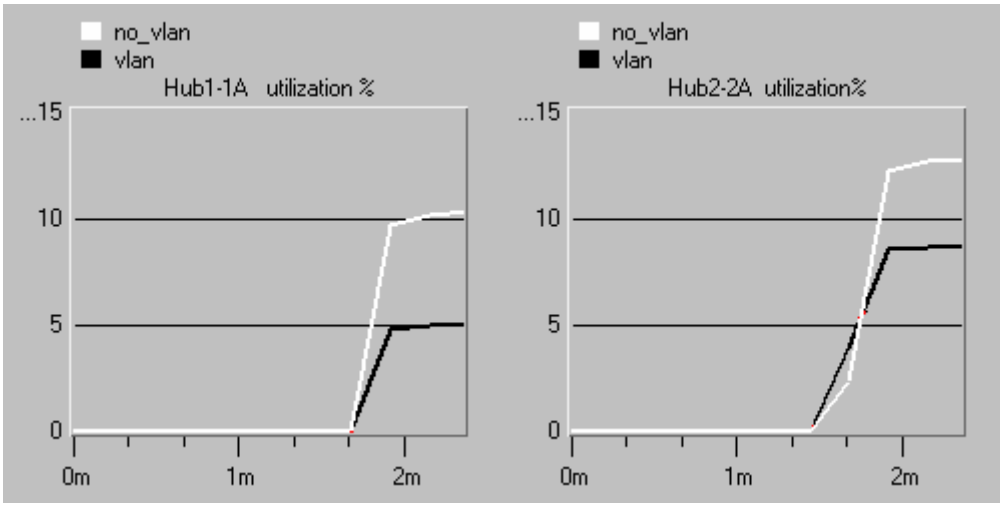
Şekil III.23'de 'Dış Hacker'ın her iki senaryoda da, veri transferi yapamadığı görülmektedir. Bunun sebebi, firewall tarafından voice uygulamasının engellenmiş olmasıdır. Önceki projede gördüğümüz gibi, firewall dış ortamdan gelen saldırganlara karşı koruma sağlamaktadır.



Şekil III.24 İç Hacker Trafiği **(**VLAN)

Şekil III.24'de 'İç Hacker'ın her iki senaryodaki veri alışverişi görülmektedir. Buna göre, 'no vlan' adlı senaryoda 'İç Hacker' diğer bileşenlerle veri alışverişinde

bulunurken, ‘vlan’ adlı senaryoda veri iletişimi yapılamadığı görülmektedir. Bunun sebebi, ‘İç Hacker’ın bağlı olduğu 14 numaralı portun veri trafiğine kapatılmış olmasıdır. Böylece, sistemin dahili saldırganlara karşı da korunmuş olduğu görülmektedir.

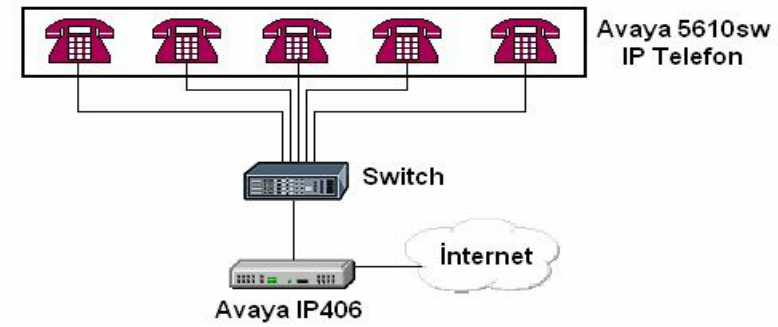


Şekil III.25 Veri Hattı Kullanım Oranı **(**VLAN)

Sanal ağların bir avantajı da, sistemin daha verimli kullanılmasını sağlamasıdır. Bileşenlerin gönderdiği sinyaller, tüm ağa değil, yalnız VLAN tarafından belirlenen portlara iletilir. Şekil III.25’te, Vlan ile birlikte, sistemin kullanım oranının düştüğü görülmektedir.

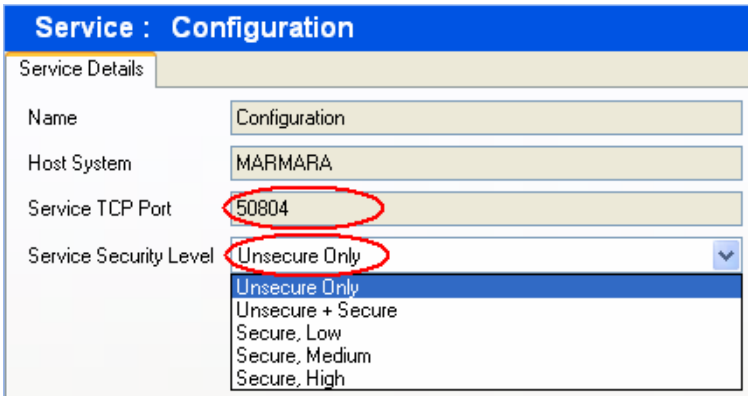
III.2 AVAYA IP406 OFFICE SANTRALİ İLE UYGULAMALAR

Avaya IP406 office, dünyanın önde gelen iletişim hizmetleri sağlayıcılarından Avaya’nın ürettiği bir IP santralidir. VoIP güvenlik uygulamalarımızın bir bölümünde, bu santral kullanılmıştır. Santral, 20 dahili hattı destekleyecek şekilde tasarlanmıştır. Uygulamalarımızda Avaya 5610sw model IP telefonlar kullanılmıştır. Santral ile IP telefonlar arasında hp 2524 model switch ile bağlantı sağlanmıştır. Uygulamalar sırasında kullanılan sistemin yapısı, Şekil III.26’da görülmektedir.



Şekil III.26 Avaya IP406 Office Sistemi

Avaya IP406 Office santralinin, beş farklı güvenlik seviyesi mevcuttur. Şekil III.27'de santrale ait güvenlik tanımlamaları görülmektedir.



Şekil III.27 Avaya IP406 Office Santrali Güvenlik Ayarları

Bu tanımlamaların içerdiği özellikler şu şekilde tanımlanmıştır:

- Unsecure Only: Bu servis türünde hiçbir güvenlik önlemi uygulanmaz. Veri iletiminde güvenli TCP port kullanılmaz. İletim sırasında, güvensiz iletim için ayrılmış 50804 nolu port kullanılır.
- Unsecure + Secure: Bu hizmet türünde güvenli (50805) ve güvensiz (50804) TCP portları birlikte kullanılır. Bu serviste TLS hizmeti sunulur, ancak şifreleme gerçekleştirilmez.
- Secure, Low: Bu hizmet türünde, TLS ve şifreleme birlikte kullanılır. Veri için kullanılan şifreleme yöntemi 'DES,40' olup, 40 bitlik şifreleme yapılır. Şifreleme sistemi zayıf olduğu için, güvenlik seviyesi düşüktür. Bu serviste, güvenli TCP portu kullanılır.
- Secure, Medium: TLS ve 52 bit şifreleme sağlayan 'DES,52' birlikte kullanılır. Orta seviyede bir güvenlik sağlar. Güvenli TCP portu kullanılır.
- Secure, High: TLS ve 3DES şifreleme sistemi kullanılır. Güvenli TCP portu üzerinden iletim gerçekleştirilir. Bu serviste ayrıca, güvenlik sertifikası kullanmak mümkündür.

Avaya IP406 santrali kullanılarak, sisteme çeşitli saldırılar düzenlenmiş ve sonuçlar analiz edilmiştir. Bu amaç için 'Cain&Abel'[52] ve 'Wireshark'[53] programları kullanılmıştır. Bu programlardan cain abel, bir şifre kurtarma programı; wireshark ise, bir paket analiz programıdır. Uygulamalar için bu programların tercih edilmesinin sebebi, birçok özelliği barındıran yapıları, kolay kullanım imkanı sağlayan arayüzleri ve en çok tercih edilen ve kullanılan güvenlik araçlarından olmalarıdır.

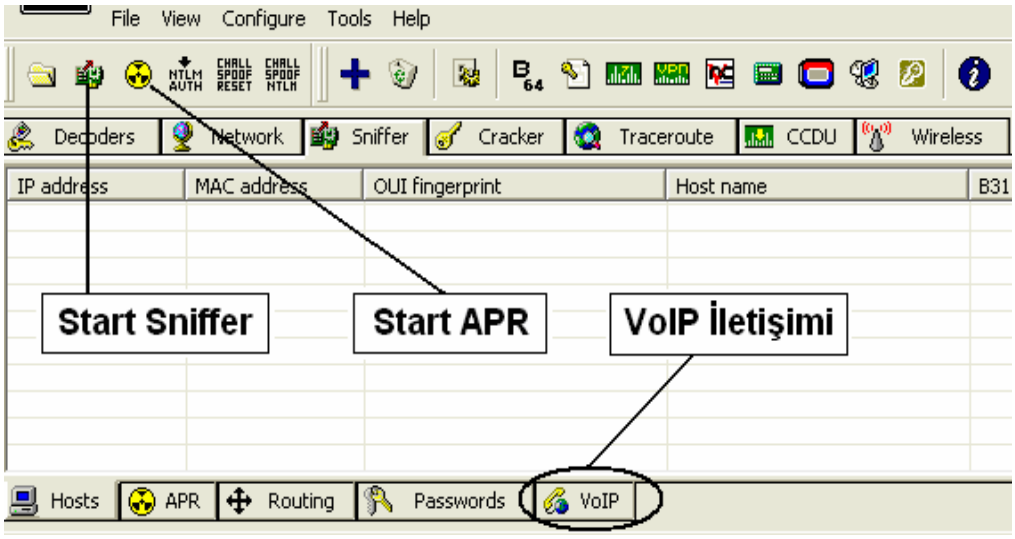
III.2.1 Cain&Abel ile Voip Analizi

Cain&Abel, Microsoft işletim sistemleri için tasarlanmış bir şifre kurtarma programıdır. Bu program; bulunduğu ağdaki MAC adresleri üzerinden tarama gerçekleştirir. Sistem üzerinde çeşitli saldırılar düzenleyerek, şifrelerin kurtarılmasını sağlar. Temel amacı, şifre kurtarma işlemini kolaylaştırmaktır. Microsoft işletim sistemleri için en çok kullanılan araçlardan biridir. Cain&Abel; sistem yöneticileri, ağ uzmanları, araştırmacılar, güvenlik yazılımı üreticileri ve test amaçlı uygulamalar için geliştirilmiştir.

Cain&Abel programı, sistemin veya herhangi bir yazılımın açıklarından faydalanan bir program değildir. Program, güvenlik özelliklerine, zayıflıklarına göre işlev görür. Bir test aracı olarak görev yapar. Protokol standartları, kimlik doğrulama yöntemlerine bağlı olarak verilere ulaşır.

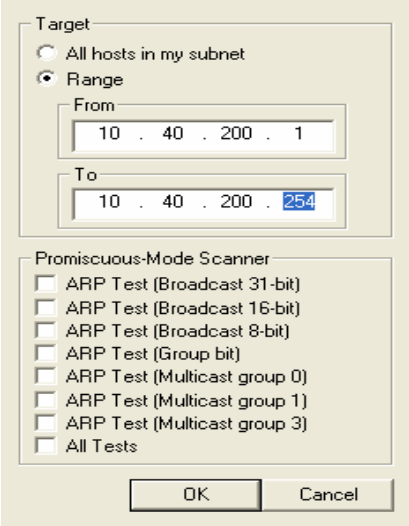
Bu program VoIP görüşmelerini kayıt altına alabilir. ARP zehirlemesi gerçekleştirerek, ortadaki adam saldırısı (Man in the middle) düzenleyebilir. Böylece ağda bulunan verilere erişilebilir.

Arp zehirlemesi saldırısı için, programın tarayıcı (Sniffer) özelliği çalıştırılmıştır. Bu özellik ağda bulunan şifrelerin tespit edilmesini sağlar. Bu uygulamada, APR (ARP Poison Routing) işleminin gerçekleştirilebilmesi için kullanılmıştır.



Şekil III.28 Cain&Abel Fonksiyonları

Programın tarama özelliği çalıştırıldıktan sonra, MAC adresi taraması gerçekleştirildi. Bu ekranda, Avaya IP Office 406 sisteminin, içinde yer aldığı küçük bir IP bloğu seçildi. Böylece tarama süresi kısaltılmış oldu.



Şekil III.29 Mac Adresi Tarama

Tarama işlemi bittikten sonra ağda bulunan bileşenler listelenir. Bizim kullandığımız sistemde bir santral ve üç IP telefon aktif durumdaydı. Şekil III.30'da aktif kullanıcılar görülmektedir. Kullanıcıların IP ve MAC adresleri, program tarafından tespit edilmiştir. Şekil III.30'da görülen bileşenlerden '10.40.200.1' IP adresine sahip bileşen, IP Office 406 santralidir. Diğer bileşenler IP telefonları göstermektedir.

IP address	MAC address	OUI fingerprint
10.40.200.1	00E007022C75	NETWORK ALCHEMY LTD.
10.40.200.23	00040DE25F7E	Avaya, Inc.
10.40.200.27	00040DE25D10	Avaya, Inc.
10.40.200.28	00040DE2726E	Avaya, Inc.

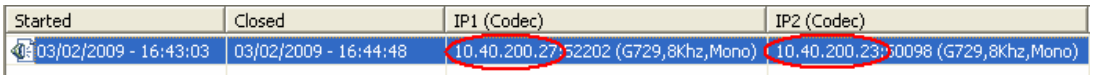
Şekil III.30 Ağda Bulunan Bileşenlerin Tespiti

Programdaki APR fonksiyonu kullanılarak, Arp zehirleme işlemini başlatılmıştır. Şekil III.31'de; işlem durumu, kullanıcılar, transfer edilen paketler hakkında elde edilen bilgiler görülmektedir.

Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address
Poisoning	10.40.200.27	00040DE25D10	5242	5240	00040DE25F7E	10.40.200.23
Poisoning	10.40.200.27	00040DE25D10	0	0	00040DE2726E	10.40.200.28
Poisoning	10.40.200.23	00040DE25F7E	3296	3293	00040DE2726E	10.40.200.28

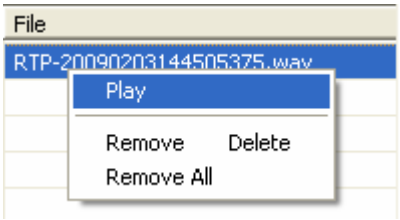
Şekil III.31 ARP Zehirlemesi Saldırısı

Sona eren görüşmeler, VoIP menüsü kullanılarak incelenebilir. Şekil III.32'de, gerçekleştirilen VoIP görüşmesinin; başlangıç ve bitiş süreleri, bileşenlerin IP adresleri, kullanıcıların ilettiği veri paketi sayısı, kullanılan ses sıkıştırma tekniği hakkında elde edilen veriler görülmektedir.



Şekil III.32 VoIP Görüşmesinin Kaydedilmesi

Kaydedilen görüşmeler, programın yüklü olduğu bilgisayarın sabit diskine kaydedilmiştir. Görüşme kaydı, saldırı işleminin ardından kolaylıkla dinlenebilir. Şekil III.33'de, program üzerinden, VoIP görüşmesinin dinlenmesi gösterilmiştir.



Şekil III.33 VoIP Görüşmesinin Dinlenmesi

Bu uygulama ile ARP zehirlemesi gerçekleştirilmiştir. Hedef seçilen bileşenin gerçekleştirdiği VoIP görüşmeleri, öncelikle Cain&Abel programını kurduğumuz bilgisayara aktarılmıştır. Daha sonra, bu bilgisayardan hedef kullanıcıya yönlendirilmiştir. Bu şekilde ortadaki adam saldırısı gerçekleştirilmiş ve görüşmelerin ARP zehirlemesi yöntemiyle kaydedilebileceği gösterilmiştir.

III.2.2 Wireshark ile Voip Analizi

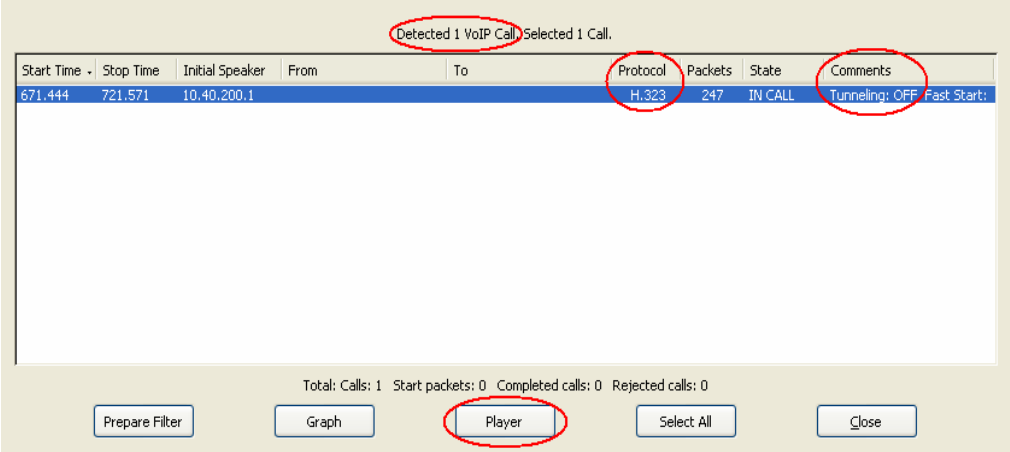
Wireshark programı bir ağ analiz programıdır. Program, bir ağ içinde dolaşan veri paketlerini yakalayarak, bu paketler hakkında bilgiler sunar. Bu program kullanılarak ağ içinde dolaşan veri paketleri incelenebilir.

Bu bölümde Avaya IP406 Office santrali kullanılarak, ağda dolaşan veri paketleri incelenmiş ve H.323 temelli bu sisteme, eavesdropping (Telekulak) saldırısı düzenlenmiştir. Bu uygulamada iki farklı senaryo kullanılmıştır. Kullandığımız santralin güvenlik özellikleri değiştirilerek, elde edilen sonuçlar analiz edilmiştir.

III.2.2.1 'Unsecure' Güvenlik Modu

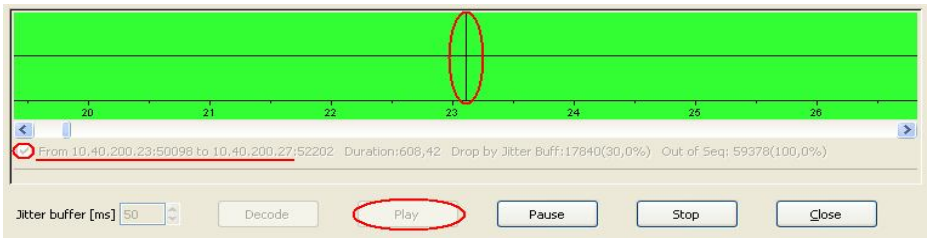
İlk uygulama için, santralin güvenlik özelliklerine girilerek, 'Unsecure' seçeneği aktif hale getirilmiştir. Bu sayede, veri ve iletim yolu üzerinde hiçbir güvenlik önlemi olmayacak ve veri paketlerine erişilebilecektir. IP telefonlar arasında görüşme başlatılmış ve wireshark programı çalıştırılarak paket analizine başlanmıştır.

Wireshark programında VoIP görüşmelerini görüntülemek için tasarlanmış bir menü bulunmaktadır. Bu menü yardımıyla ağ üzerinde dolaşan veri paketleri taranır ve VoIP görüşmeleri belirlenir.



Şekil III.34 Wireshark İle VoIP Görüşmelerinin Belirlenmesi (Unsecure)

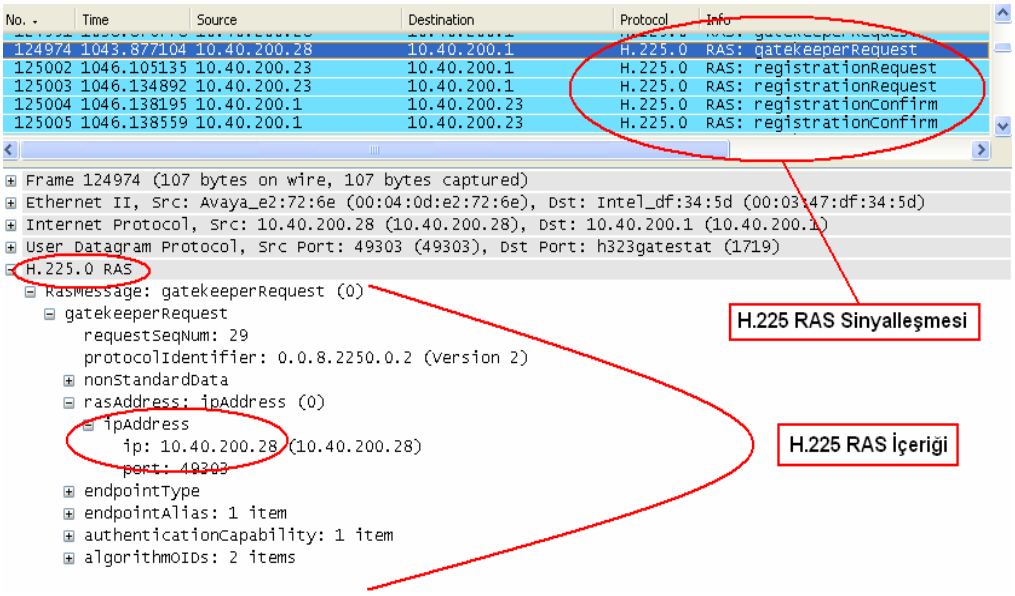
Şekil III.34'de wireshark kullanılarak, tespit edilen bir VoIP görüşmesi görülmektedir. Şekilde tespit edilen veri ile ilgili veriler yer almaktadır. Buna göre, uygulamamızda bir VoIP görüşmesi tespit edilmiş olup, H.323 protokolünü kullanılmıştır. Şekilde görülen 'Comments' bölümünden, uygulamada tünelleme yapılmadığı bilgisi verilmiştir. Şekilde bulunan player tuşu kullanılarak, tespit edilen görüşmenin dinlenmesi mümkündür.



Şekil III.35 Wireshark İle VoIP Görüşmelerinin Dinlenmesi

Şekil III.35'de tespit edilen VoIP görüşmesinin dinlenmesi gösterilmiştir. Bu durum, güvenlik önlemi olmadığı zaman, VoIP görüşmelerinin dinlenebileceğini göstermektedir.

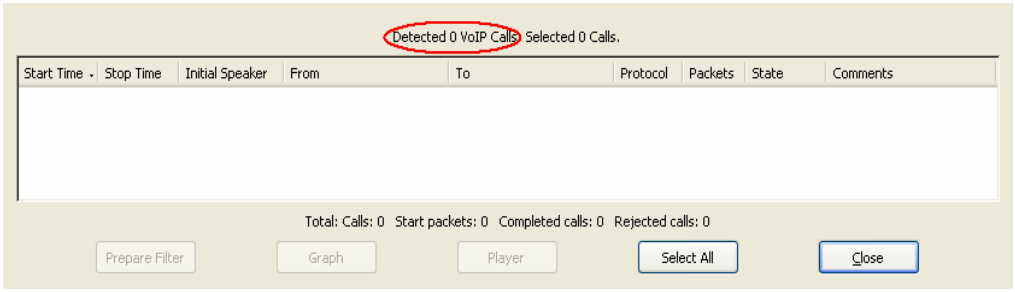
Wireshark aynı zamanda iletilen sinyalleri de görüntüleyebilir. Şekil III.36'da, terminal ile gatekeeper arasındaki sinyalleşme görülmektedir. Uygulamamızda, gatekeeper santral olup IP numarası '10.40.200.1'; terminal ise IP telefonlar olup, IP numarası '10.40.200.28'dir. Şekilde bileşenler arasındaki mesajlaşma sinyalleri ve bu sinyallerin içerikleri gösterilmiştir.



Şekil III.36 H.323 RAS Sinyallerinin Görüntülenmesi

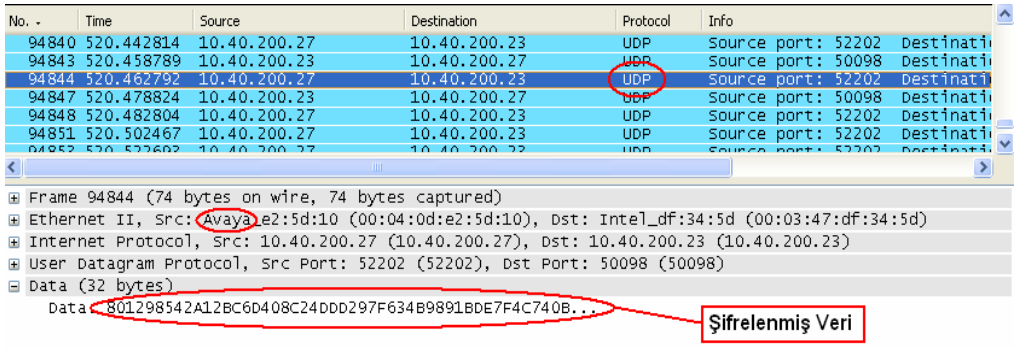
III.2.2.2 'Secure, High' Güvenlik Modu

Güvensiz iletimin test edildiği ilk uygulamanın ardından, santralin özelliklerine girilerek, güvenlik ayarları 'Secure, High' olarak belirlenmiştir. Santral bu moda çalışırken, iletim sırasında TLS kullanılacak ve şifreleme gerçekleştirilecektir. Bu ayarları gerçekleştirdikten sonra, wireshark programı çalıştırılmış, veri paketleri analiz edilmiş, ancak VoIP görüşmesi tespit edilememiştir.



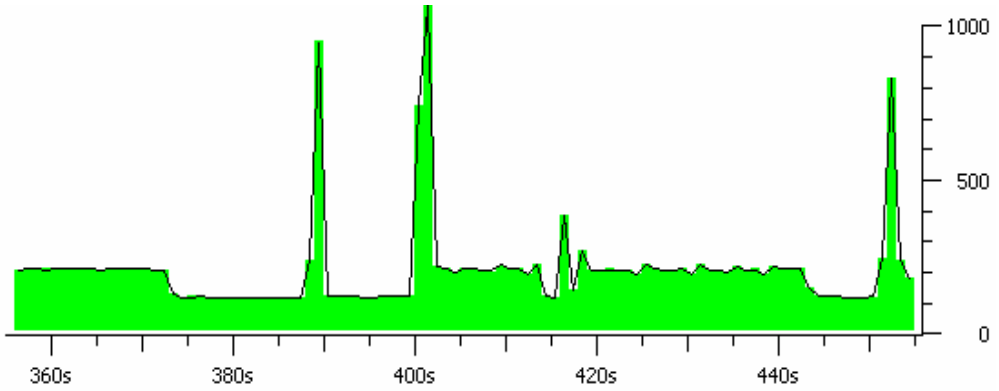
Şekil III.37 Wireshark İle VoIP Görüşmelerinin Belirlenmesi (Secure, High)

Güvenlik düzeyi artırılınca, VoIP görüşmeleri tespit edilememiştir. Ancak wireshark programı ağ üzerinde dolaşan paketleri tespit etmiştir. Şekil III.38'de UDP paketlerinin iletimi görülmektedir. Seçilen paket için; kullanıcıların IP adresleri, kullandıkları protokol, transferin gerçekleştiği port bilgileri yer almaktadır. Şeklin alt kısmında daha detaylı bilgiler gösterilmiştir. Bu bölümde sırasıyla; Frame, Ethernet, IP, UDP, veri paketleri ile H.323 sistemi tanımlanmıştır. En üst kademede şifrelenmiş veri paketi görülmektedir. Bu katmanın üstünde uygulama katmanı yer alır. Wireshark programı da, uygulama katmanını temsil etmektedir.



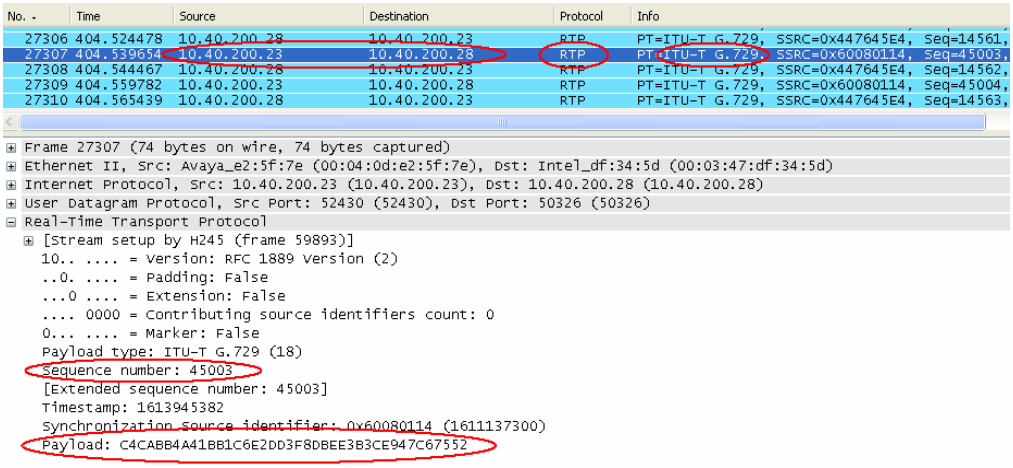
Şekil III.38 UDP paketlerinin Görüntülenmesi

Şekil III.39'da, tespit edilen bu UDP paketlerinin grafiksel gösterimi görülmektedir. Şekle göre 355-455 saniyeleri arası UDP trafiği görülmektedir. Bu uygulamada, bir paket analiz programı olan wireshark, veri paketlerini görebilmiş, ancak onlara erişememiştir. Bu durum, veri iletiminde TLS ve şifreleme kullanmanın ne kadar önemli olduğunun kanıtıdır.



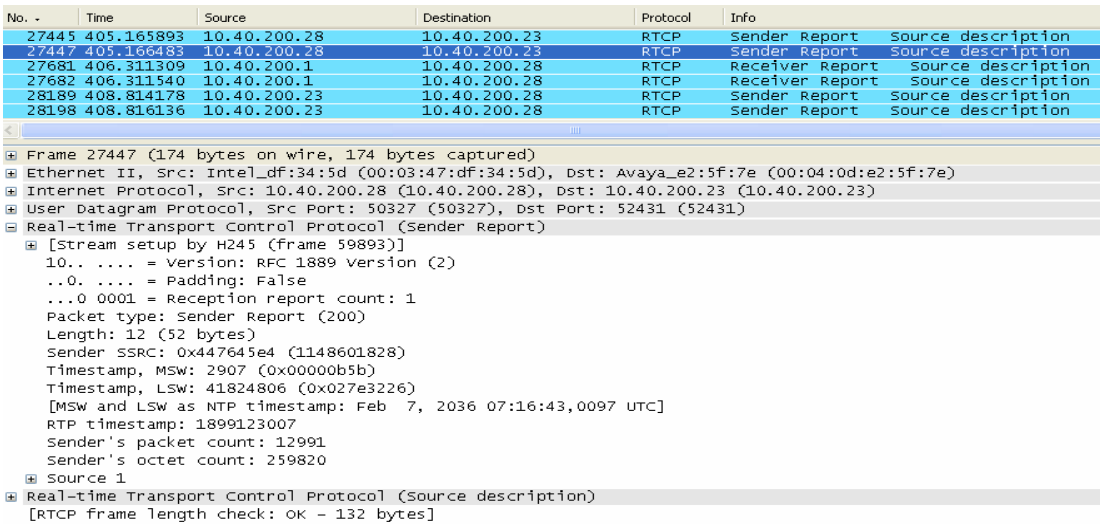
Şekil III.39 UDP Grafiği

Ses, gerçek zamanlı iletilmesi gereken bir veridir. VoIP teknolojisinde, bu işlemi RTP protokolü gerçekleştirir. Şekil III.40'da, gerçek zamanlı veri iletimini sağlayan RTP paketlerinin içeriği görülmektedir. Şekilde kullanıcı bilgileri, kullanılan ses kodlama tekniği ve paket içeriği görülmektedir. RTP protokolü aynı zamanda, veri paketlerinin sıraya dizilmesinde görev alır. Şekilde 'Sequence number' olarak belirtilen kısım, incelenen veri paketinin sırasını belirtmektedir. Bunun yanında zaman damgası (timestamp) ve kullanıcı bilgilerini (syncronization source identifier) kullanarak senkronizasyon işlemi gerçekleştirir. Bu bilgiler RTP paket içeriğinde görülmektedir.



Şekil III.40 RTP Paketlerinin Görüntülenmesi

Şekil III.41'de RTCP protokolünün yapısı görülmektedir. Bu protokol gerçek zamanlı iletimi gerçekleştirilen veri paketlerinin, iletilme durumunu kontrol eder. Şekilde, RTCP paketinde yer alan, kullanıcılara ve iletilen verilere ait bilgiler görülmektedir.



Şekil III.41 RTCP Paketlerinin Görüntülenmesi

Bu uygulamada wireshark programı kullanılarak, telekulak saldırısı düzenlenmiştir. Avaya IP 406 santralinin güvenlik ayarları iki farklı modda çalıştırılmış, elde edilen sonuçlar değerlendirilmiştir. Bu uygulama sonucunda, veri paketlerinin şifrelenmesinin ve iletim hattının güvenliğinin sağlanmasının önemi ortaya konmuştur.

BÖLÜM IV

SONUÇLAR ve TARTIŞMA

VoIP teknolojisinde bulunan güvenlik açıklarına karşı, birçok güvenlik önlemi bulunmaktadır. Bunlardan bir kısmı sinyalleşmeyi, bir kısmı veriyi korumaya yönelik önlemlerdir. Bu önlemler çeşitli kuruluşlar tarafından tanımlanmakta ve geliştirilmektedir. Bu önlemlerin kullanıcıya yansıyan kısmı, güvenlik teknolojileri olarak karşımıza çıkmaktadır. Güvenlik teknolojilerinden olan firewall ve VLAN teknolojilerinin, uygulama bölümünde opnet programı ile simülasyonu gerçekleştirilmiştir. (bkz. III.1) Veri korumaya yönelik olarak, şifreleme yöntemleri ve iletim hattının güvenliğini sağlayan protokoller geliştirilmiştir. Bu teknolojilerden TLS ve şifreleme yöntemleri gerçekleştirilen uygulamalarla test edilmiştir. (bkz. III.2) Gerçekleştirilen uygulamalar sonucunda aşağıda belirtilen sonuçlara ulaşılmıştır.

- DoS Saldırısı Sonuçları

Uygulama bölümünde öncelikle bir DoS saldırısı projelendirilmiştir. DoS saldırısının sistem üzerindeki olumsuz etkileri incelenmiştir. Bu saldırı türünün hangi bileşenleri ne kadar etkilediği grafiklerle ortaya konmuştur. Buna göre bir DoS saldırısın sistem üzerindeki olumsuz etkileri şu şekilde sıralanabilir:

DoS saldırıları sistem kaynaklarını kullanmaya yönelik bir saldırı olduğu gösterilmiştir. Bir saldırı sırasında, veri trafiğinin arttığı belirlenmiştir. (bkz. Şekil III.6)

Saldırı sırasında veri tarafiğinin artmasıyla birlikte, sunucuların yanıt süreleri artmaktadır. Bu durum, DoS saldırılarının sistemi yavaşlattığını göstermektedir. (bkz. Şekil III.7)

Saldırgan kullanıcılar arası gerçekleştirilen veri transferlerinde, sunuculardan bağımsız olarak kullanıcıları etkileyebilir. Bu durum, kullanıcıların saldırgan tarafından meşgul edilmesi, servislerden gerektiği gibi yararlanamaması sonucunu doğurur. (bkz. Şekil III.8)

Saldırganın, sisteme etkisi gönderdiği sinyal boyutu ile doğru orantılı olarak değişmektedir. Büyük çapta saldırılar, sistem kaynaklarının büyük kısmını saldırganın kullanmasına neden olabilir. (bkz. Şekil III.9)

Saldırganlar, sistemin fazla çalışması sonucunu doğuracağından, işlem kapasitesi artar. Bu durum işlemcilerin çalışma oranını artırır. DoS saldırılarının işlemci kullanım oranlarını olumsuz yönde etkilediği görülmektedir. (bkz. Şekil III.10)

DoS saldırıları verilerin iletim hattı üzerinden iletim sürelerinin artmasına neden olur. (bkz. Şekil III.11)

DoS saldırısı sonucu sistem olumsuz yönde etkilenmiş, sistem kaynakları saldırgan tarafından kullanılmış, sistem yavaşlamış, ancak kullanıcılar hizmet almaya devam edebilmişlerdir. (bkz. Şekil III.10, Şekil III.12) Bu durum güvenlik kriterlerinde belirtilen 'erişilebilirlik' ilkesine uygundur. Yani, sisteme bir saldırı olması durumunda dahi, kullanıcılar hizmet almaya devam edebilmektedirler.

- Firewall Uygulaması Sonuçları

Bir sisteme bir saldırı düzenlenmesi, bir saldırganın o sisteme erişmesi anlamına gelmektedir. Sistemi saldırılardan korumak için, saldırganın sisteme erişimini engellemek gerekir. Bunun için kullanılan en temel önlemlerden biri firewall olarak gösterilebilir. Güvenlik duvarları, üzerinden geçen trafiği filtreleme özelliğine sahiptir. Bu özellik sayesinde, trafik akışını kontrol edebilirler. Bunun için gerekli olan, verinin firewall üzerinden iletilmesidir. Firewall uygulaması ile, aşağıdaki sonuçlara ulaşılmıştır.

Bir firewall, üzerinden geçen trafiği engelleyebilir. Saldırganların erişmesinin istenilmediği bir uygulama, firewall kullanılarak güvenli hale getirilebilir. (bkz. Şekil III.15)

Saldırgan tarafından gönderilen sinyaller, firewall tarafından etkisiz hale getirilir. (bkz. Şekil III.16)

Firewall yalnızca üzerinden geçen trafiği kontrol edebildiği için, sistem içerisindeki yerel ağlarda bulunan saldırganlara karşı, koruma sağlayamaz. Güvenlik duvarları, dahili saldırganlara karşı etkisizdir. (bkz. Şekil III.17)

• VLAN Uygulaması Sonuçları

VLAN, bir ağ üzerinde sanal ağlar oluşturarak, ağın mantıksal bölümlere ayrılmasını sağlayan teknolojidir. VLAN uygulamasında, bir switch üzerine VLAN yapılandırması gerçekleştirilerek, saldırganlar ve sistem üzerindeki etkisi incelenmiştir.

Sanal ağ tanımlamaları sırasında erişime engellenen portlardan veri transferi yapılamamaktadır. Bu nedenle sistemde tanımlı olan kullanıcılar haricindeki portlar veri trafiğine kapanarak, saldırganların sisteme erişmeleri engellenir. (bkz. Şekil III.24)

Sanal ağlar, sistemde daha az yayın (broadcast) yapıldığı için, iletim hatlarının kullanım oranı düşer. Bu durum sistemin daha verimli çalışmasını sağlar. (bkz. Şekil III.25)

• Cain&Abel ile Voip Analizi Sonuçları

Cain&Abel, ağ üzerinde tarama yapan ve ağda bulunan bileşenlere 'ARP Poisoning' saldırısı uygulayabilen bir programdır. Program kullanılarak 'Avaya IP406 Office' santraline saldırılar düzenlenmiştir. Bu program ile gerçekleştirilen uygulama sonucunda şu sonuçlara varılmıştır:

Ağ taraması gerçekleştiren bir program kullanarak, sistem üzerindeki bileşenler tespit edilebilir. Bileşenlerin IP adreslerine ve MAC adreslerine ulaşılabilir. (bkz. Şekil III.30)

Cain&Abel programı kullanılarak, ARP poisoning saldırısı gerçekleştirilebilir. Böylece hedef alınan kullanıcılar arası görüşmeler kayıt altına alınabilir ve dinlenebilir. (bkz. Şekil III.31, Şekil III.32, Şekil III.33)

• Wireshark ile Voip Analizi Sonuçları

Wireshark programı kullanılarak 'Avaya IP406 Office' santrali üzerinde paket analizleri yapılmıştır. Santralin güvenlik ayarları değiştirilerek, sistem güvenliği test edilmiştir.

Hiçbir güvenlik önleminin alınmadığı durumlarda, wireshark programı ile VoIP görüşmeleri tespit edilebilir ve dinlenebilir. (bkz. Şekil III.34, Şekil III.35)

Bileşenler arası iletişimi sağlayan H.225 RAS sinyalleri incelenebilir. Paket içerikleri görülebilir. (bkz. Şekil III.36)

Sistem güvenli moda çalışırken, VoIP görüşmeleri wireshark programı tarafından dinlenemez. (bkz. Şekil III.37) Bunun anlamı, veri paketleri ve iletim hattının güvenli hale getirilmesiyle, VoIP sistemlerinde güvenliğin sağlanabileceğidir.

Wireshark programı paket analizi gerçekleştiren bir program olduğundan, bileşenler arası iletilen sinyalleşmeleri görebilir. Bu şekilde veri paketleri tespit edilebilir. Ancak sistemde bulunan güvenlik önlemleri, bu paketlerin dinlenmesini engeller. (bkz. Şekil III.38)

Ses paketleri UDP protokolü üzerinden gönderilmektedir. Bu durum wireshark programı ile grafiksel olarak analiz edilebilir. (bkz. Şekil III.39)

Gerçek zamanlı iletim sağlayan RTP ve bu iletimi kontrol eden RTCP protokolleri analiz edilebilir. (bkz. Şekil III.40, Şekil III.41)

BÖLÜM V

SON DEĞERLENDİRMELER ve ÖNERİLER

Bu tezde internet üzerinden ses taşıma teknolojisi olan VoIP teknolojisinin yapısı, VoIP teknolojisindeki güvenlik sorunları, bu sorunlara karşı alınan önlemler incelenmiştir. Kullanılan teknolojiler opnet programında örneklenmiş, çeşitli senaryolar tasarlanarak, güvenlik tehditleri ve güvenlik önlemleri ile ilgili simülasyonlar gerçekleştirilmiştir. Avaya IP406 Office santrali kullanılarak, gerçek bir VoIP sistemi üzerinde, saldırılar düzenlenmiş ve farklı güvenlik seviyelerinde test edilmiştir. Bu tez çalışması sonucunda güvenli bir VoIP iletişimi için gerekli kriterler şu şekilde belirlenmiştir:

- Bir VoIP sisteminin dış tehditlere karşı korunarak güvenli hale getirilebilmesi için firewall kullanılmalıdır.
- Sisteme etki edebilecek dahili saldırganlara karşı sanal ağ kurulmalı, kullanılmayan portlar veri trafiğine kapatılmalıdır.
- Bir VoIP sisteminde iletim hattının güvenliğini sağlamak için, TLS protokolü kullanılmalıdır.
- İletilen veri paketlerinin güvence altına alınabilmesi için, şifreleme yöntemleri kullanılmalıdır.
- Bir sistem tasarımı gerçekleştirilirken, güvenlik kriterleri dikkate alınmalı, sistemin gizlilik ve güvenliği sağlanırken, sistem erişilebilirliği göz ardı edilmemelidir. Bu şekilde, sisteme karşı yapılan saldırılardan, kullanıcıların en az derecede etkilenmesi sağlanır.

KAYNAKLAR

[1] Davidson, J.; Peters, J.; Bhatia, M.; Kalidindi, S.; Mukherjee, S. "*Voice over IP Fundamentals*", Cisco Systems, Inc., Indianapolis, USA, **(2007)**

[2] Küçük, Ş.C.: "Voice over IP, IP üzerinde Ses", Hacettepe Üniversitesi, Bilgisayar Bilimleri Mühendisliği, **(2002)**

[3] Yavaş, S.: "VoIP Güvenliği", İstanbul Teknik Üniversitesi Bilgisayar Bilimleri, **(2007)**

[4] Keskin, S.: "İnternet protokolü üzerinden ses iletiminde (VoIP) güvenlik", Yüksek Lisans Tezi, Yıldız Teknik Üniversitesi Fen Bilimleri Enstitüsü, İstanbul, Türkiye, **(2007)**

[5] Porter, T.; Baskin, B.; Chaffin, L.; Cross M.; Kanclirz, Jr.J.; Rosela, A; Shim, C.; Zmolek, Andy.: "*Pratical VoIP Security*", Syngress Publishing, Inc., Canada, **(2006)**

[6] Kuhn, D.R.; Walsh, T.J.; Fries, S.; "*Security Considerations for Voice Over IP Systems*", National Institute of Standards and Technology, Gaithersburg, MD, **(2005)**

[7] Thermos, P.; Takanen, A.: **"***Securing Voip Networks*"**,** Pearson Education, Inc., Massachusetts, USA, **(2008)**

[8] Pena, E.A.: "Miami Man Arrested in Network Hacker Fraud that Victimized New Jersey Voice-Over-Internet Provider", http://www.usdoj.gov/usao/nj/press/files/pena0607_r.htm, **(2006)**

[9] Luthra, A.; Ashraf, W.: "Security in VoIP Systems", Master's Thesis, Technical University of Denmark, **(2005)**

[10] Sen, E.: "Kriptografi ve Kullanım Alanları - I", http://www.scribd.com/doc/2581535/Kriptografi-ve-Kull-Alan-I, (Son Erişim Tarihi: Şubat **2009**)

[11] Görmen, E.: "İletişim Ağı Güvenliği", ASES Bilgi Güvenlik Teknolojileri Ltd., http://www.ases.com.tr/pdf/PKI.pdf, (Son Erişim Tarihi: Şubat **2009**)

[12] Tektaş, M.; Baba, F.; Çalışkan, E.M.: "Şifreleme Algoritmalarının Sınıflandırılması ve Bir Kredi Kartı Uygulaması", 3RD International Advanced Technologies Symposium, Ankara, Türkiye, Ağustos, **(2003)**

[13] Yerlikaya, T.; Buluş, E.; Arda, D.: "Asimetrik Kripto Sistemler ve Uygulamaları", II. Mühendislik Bilimleri Genç Araştırmacılar Kongresi, İstanbul, Kasım **(2005)**

[14] Urazimbetova, S.; Madsen, M.K.: "Transport Layer Security Analysis", Aarhus University, Department of Computer Science, December 16, **(2008)**

[15] Jain, R.: "Secure Socket Layer (SSL) and Transport Layer Security (TLS)", Washington University, Saint Louis, **(2007)**

[16] Kalmaz, D. **"**IPsec IKE Şifreleme Standartları", http://www.enderunix.org/docs/ipsec_ike.pdf, **(2006)**

[17] Yücel, N. "IPsec Nasıl", http://docs.comu.edu.tr/howto/ipsec-howto-theory.html, Ekim **(2008)**,

[18] Jain, R.: "IPsec", Washington University, Saint Louis, **(2007)**

[19] Arslan, M.: "Firewall", Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Bilgisayar Mühendisliği Bölümü", Haberleşme Temelleri Dersi Araştırma Ödevi, Aralık, **(2006)**

[20] ERYOL, G.: "Sanal Yerel Ağları (VLAN'lar) ve Uygulamaları", http://blog.csirt.ulakbim.gov.tr/?p=48, Aralık, **(2007)**

[21] Düyen, S.: "VPN (Virtual Private Network/Özel Sanal Ağ)", http://www.ozbilen.net/dokumanlar/VPN_virtual_private_network_sevgi_duyen.pdf, **(2006)**

[22] Jain, R.: "Virtual Private Networks", Washington University, Saint Louis, http://www.cse.wustl.edu/~jain/cse571-07/l_17vpn.htm, **(2007)**

[23] "VPN Technologies: Definitions and Requirements", VPN Consortium, http://www.vpnc.org/vpn-technologies.html, July, (**2008**)

[24] Butcher, D.; Li, X.; Guo, J. "Security Challenge and Defense in VoIP Infrastructures", **(2007)**

[25] Kim, J.; Yoon, S.; Won, Y.; Lee, J.: "VoIP Secure Communication Protocol satisfying Backward Compatibility" **(2007)**

[26] Abdelnur, H.; Cridlig, V.; State, R.; Festor, O.: "VoIP Security Assessment: Methods and Tools" **(2006)**

[27] Mihai,S.: "Voice over IP Security A Layered Approach", XMCO Partners, **(2008)**

[28] Baumann, R.; Cavin, S.;Schmidt, S.: "Voice Over IP - Security and SPIT", University of Berne, **(2006)**

[29] Bhupathiraju, G.: "Security aspects in Voice over IP systems", Master's Project, Rochester Institute of Technology, Department of Telecommunications Engineering and Technology, **(2006)**

[30] Hung, P.C.K,; Martin, M.V.: "Security Issues in VoIP Applications", University of Ontario Institute of Technology, Oshawa, Canada, May **(2006)**

[31] Nascimento, A.; Passito, A.; Mota, E.; Nascimento, E.; Carvalho L.: "Can I Add a Secure VoIP Call?", Computer Science Department Federal University of Amazonas, Amazonas, Brazil, **(2006)**

[32] Cao, F.; Malik, S.: "Security Analysis and Solutions for Deploying IP Telephony in the Critical Infrastructure", Cisco Systems, INC, San Jose, CA, USA, **(2005)**

[33] Cao, F.; Jennings, C.: "Providing Response Identity and Authentication in IP Telephony", Cisco Systems, INC, San Jose, CA, USA, **(2006)**

[34] Chu, C.K.; Pant, H.; Richman, S.H.; Wu, P.: "Enterprise VoIP Reliability", 12th International Telecommunications Network Strategy and Planning Symposium, New Delhi, **(2006)**

[35] Alfonsi, B.: "Alliance Addresses VoIP Security", IEEE Computer Society, **(2005)**

[36] Feng Cao; Malik, S.: "Vulnerability analysis and best practices for adopting IP telephony in critical infrastructure sectors**",** Cisco Systems, Inc., April , **(2006)**

[37] Marshall, W.; Faryar, A.F.; Kealy, K.; de los Reyes, G.; Rosencrantz, I.; Rosencrantz, R.; Spielman, C.: "Carrier VoIP Security Architecture", 12th International Telecommunications Network Strategy and Planning Symposium, **(2006)**

[38] Sakhardande, R.R.: "The Use of Modelling and Simulation to Examine Network Performance under Denial of Service Attacks", Master of Science, State University of New York, Institute of Technology, Utica, NY, March, **(2008)**

[39] Gowda, S.B.: "Simulation of Voice Over Internet Protocol Service Performance When Overlaid With Background Traffic Over A Local Area Network", Master of Science, California State University, Long Beach, January, **(2008)**

[40] Qu, H.:, "Integrated Wireless-Based Information Processing and Communications for E-Healthcare Sysytem: Design, Analysis, Optimization and Resourse Protection", *PhD Thesis*, Wayne State University, Detroit, Michigan, **(2007)**

[41] Pandey, S.: "Secure Localization and Node Placement Strategies for Wireless Networks", *PhD Thesis,* Auburn University, Alabama, August, **(2007)**

[42] Dorleus, J.[a] ; Holweck,R.[a]; Ren, Z.[b]; Li,H.[b]; Cui,H.[b]; Medina,J.[c]: "Modeling and Simulation of Fading and Pathloss in OPNET for Range Communications", (a)US Army PEO STRI, Orlando, Florida, (b)L.C. Pegasus Corporation,New Jersey, CWSMR, New Mexico, **(2007)**

[43] Yang, K.; Ma, J.: "Implementation of IEEE802.1x in OPNET", 7th Intl. Conf. on Sys. Simulation and Scientific Computing, **(2008)**

[44] Li, L.; Zhu, L.; Wu, S.: "Design on The Simulation Platform for Mobility Management in LEO Satellite Network Based on OPNET", **(2007)**

[45] Fras, M.; Mohorko, J.: "Estimating the parameters of measured self similar traffic for modeling in OPNET", Faculty of Electrical Engineering and Computer Science, University of Maribor, Maribor, Slovenia, **(2007)**

[46] Mohorko, J.; Fras, M.; Cucej, Z.: "Modeling methods in OPNET simulations of Tactical Command and Control Information Systems", Faculty of Electrical Engineering and Computer Science, University of Maribor, Maribor, Slovenia, June, **(2007)**

[47] Boltjes,B.; Thiele,F.; Diaz,F.: "Credibility and Validation of Simulation Models for Tactical IP Networks", Military Communications Conference, **(2006)**

[48] Kelly, T. "*VoIP For Dummies*", Wiley Publishing, Inc., Indianapolis,USA. **(2005)**

[49] Wallingford, T.; "*VoIP Hacks*" O'Reilly Media, Sebastopol,USA **(2005)**

[50] http://www.voipsa.org/Resources/tools.php, (Son Erişim Tarihi: Şubat **2009**)

[51] http://www.hackingvoip.com/sec_tools.html, (Son Erişim Tarihi: Şubat **2009**)

[52] http://www.voipsa.org/About/, (Son Erişim Tarihi: Şubat **2009**)

[53] http://www.opnet.com/university_program/participant_spotlight/universities.html, (Son Erişim Tarihi: Şubat **2009**)

[54] http://www.mm.anadolu.edu.tr/eee/Pc%20Lab.html, (Son Erişim Tarihi: Şubat **2009**)

[55] http://netlab.boun.edu.tr/projects/projects.htm, (Son Erişim Tarihi: Şubat **2009**)

[56] http://fens.sabanciuniv.edu/telecom/eng/software/OPNETatSabanci University/OPNET_TE404.htm (Son Erişim Tarihi: Şubat **2009**)

[57] http://www.oxid.it/cain.html (Son Erişim Tarihi: Şubat **2009**)

[58] http://www.wireshark.org/ (Son Erişim Tarihi: Şubat **2009**)

[59] Kale, Ö.: Kişisel Görüşme (Toptel Telekomünikasyon), Aralık **(2008)**

[60] Ataytur, V.: Kişisel Görüşme (Tesan İletişim A.Ş.), Ekim **(2008)**

[61] Işınak, K.: Kişisel Görüşme (Boyut Çağrı Merkezi Hizmetleri A.Ş.), Ekim **(2008)**

[62] Alakavuk, Y.: Kişisel Görüşme (Grid Telekom), Nisan **(2008)**

ÖZGEÇMİŞ

Ceyhun ÇAKIR 29 Kasım 1984 tarihinde İstanbul'da doğdu. İlköğretimi Zuhal İlköğretim Okulu'nda, lise öğrenimini Kağıthane Profilo Anadolu Meslek Lisesi Elektronik Bölümü'nde tamamladı. 2002 yılında Marmara Üniversitesi Elektronik ve Haberleşme Öğretmenliği Bölümü'nü kazandı. 2006 yılında lisans eğitimini tamamladı. Aynı yıl Marmara Üniversitesi Fen bilimleri Enstitüsü Elektronik ve Haberleşme Eğitimi Bölümü'nde yüksek lisans eğitimi'ne başladı. 2005-2006 yılları arasında telekomünikasyon sektöründe hizmet veren AB Teknoloji ve 2006-2008 yılları arasında Vestel A.Ş'de çalıştı.