



YILDIZ TEKNİK ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

internet protokolü üzerinden ses..

Yüksek Lisans Tezi

serkan keskin

73-
12

**YILDIZ TEKNİK ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ**

**İNTERNET PROTOKOLÜ ÜZERİNDEN
SES İLETİMİNDE (VoIP) GÜVENLİK**

215

Elektronik ve Haberleşme Mühendisi Serkan KESKİN

FBE Elektronik ve Haberleşme Mühendisliği Anabilim Dalı Haberleşme
Programında Hazırlanan

YÜKSEK LİSANS TEZİ

Tez Danışmanı :Yrd. Doç. Dr. Soner ÖZGÜNEL (YTÜ)

İSTANBUL, 2007

YILDIZ TEKNİK ÜNİVERSİTESİ
KÜTÜPHANE VE DOKÜMANTASYON
DAİRE BAŞKANLIĞI

Yer No (DDC) : R-373-142

Kayıt No : 3584

Geldiği Yer : Fen Bilimleri
Enstitüsü

Tarih : 05.12.2007

Fiyat : 6.95

Fatura No : İNTE

Ayniyat No : 23

Ek :

YILDIZ TEKNİK ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

XIII - 139

İNTERNET PROTOKOLÜ ÜZERİNDEN
SES İLETİMİNDE (VoIP) GÜVENLİK

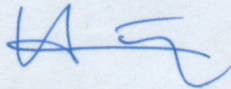
Elektronik ve Haberleşme Mühendisi Serkan KESKİN

FBE Elektronik ve Haberleşme Mühendisliği Anabilim Dalı Haberleşme
Programında Hazırlanan

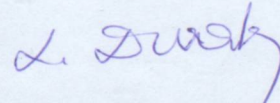
YÜKSEK LİSANS TEZİ

Tez Danışmanı : Yrd. Doç. Dr. Soner ÖZGÜNEL (YTÜ)

Yrd. Doç. Dr. Soner ÖZGÜNEL



Yrd. Doç. Dr. Lutfiye Durak



Yrd. Doç. Dr. M. Elif Karsligil
E. Karsligil

İSTANBUL, 2007

İÇİNDEKİLER

Sayfa

KISALTMA LİSTESİ.....	v
ŞEKİL LİSTESİ	vii
ÇİZELGE LİSTESİ.....	x
ÖNSÖZ.....	xi
ÖZET	xii
ABSTRACT	xiii
1. GİRİŞ.....	1
2. VERİ İLETİŞİMİ TEMEL KAVRAMLARI.....	3
2.1 Katman Kavramı ve Protokoller.....	3
2.2 Açık Sistemler Bağlantısı (OSI-Open Systems Interconnection) Referans Modeli	5
2.3 TCP/IP (Transmission Control Protocol/Internet Protocol) Referans Modeli	8
2.3.1 Aktarım Denetim Protokolü (TCP-Transmission Control Protocol)	10
2.3.2 Kullanıcı Datagram Protokolü (UDP-User Datagram Protocol).....	11
2.3.3 İnternet Protokolü (IP-Internet Protocol)	12
2.3.4 Gerçek Zamanlı Taşıma Protokolü (RTP-Real Time Transport Protocol)	13
2.3.5 Gerçek Zamanlı Taşıma Kontrol Protokolü (RTCP-Real-time Transport Control Protocol)	15
3. İNTERNET PROTOKOLÜ ÜZERİNDEN SES İLETİMİ (VOICE OVER IP) ..	16
3.1 VoIP'in Kullanım Alanları ve Entegrasyonu	17
3.2 H.323 Protokolü	21
3.2.1 H.323 Protokol Yığını	21
3.2.2 H.323 Bileşenleri.....	22
3.2.3 H.323 Mesajları	24
3.2.4 H.323 Protokol Versiyonları	26
3.3 Oturum Başlatma Protokolü (SIP-Session Initiation Protocol).....	29
3.3.1 SIP Bileşenleri.....	30
3.3.2 SIP Sunucuları	30
3.3.3 SIP Mesajları	31
3.3.4 SIP İsimleri ve Adresleri	35
3.3.5 SIP Çağrı Kurulumu	35
3.4 SIP ve H.323 Protokollerinin Karşılaştırılması	36
4. VOIP TEKNOLOJİSİNİN GÜVENLİK AÇIKLARI	38
4.1 Servis Reddi Saldırıları (DoS- Denial of Service Attacks)	38
4.2 İnternet Telefonculuğu Üzerinden Spam (SPIT-Spam over Internet Telephony). 42	
4.3 Ağ ve Medya Güvenlik Açıkları	42

4.4	IP ve Yazılımsal Telefonların (Softphone) Güvenlik Açıkları.....	43
4.5	SIP Protokolü Güvenlik Açıkları	44
4.5.1	Kayıt Sahteciliği (Registration Hijacking)	44
4.5.2	Proxy Taklit Etme (Proxy Impersonation)	46
4.5.3	Mesaj Değiştirme (Message Tampering)	47
4.5.4	SIP Oturumu Sonlandırma (SIP Session Tear Down).....	48
4.6	H.323 Protokolü Güvenlik Açıkları	48
5.	İNTERNET PROTOKOLÜ ÜZERİNDEN SES İLETİMİNDE GÜVENLİK.....	50
5.1	Veri Şifreleme (Kriptoloji) Metotları	50
5.1.1	Veri Şifrelemeye Giriş.....	52
5.1.2	Simetrik Şifreleme Algoritmaları	56
5.1.3	Asimetrik Şifreleme Algoritmaları.....	61
5.1.3.1	Diffie-Hellman Anahtar Anlaşma/Takas Metodu	65
5.1.3.2	RSA (Rivest Shamir Adleman) Şifreleme Algoritması	67
5.1.4	Özetleme/Karma Algoritmaları (Digest/Hash Algorithms)	70
5.1.5	Anahtar Anlaşma/Takas Metotları (Key Agreements/Exchange Methods).....	73
5.1.5.1	Ön-Paylaşımlı Anahtar Anlaşma Metodu (PSK-Pre-Shared Key Agreement).....	74
5.1.5.2	Açık Anahtar Altyapısı (PKI – Public Key Infrastructure)	75
5.1.6	Anahtar Yönetim Protokolleri (Key Management Protocols).....	76
5.1.6.1	İnternet Güvenlik İlişkisi ve Anahtar Yönetim Protokolü (ISAKMP- The İnternet Security Association and Key Management Protocol)	77
5.1.6.2	İnternet Anahtar Takası (IKE- İnternet Key Exchange).....	77
5.1.6.3	Çoklu Ortam İnternet Anahtarlama (MIKEY-Multimedia İnternet Keying).....	78
5.1.7	Güvenlik Protokolleri	80
5.1.7.1	Güvenli Gerçek Zamanlı Taşıma Protokolü (SRTP-Secure Real-Time Transport Protocol).....	81
5.1.7.2	İnternet Protokolü Güvenliği (IPSec-IP Security).....	84
5.1.7.3	Ulaşım Katmanı Güvenliği (TLS-Transport Layer Security)	93
5.2	Güvenlik Duvarı (Firewall) ve Ağ Adres Çevrimi (NAT-Network Address Translation) Uygulamaları	99
5.2.1	Güvenlik Duvarı (Firewall).....	100
5.2.2	Ağ Adres Çevrimi (NAT-Network Address Translation)	103
5.2.3	Güvenlik Duvarı/NAT ve VoIP Problemleri.....	104
5.2.4	VoIP’te Güvenlik Duvarı/NAT Problemlerinin Çözüm Yöntemleri	107
5.2.4.1	Uygulama Düzeyinde Ağ Geçitleri (ALG- Application Level Gateways)	107
5.2.4.2	Merkezi Cihaz (MiddleBox) Çözümleri.....	108
5.2.4.3	Oturum Sınır Denetleyicisi (SBC-Session Border Controllers).....	109
5.2.5	NAT Problemi Çözüm Yöntemleri	110
5.2.5.1	UDP’nin NAT Üzerinden Basit Geçişi (STUN- Simple Traversal of UDP through NATs)	111
5.2.5.2	Röle Kullanımı ile NAT Geçişi (TURN-Traversal Using Relay NAT).....	112
6.	VoIP GÜVENLİK PROTOKOLLERİ İLE İLGİLİ UYGULAMALAR	114
6.1	Uygulama 1: Ağ Geçitleri Kullanılarak Gerçekleştirilen Basit Bir VoIP Senaryosu	114
6.2	Uygulama 2: Ortadaki Adam Saldırısı ile VoIP Görüşmelerinin Gizli Dinlenmesi.....	116
6.3	Uygulama 3: SRTP Protokolü Uygulaması.....	121
6.4	Uygulama 4: IPSec Protokolü Uygulaması.....	122
7.	ŞİFRELEME ALGORİTMALARININ PERFORMANS ANALİZİ	128

7.1	IPSec Güvenlik Protokolünün Ses İletimi Üzerindeki Olumsuz Etkileri.....	128
8.	SONUÇLAR	134
	KAYNAKLAR.....	137
	ÖZGEÇMİŞ	139

KISALTMALAR LİSTESİ

3DES	Triple Data Encryption Standard
AES	Advanced Encryption System
AH	Authentication Header
ALG	Application Level Gateway
ASCII	American Standard Codes for Information Interchange
ASN.1	Abstract Syntax Notation One
ATM	Asynchronous Transfer Mode
DARPA	Defense Advanced Research Projects Agency
DDoS	Distributed Denial-of-Service
DES	Data Encryption Standard
DoS	Denial-of-Service
ESP	Encapsulating Security Payload
FTP	File Transfer Protocol
HDL	High Level Data Link Control
HMAC	Hashed Medium Access Control
HTTP	Hyper Text Transfer Protocol
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
IP	Internet Protocol
IPSec	Internet Protocol Security
ISAKMP	The Internet Security Association and Key Management Protocol)
ISO	International Standard Organization
ITU-T	International Telecommunication Union-Telecommunication
LAN	Local Area Network
MAC	Message Authentication Code
MD5	Message-Digest algorithm 5
MEGACO	Media Gateway Control
MG	Media Gateway
MGC	Media Gateway Controller
MGCP	Media Gateway Control Protocol
MIKEY	Multimedia Internet Keying
MIME	Multipurpose Internet Mail Extension
NAT	Network Address Translation
NAPT	Network Address Port Translation
NGN	Next Generation Networks
OSI	Open Systems Interconnection
PBX	Private Exchange Branch
PKI	Public Key Infrastructure
PSK	Pre-Shared Key Agreement
PSTN	Public Switched Telephone Network
QoS	Quality-of-Service
RAS	Registration, Admission and Status
RC2	Rivest's Code 2
RC4	Rivest's Code 4
RC5	Rivest's Code 5
RSA	Rivest, Shamir and Adleman
RTCP	RTP Control Protocol
RTP	Real-Time Transport Protocol
SA	Security Association
SBC	Session Border Controllers

SDP	Session Description Protocol	5
SDLC	Synchronous Data Link Control	6
SHA	Secure Hash Algorithm	7
SIP	Session Initiation Protocol	8
S/MIME	Secure Multipurpose Internet Mail Extension	9
SNMP	Simple Network Management Protocol	10
SPD	Security Policy Database	11
SPI	Secure Parameter Index	12
SRTP	Secure RTP	12
SS7	Signaling System 7	13
SSL	Secure Socket Layer	14
STUN	Simple Traversal of UDP through NAT	14
TCP	Transmission Control Protocol	18
TFTP	Trivial File Transport Protocol	19
TLS	Transport Layer Security	19
TURN	Traversal Using Relay NAT	22
UA	User Agent	23
UDP	User Datagram Protocol	23
UTP	Unshielded Twisted Pair	25
VLAN	Virtual LAN	31
VoIP	Voice over Internet Protocol	31
VPN	Virtual Private Network	33
WAN	Wide Area Network	34
WLAN	Wireless LAN	34
Şekil 3.9	Temel SIP çağrı kurulumu (Orriblad, 2004)	35
Şekil 3.10	Proxy sunucu üzerinden SIP çağrı kurulumu (Orriblad, 2004)	36
Şekil 3.11	TCP bağlantısının kurulumu	40
Şekil 3.12	SYN saldırısı ve saldırı	40
Şekil 3.13	Denetimli taşıma saldırısı (Porter vd., 2006)	41
Şekil 3.14	Çizgi saldırısı (Won, 2006)	43
Şekil 3.15	Kayıp paketler (Kuhn ve Ashraf, 2005)	44
Şekil 3.16	Kayıp saldırısında saldırıya uğrayan SIP sunucuları arasındaki mesajlaşma	46
Şekil 3.17	Proxy saldırısı (Kuhn ve Ashraf, 2005)	47
Şekil 3.18	SIP sunucuları arasındaki saldırı (Won, 2006)	48
Şekil 3.1	İki yönlü bir saldırıya karşı şifrelemenin kullanılması (Thalhammer, 2000)	53
Şekil 3.2	Temel kriptoloji mekanizması (Thalhammer, 2000)	54
Şekil 3.3	Blök şifreleme (Kurt, 2001)	57
Şekil 3.4	DİE algoritması (Kurt, 2001)	58
Şekil 3.5	3DES algoritması (Kurt, 2001)	60
Şekil 3.6	Sembolik ve asimetrik şifreleme algoritmalarında anahtar yapısı	62
Şekil 3.7	Açık anahtar mekanizması (Kuhn, 2005)	64

ŞEKİL LİSTESİ

Şekil 2.1	Ağlarda katman kavramı (Baykal, 2001).....	5
Şekil 2.2	OSI referans modelinde katmanlar aracılığı ile veri aktarımı (Baykal, 2001) ...	8
Şekil 2.3	TCP/IP katmanları (Baykal, 2001)	9
Şekil 2.4	TCP segmenti.....	11
Şekil 2.5	Katmanlar arası bilgi akışı (Baykal, 2001)	12
Şekil 2.6	IP datagramı (Baykal, 2001).....	13
Şekil 2.7	RTP mesaj formatı.....	14
Şekil 3.1	VoIP bileşenleri ve entegrasyonu (Won, 2006).....	18
Şekil 3.2	IP üzerinden ses iletim aşamaları (Kuhn ve Thomas, 2005)	19
Şekil 3.3	H.323 protokol yığını	22
Şekil 3.4	H.323 bileşenleri.....	23
Şekil 3.5	H.323 mesajları ve çağrı kurulumu	25
Şekil 3.6	SIP bileşenleri.....	31
Şekil 3.7	Örnek bir SIP istek mesajı	33
Şekil 3.8	Örnek bir SIP cevap mesajı	34
Şekil 3.9	Temel SIP çağrı kurulumu (Orrblad, 2004).....	35
Şekil 3.10	Proxy sunucu üzerinden SIP çağrı kurulumu (Orrblad, 2004)	36
Şekil 4.1	TCP bağlantısının kurulması	40
Şekil 4.2	SYN baskını saldırısı	40
Şekil 4.3	Dağıtılmış DoS saldırısı (Porter vd., 2006)	41
Şekil 4.4	Gizli dinleme (Won, 2006).....	43
Şekil 4.5	Kayıt sahteciliği (Luthra ve Ashraf, 2005)	44
Şekil 4.6	Kayıt sahteciliğinde saldırganla SIP sunucusu arasındaki mesajlaşma.....	46
Şekil 4.7	Proxy taklit etme (Luthra ve Ashraf, 2005).....	47
Şekil 4.8	SIP oturumu sonlandırma saldırısı (Won, 2006)	48
Şekil 5.1	Hattı dinleyen bir saldırgana karşı şifrelemenin kullanılması (Thalhammer, 2000).....	53
Şekil 5.2	Temel kriptoloji mekanizması (Thalhammer, 2000)	54
Şekil 5.3	Blok şifreleme (Kurt, 2001).....	57
Şekil 5.4	DES algoritması (Kurt, 2001).....	58
Şekil 5.5	3DES algoritması (Kurt, 2001).....	60
Şekil 5.6	Simetrik ve asimetrik şifreleme algoritmalarında anahtar yapısı	62
Şekil 5.7	Açık anahtar mekanizması (Kultti, 2005).....	64

Şekil 5.8	Diffie-Hellman anahtar anlaşma/takas metodu (Kultti, 2005)	67
Şekil 5.9	RSA asimetrik şifreleme algoritması (Porter vd., 2006)	69
Şekil 5.10	Ön-Paylaşımlı anahtar anlaşma metodu (Kultti, 2005)	74
Şekil 5.11	X.509 standardına uygun bir sertifika örneği (Tübitak UEKAE, 2006).....	76
Şekil 5.12	MIKEY anahtar yönetim protokolü (Orrblad, 2004).....	80
Şekil 5.13	SRTP protokolü paket yapısı (Baugher ve McGrew, 2004).....	83
Şekil 5.14	OSI referans modelinde IPSec protokolünün yeri (Orrblad, 2004).....	84
Şekil 5.15	IPSec AH başlık formatı (Orrblad, 2004).....	87
Şekil 5.16	IPSec ESP başlık formatı (Orrblad, 2004).....	89
Şekil 5.17	IPSec tünel ve ulaşım modları (Kuhn ve Thomas, 2005).....	90
Şekil 5.18	TLS protokolü istemci/sunucu modeli (Dierks ve Allen, 1999).....	94
Şekil 5.19	TLS protokolü katmanları (Dierks ve Allen, 1999)	95
Şekil 5.20	TLS protokolü mesaj akış şeması (Dierks ve Allen, 1999).....	97
Şekil 5.21	Basit bir güvenlik duvarı uygulaması (Porter vd., 2006).....	101
Şekil 5.22	Güvenlik duvarı ve NAT arkasında bulunan IP telefonlar (Kuhn ve Thomas, 2005)	105
Şekil 5.23	Basit bir NAT uygulaması (Porter vd., 2006)	106
Şekil 5.24	Uygulama Düzeyinde Ağ Geçidi (ALG- Application Level Gateway)	107
Şekil 5.25	VoIP'te Merkezi cihaz senaryosu (Kuhn ve Thomas, 2005).....	109
Şekil 5.26	Oturum Sınır Denetleyicisi (SBC-Session Border Controller).....	109
Şekil 5.27	Farklı VoIP ağlarının SBC'lerle birbirine entegrasyonu (Porter vd., 2006)...	110
Şekil 5.28	UDP'nin NAT Üzerinden Basit Geçişi (STUN) (Porter vd., 2006)	111
Şekil 5.29	Röle Kullanımı ile NAT Geçişi (TURN) (Porter vd., 2006)	113
Şekil 6.1	SIP protokolü konuşan iki ağ geçidinden oluşan basit bir VoIP senaryosu ...	114
Şekil 6.2	Ağ geçitlerinin telefon numaralarının belirlenmesi.....	115
Şekil 6.3	Ağ geçitlerinin adres tablolarının belirlenmesi.....	116
Şekil 6.4	Ortadaki adam saldırısı senaryosu	117
Şekil 6.5	Ethereal programı ile VoIP görüşmelerini kaydetme_1	118
Şekil 6.6	Ethereal programı ile VoIP görüşmelerini kaydetme_2	118
Şekil 6.7	Ethereal programı ile VoIP görüşmelerini kaydetme_3	119
Şekil 6.8	Ethereal programı ile VoIP görüşmelerini kaydetme_4	119
Şekil 6.9	Ethereal programı ile VoIP görüşmelerini kaydetme_5	120
Şekil 6.10	Ethereal programı ile VoIP görüşmelerini kaydetme_6	120
Şekil 6.11	Ağ geçitlerinde SRTP protokolünü aktif etme	121
Şekil 6.12	SRTP protokolü aktif edilmiş ağ geçitleri arasındaki RTP paket akışı	122

Şekil 6.13	Ağ geçitlerinde IPSec protokolünü aktif etme.....	124
Şekil 6.14	Ağ geçitlerinde tanımlanması gereken IKE protokolü parametreleri.....	124
Şekil 6.15	Ağ geçitlerinde tanımlanması gereken IPSec protokolü parametreleri	126
Şekil 6.16	IPSec protokolü aktif edilmiş ağ geçitleri arasındaki mesajlaşma	126
Şekil 6.17	IKE protokolünün ilk fazında gerçekleşen mesajlaşma.....	127
Şekil 7.1	IPSec protokolünün paket yükü üzerine etkisi (Barbieri ve Bruschi, 2005) ..	129
Şekil 7.2	Şifreleme ve doğrulama algoritmalarının işlem hızı üzerine etkileri (Barbieri ve Bruschi, 2005)	133

ÇİZELGE LİSTESİ

Çizelge 3.1	H.323 ve SIP protokollerinin karşılaştırılması	37
Çizelge 5.1	Farklı hızdaki bilgisayarların farklı anahtar uzunluğundaki şifreleri çözme süreleri	54
Çizelge 5.2	Simetrik şifreleme algoritmalarının karşılaştırılması	61
Çizelge 5.3	Simetrik ve asimetrik şifreleme algoritmalarının karşılaştırılması.....	65
Çizelge 5.4	SHA algoritmalarının karşılaştırılması	73
Çizelge 7.1	IPSec protokolünün eş zamanlı çağrı adedi üzerindeki etkisi	130
Çizelge 7.2	Şifreleme ve doğrulama algoritmalarının çağrı kurulum süresi üzerine etkileri	132

ÖNSÖZ

Tez çalışmamda benden yardımlarını ve desteğini hiçbir zaman eksik etmeyen değerli hocam Sayın Yrd. Doç. Dr. Soner ÖZGÜNEL'e teşekkürü bir borç bilirim. Ayrıca manevi desteğini her zaman bana hissettiren ve bana sürekli motivasyon veren sevgili Anneme her zaman yanımda olduğu için teşekkür ederim.

Buğün bu çalışmada zorluklarının yanı sıra, VoIP'in aşması gereken çeşitli problemler de bulunmaktadır. Bu problemlerin en önemlisi güvenlik konusudur. VoIP teknolojisi henüz bir süre önce geliştirilen bir güvenlik problemi de getirmektedir. VoIP trafiği kötü niyetli kişi tarafından ele geçirilebilir, kopyalanabilir, yavaşlatılabilir veya değiştirilebilir. Bununla birlikte, VoIP uygulamalarının sebep olduğu güvenlik açıkları ağ seviyelerine değeri olduğu zararlar vermektedir.

Bu çalışmada, VoIP teknolojisinin beraberinde getirdiği güvenlik tehditlerine neler olduğu, VoIP uygulamaları karşı gerçekleştiren saldırıların muhtemel sonuçları, bu saldırılara karşı ne gibi önlemler alınabileceği, güvenlik amaçlı kullanılacak şifreleme algoritmalarına ve güvenlik protokollerine değinilmiştir. Sonrasında, bu güvenlik tehditlerine karşı alınabilecek güvenlik protokollerinin önemini gösteren uygulamalar gerçekleştirilmiştir. Bu uygulamalar neticesinde, güvenlik protokollerinin kullanılması durumunda VoIP uygulamaları nasıl etkileyeceği gerçekleştirilen saldırıların etkili olacağı, güvenlik protokollerinin etkili olacağı konusunda bu bu saldırıların başarısız olacağı gösterilmiştir. Son bölümde ise VoIP ve VoIP protokollerinin kullandığı şifreleme algoritmalarının VoIP görüşmelerini güvenli olarak etkileyecek şekilde bir performans analizi gerçekleştirilmiştir.

Analizler Kullandığı VoIP, H.323, SIP, VoIP teknolojisinin güvenlik açıkları, VoIP güvenlik protokollerini, DES, AES, MD5, IPSec, TLS, SRTP.

ÖZET

İnternet üzerinden ses iletimi (VoIP) son yıllarda çok popüler bir konu haline gelmiştir. Özellikle, ekonomik açıdan çeşitli avantajlara sahip olan VoIP, varolan internet altyapısını kullanması, herhangi bir ek maliyet getirmemesi ve kurulum ve operasyon maliyetlerinin düşük olması nedeniyle hem son kullanıcıların hem de işletmelerin oldukça ilgisini çekmektedir.

Bütün bu olumlu özelliklerinin yanında, VoIP'in aşması gereken çeşitli problemler de bulunmaktadır. Bu problemlerin en önemlisi güvenlik konusudur. VoIP teknolojisi beraberinde aynı hızda gelişen bir güvenlik problemini de getirmektedir. VoIP trafiği kötü niyetli biri tarafından engellenebilir, kopyalanabilir, yavaşlatılabilir veya değiştirilebilir. Bununla birlikte, VoIP uygulamalarının sebep olduğu güvenlik açıkları ağ şebekelerine önemli ölçüde zararlar verebilmektedir.

Bu çalışmada, VoIP teknolojisinin beraberinde getirdiği güvenlik tehditlerinin neler olduğuna, VoIP sistemlerine karşı gerçekleştirilen saldırıların muhtemel sonuçlarına, bu saldırılara karşı ne gibi önlemler alınabileceğine, güvenlik amaçlı kullanılabilecek şifreleme algoritmalarına ve güvenlik protokollerine değinilmiştir. Sonrasında, bu güvenlik tehditlerine karşı uygulanabilecek güvenlik protokollerinin önemini gösteren uygulamalar gerçekleştirilmiştir. Bu uygulamalar neticesinde, güvenlik protokollerinin kullanılmaması durumunda VoIP sistemleri hedef alınarak gerçekleştirilen saldırıların etkili olacağı; güvenlik protokollerinin aktif edilmesi durumunda ise bu saldırıların başarısız olacağı gösterilmiştir. Son bölümde ise VoIP güvenlik protokollerinin kullandığı şifreleme algoritmalarının VoIP görüşmeleri üzerindeki olumsuz etkilerinin incelendiği bir performans analizi gerçekleştirilmiştir.

Anahtar Kelimeler: VoIP, H.323, SIP, VoIP teknolojisinin güvenlik açıkları, VoIP güvenlik protokolleri, DES, AES, MD5, IPsec, TLS, SRTP.

ABSTRACT

Recently, Voice Over IP (VoIP) has been a very popular subject all over the world. VoIP presents more economical opportunities for both end users and the enterprises, because it can be integrated on the existing internet infrastructure, it does not need any further cost and decreases the setup and operational cost.

Despite of all these constructive features, there are some difficulties that VoIP must overcome. The most important difficulty is the security issue. The VoIP traffic can be blocked, copied, changed or made slow by malicious people. In addition, the vulnerabilities of VoIP applications can damage the network systems of enterprises.

In this study, security threats of VoIP, the possible results of these threats, the measures that can be taken against these threats and the most important security algorithms and protocols are investigated. Following this investigation, special applications that show the importance of these protocols are performed. At the end of these applications, it will be shown that the attacks against VoIP systems can be successful if the VoIP security protocols are disabled and then the attacks against VoIP systems are never successful if the VoIP security protocols are enabled. At the last section, a performance analyses that show negative effects of encryption algorithms on VoIP is performed.

Keywords: VoIP, H.323, SIP, Security vulnerabilities of VoIP, VoIP security protocols, DES, AES, MD5, IPSec, TLS, SRTP.

1. GİRİŞ

IP ağları artık sadece klasik veri iletiminde değil, ses ve hareketli görüntü (video) iletiminde de yaygın olarak kullanılmaktadır. Günümüzde yerel telekom operatörlerinin sunduğu klasik PSTN ses hizmetine alternatif olarak sunulan VoIP tabanlı ses hizmetleri, maddi anlamda kullanıcılara çok cazip gelmektedir. Bununla birlikte VoIP, firmaların kendi şubeleri arasında ücretsiz görüşebilmelerine imkan sağlaması sebebiyle de günümüzde çok yaygın olarak tercih edilmektedir.

Öncesinde sadece data hizmeti veren internet servis sağlayıcıları bugün data hizmeti yanında IP telefon iletişimi ile ilgilenmekte ve VoIP temelli servisler sunmaktadır. Ayrıca müşterilerine VoIP hizmeti vermek için yeni alternatif telekom operatörleri ortaya çıkmış ve bu operatörler ağlarını tümüyle IP temelli “Yeni Kuşak Ağ (NGN-Next Generation Networks)” mimarisine uygun olarak hazırlamışlardır. Kurumsal kullanıcılar için IP üzerinden ses iletişimi hemen hemen tek seçenek haline gelmiştir. Telekom teçhizat üreticileri geleneksel telefon haberleşmesi sistemlerini çoktan gündemlerinden çıkarmışlar ve Ar-Ge yatırımlarını tümüyle IP telefon temelli sistemlerin geliştirilmesine tahsis etmektedirler.

Tüm bu önemli gelişmelerin yanında çok önemli bir konu olan güvenlik konusu göz ardı edilmektedir. Bilindiği üzere genel ağ saldırılarını veri çalma, yok etme, değiştirme ve engelleme olmak üzere dört ana grupta incelemek mümkündür. Bugüne kadar veri ağlarında hep karşımıza bu dört saldırı tipinden biri çıkmıştır. VoIP’te bu bahsedilen saldırıların yanı sıra kaynak kullanımı gibi önemli bir saldırı da söz konusudur. Herhangi bir alternatif telekom operatörünün sistemini çökertmek, verileri silip sistemi kapatmak, trafiği engellemek ya da sahtecilik yaparak mevcut kaynaklarını kullanmak bu saldırılara örnek olarak verilebilmektedir. Hiçbir koruması olmayan bir operatörün sistemine girip gerekli tanımlamaları çalabilirseniz, artık bu operatöre doğru istediğiniz gibi trafik yollama şansına sahip olursunuz. Bu saldırılar ayrıca herhangi bir operatörden bağımsız kendi şubeleri arasında ücretsiz görüşme yapmak amaçlı kendi VoIP altyapısını kurmuş bir firma için de önemli bir güvenlik tehdidi olarak karşımıza çıkmaktadır.

Bu çalışmanın amacı, günümüzde yaygın olarak kullanılmakta olan ve gelecekte de büyük ölçüde klasik PSTN şebekelerinin yerini alacağı öngörülen VoIP teknolojisinin beraberinde getirdiği güvenlik tehditlerine ve bu güvenlik tehditlerine karşı alınabilecek önlemlerin neler olduğuna değinmektir.

Tezin ikinci bölümünde veri iletişimi temel kavramlarına genel bir bakış yapılmıştır. Üçüncü

bölümde ise VoIP teknolojisinin yapısı, işleyişi, kullanım alanları, entegrasyonu ve VoIP'te kullanılan protokoller hakkında genel bilgiler verilmiştir. Dördüncü bölümde VoIP teknolojisinin güvenlik açıklarına ve bu açıkların sebep olduğu güvenlik tehditlerinin neler olduğuna değinilmiştir.

Tezin beşinci bölümünde, bir önceki bölümde bahsedilen güvenlik tehditlerine karşı ne gibi önlemler alınabileceği, ne gibi şifreleme algoritmalarının ve güvenlik protokollerinin kullanılabileceği ve bu protokollerin genel özellikleri hakkında ayrıntılı bilgiler verilmiştir.

Altıncı bölümde, basit bir VoIP senaryosu gerçekleştirilerek bir önceki bölümde bahsedilen güvenlik protokollerinin kullanımının gerçekten ne kadar faydalı olduğunu gösteren çeşitli uygulamalar gerçekleştirilmiştir. Bu uygulamalar neticesinde, VoIP sistemlerine karşı gerçekleştirilebilecek muhtemel saldırıların VoIP güvenlik protokollerinin kullanımı ile nasıl başarısız olduğu açıkça görülmüştür. Yedinci bölümde, VoIP güvenlik protokollerinin kullandığı şifreleme algoritmalarının VoIP görüşmeleri üzerindeki olumsuz etkilerini gösteren bir performans analizi gerçekleştirilmiştir. Bu analiz neticesinde, farklı algoritmaların VoIP görüşmeleri üzerine farklı etkiler yaptıkları gözlemlenmiştir. Son bölümde ise elde edilen sonuçlar belirtilmiştir.

2.1. Kapsam, Kavramlar ve Protokoller

Protokoller VoIP sistemlerindeki öğeler arasındaki iletişimi sağlamak için kullanılmaktadır. Bir bilgisayar, bir terminal, bir ağ arayüzü ya da bir uzaktan algılama aygıtı olabilir. Bu öğeler birer cihaz, uygulama programları, donanım parçaları, veya tabiri caza birer yazılım ve donanım paketi olabilir. Genel bir tanıma yaparsak örneğin, bilgi gönderme ve alma işlemleri yapan birer cihaz, öğem ise bir ya da birden fazla öğelerden oluşan fiziksel bir

2. VERİ İLETİŞİMİ TEMEL KAVRAMLARI

İki sistem arasında veri iletişimini gerçekleştirmek için bu iki sistemin herhangi bir kablo ile birbirine ya da bir ağı bağlanması yeterli değildir. Bilgisayarlar, terminaller ve diğer veri işleme aygıtlarının birbirlerine veri gönderebilmeleri için yapmaları gereken işlemler oldukça fazladır. Örneğin, iki bilgisayar arasındaki dosya aktarım sürecini ele aldığımızda yapılması gereken temel işlevler aşağıdaki gibi özetlenebilir (Baykal, 2001):

- Kaynak bilgisayar ya doğrudan veri iletim yolunu etkin hale getirmelidir ya da istenen hedef bilgisayarın tanımlanması için iletişim ağını bilgilendirmelidir.
- Kaynak bilgisayar hedef bilgisayarın veri almaya hazır olup olmadığını öğrenmelidir.
- Kaynak bilgisayardaki dosya aktarımı uygulaması, hedef bilgisayardaki dosya yönetimi programının dosyayı almak ve depolamak için hazır olup olmadığını öğrenmelidir.
- İki bilgisayar arasındaki dosya formatları uyumlu değil ise iki bilgisayardan biri dönüştürme işlemi gerçekleştirmelidir.

Tüm bu işlemleri gerçekleştirebilmek için iki bilgisayar sistemi arasında üst düzey bir işbirliği gerekmektedir. Bu işbirliği bilgisayarlar arası iletişim olarak adlandırılmaktadır. Bilgisayarlar arası iletişimi tartışabilmek için iki önemli kavram vardır: Katmanlar ve protokoller.

Bu bölümde genel ağ yapısı, VoIP teknolojisinde kullanılan önemli protokoller, bir ağ yapısının temel iki modeli olan OSI (Open Systems Interconnection) referans modeli ve TCP/IP modeli ve önemli protokollerden, IP (Internet Protocol), UDP (User Datagram Protocol), TCP (Transmission Control Protocol), RTP (Real-Time Transport Protocol) ve RTCP (RTP Control Protocol) protokolleri hakkında temel bilgiler verilecektir.

2.1 Katman Kavramı ve Protokoller

Protokoller farklı sistemlerdeki ögeler arasındaki iletişimi sağlamak için kullanılmaktadır. Sistem bir bilgisayar, bir terminal, bir ağ geçidi ya da bir uzaktan algılama aygıtı olabilir. Bu ögelere örnek olarak, uygulama programları, dosya aktarım paketleri, veri tabanı yönetim sistemleri ve elektronik posta verilebilir. Genel bir tanım yapılırsa öge, bilgi gönderme ve alma işlevini yerine getiren birim, sistem ise bir ya da birden fazla ögeden oluşan fiziksel bir bütündür.

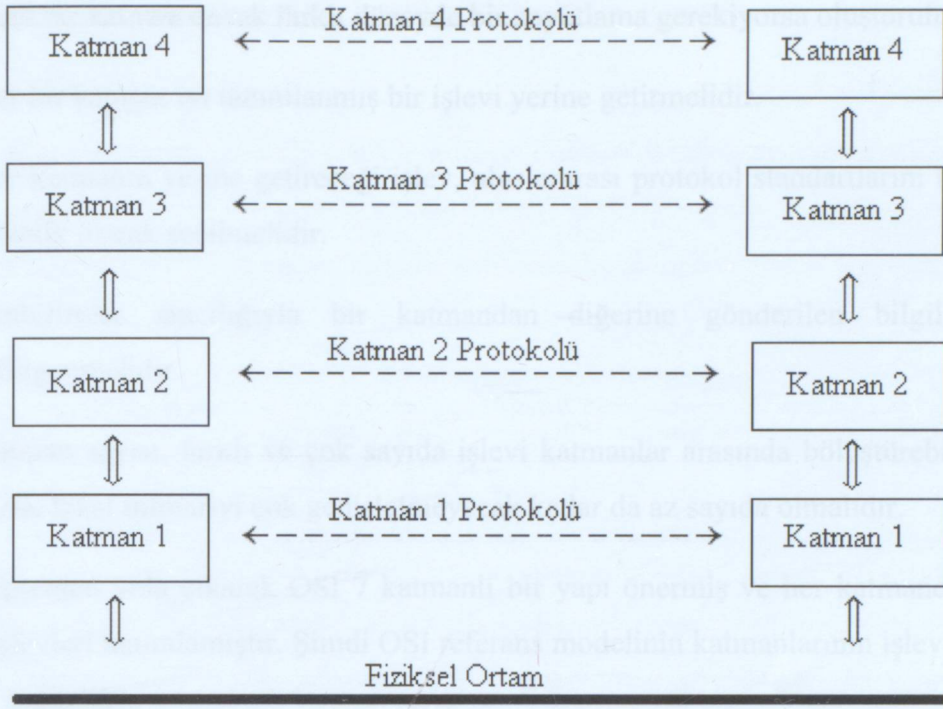
İki öğenin başarılı bir şekilde iletişim kurabilmesi için “aynı dili” konuşabilmesi gerekir. Nasıl ve ne zaman iletişim kurulacağının iki öge arasında kararlaştırılması gereklidir. Bunun için de öğelerin karşılıklı olarak birbirini anlayabileceği ortak bir dil olması gereklidir. Bu dil, protokoller aracılığı ile sağlanmaktadır. Protokoller, iki öge arasında veri değişiminin kurallarını belirler. Bir protokolün öncelikle belli bir sözdizimine sahip olması gerekir. Gönderilen işaretin düzeyi, verinin hangi formatta gönderileceği gibi unsurların belirli olması gerekir. İkinci olarak bir protokol, eşgüdüm ve hata saptama/düzeltilme yöntemlerini tanımlaması gerekir. Son olarak da, hız uyumu ve ardışık veri gönderme gibi zamanlama yöntemlerini belirlemesi gerekir (Baykal, 2001).

Sistem pek çok protokolün bulunduğu ve pek çok işlevi bir arada yerine getiren karmaşık bir yapıya ulaştığı anda, tasarımı kolaylaştırmak için soyutlama (abstraction) düzeyleri tanımlanabilir. Soyutlama kavramının 3 ögesi bulunmaktadır.

- Sistemin bazı önemli özelliklerini barındıran bütünleştirici bir model tanımlamak.
- Bu modeli sistemin başka bileşenlerinin erişebildiği bir ara yüze sahip bir nesne içerisine koymak.
- Bu nesnenin nasıl oluşturulduğunun detaylarını nesne kullanıcılarından saklamak.

Soyutlamalar ağlarda katmanlara karşılık gelir. Yani ağlar, genellikle katmanlar halinde düzenlenmiştir (Şekil 2.1). İki farklı ağdaki bilgisayarlar birbiri ile iletişime geçeceği zaman, bilgisayarların karşılıklı olarak birbirlerine denk gelen eş katmanları (aynı düzey katmanları) arasındaki protokollerin kullanımı ile iletişim sağlanır. Her protokolün farklı bir amacı vardır ve farklı işler yaparak iletişime olanak tanır. Ayrıca her protokolün kendine özgü sınırlamaları ve üstünlükleri vardır. Bazı protokoller birlikte çalışarak protokol yığınlarını oluştururlar. Bu katmanlar ve katmanlarda uygulanan protokollerin bütününe Ağ Mimarisi adı verilir.

Şekil 2.1’de ağ mimarisi şematik olarak gösterilmektedir. En altta veri aktarımının yapıldığı fiziksel ortam vardır. Bunun üzerinde katmanlar yer alır. Protokoller eş düzey katmanlar arasında ortak bir dil oluşturur. Ancak veri aktarımı sadece fiziksel ortamdan yapılabileceği için bu katmanlar arasında doğrudan bir iletişim yoktur. Bunun yerine her bir katman veriyi ve denetim bilgilerini bir altındaki katmana aktarır. Bitişik katmanlar arasındaki arabirimler, temel işlevleri ve servisleri sağlayarak bu aktarımı mümkün kılar.



Şekil 2.1 Ağlarda katman kavramı (Baykal, 2001)

2.2 Açık Sistemler Bağlantısı (OSI-Open Systems Interconnection) Referans Modeli

Uluslar arası protokol standardının ilk adımı, Uluslararası Standartlar Organizasyonu (ISO) tarafından 1979 yılında önerilmiş ve geliştirilmiştir. Bu standart Açık Sistemler Bağlantısı (OSI-Open Systems Interconnection) referans modeli olarak adlandırılır. Bu standardın bu şekilde adlandırılmasının nedeni açık sistemlerin (üreticiden bağımsız, farklı sistemler ile iletişim kurabilen sistemlere açık sistemler denir) birbirleri ile bağlantılarının nasıl olması gerektiği üzerine hazırlanmış olmasıdır.

OSI referans modeli veri haberleşmesi sürecinde yapılması gereken işlemleri katmanlar düzeyinde tanımlayan örnek bir yapıdır. Bu yapıda veri haberleşmesi için yapılması gereken tüm işlemler, birbirinden bağımsız olarak parçalara ayrılmış ve her parçaya ait görev tanımlamaları yapılmıştır. OSI, diğer tüm protokol ve standartların açıklanmasında örnek bir başvuru modeli olmuştur.

Protokollerin standartlaştırılmasındaki amaç, farklı sistemlerin birbirleri ile etkin ve doğru olarak etkileşimde bulunabilmelerine olanak sağlamaktır.

OSI referans modeli 7 katmandan oluşmaktadır. Katman kavramının oluşturulması ve katman sayısının belirlenmesinde temel alınan ilkeler şunlardır (Baykal, 2001):

1. Yeni bir katman ancak farklı düzeyde bir soyutlama gerekiyorsa oluşturulur.
2. Her bir katman iyi tanımlanmış bir işlevi yerine getirmelidir.
3. Her katmanın yerine getireceği işlev, uluslararası protokol standartlarını tanımlamaya yönelik olarak seçilmelidir.
4. Arabirimler aracılığıyla bir katmandan diğerine gönderilen bilgiler en aza indirgenmelidir.
5. Katman sayısı, farklı ve çok sayıda işlevi katmanlar arasında bölüştürebilecek kadar fazla, fakat mimariyi çok genişletmeyecek kadar da az sayıda olmalıdır.

Bu prensiplerden yola çıkarak OSI 7 katmanlı bir yapı önermiş ve her katmanda yapılması önerilen işlevleri tanımlamıştır. Şimdi OSI referans modelinin katmanlarının işlevlerinin neler olduğuna değinelim.

Fiziksel Katman: Fiziksel katman fiziksel ortam üzerinden ikilerin 1 ve 0 olarak aktarılmasından sorumludur. Bu katman, bir uçtaki gönderici sistem tarafından '1' mantıksal işareti gönderildiğinde, alıcı sistemin de bu işareti '1' olarak almasından yani, hatasız veri iletişimi kurabilmek için gereken yöntemlerden sorumludur. Fiziksel katman tamamen donanım ile ilgilidir ve tasarım çalışmaları büyük ölçüde elektriksel, mekanik arabirimler ve fiziksel iletişim ortamı ile ilgilidir. Kablo, konnektör standartları bu katmanda uygulanır. UTP, RJ45, RS-232, V.35 bu katmanda çalışan bazı standartlardır.

Veri-Bağlantı Katmanı: Veri bağlantı katmanı gerekli eş zamanlama, hata ve akış denetimlerini sağlayarak fiziksel bağ üzerinden bilginin güvenli bir biçimde aktarılmasını sağlar. Bu katmanın asıl görevi, gönderilen veriyi iletişim hatalarından arındırılmış olarak fiziksel katmandan almak ve ağ katmanına göndermektir. Alıcı tarafta hatanın sezinlenmesi/düzeltilmesi, düzeltilemiyorsa doğrusunun elde edilmesi için gönderilenin uyarılması gibi işlevleri vardır. Gönderilen ya da alınan veri bloklarına çerçeve adı verilmektedir. HDLC, SDLC gibi protokoller bu katmanda çalışmaktadır.

Ağ Katmanı: Ağ katmanı alt ağlar arasında bağlantı kurulmasından, sürdürülmesinden ve sonlandırılmasından sorumludur. Bu katmanın temel görevi, paketlerin gönderici sistemden alıcı sisteme nasıl ulaştırılacağını belirlemektir. Bundan dolayı yönlendirme protokolleri bu katman düzeyinde çalışırlar. Yönlendirme, durağan bir tabloya bakılarak yapılabilir veya her oturumun başında belirlenebilir veya her bir paket için yeniden belirlenecek şekilde oldukça

dinamik bir yapıda olabilir. IP protokolü bu katmanda çalışır. Bu katmandaki veri bloklarına paket adı verilir.

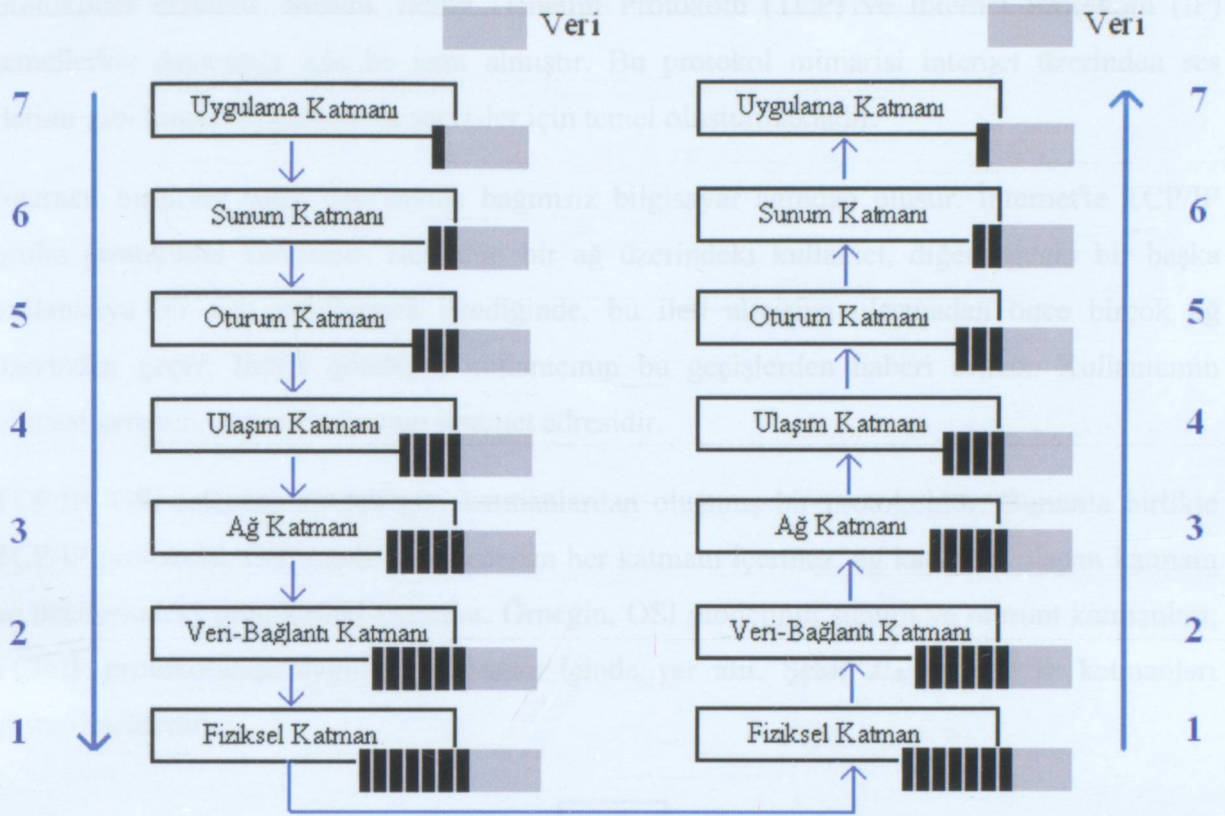
Ulaşım Katmanı: Ulaşım katmanının temel işlevi oturum katmanından verileri alıp, gerekirse küçük parçalara ayırarak ağ katmanına geçirmek ve karşı tarafa bu parçaların doğru bir şekilde ulaştığını sağlama almaktır. Ulaşım katmanı birçok ileti dizisini aynı kanal üzerinden çoklayarak iletmeye ek olarak, ağ üzerinden bağlantının kurulması ve kaldırılmasından sorumludur. Bu işlem çeşitli adlandırma (naming) ve bilgi akışını düzenleme (flow control) mekanizmaları gerektirir. Ulaşım katmanı ayrıca gelen verinin doğruluğunu kontrol eder ve verinin taşınması sırasında oluşan hataları ortaya çıkarır.

Oturum Katmanı: Oturum katmanı uygulamalar arasında oturum açma, sürdürme ve kapama görevini yerine getirerek uygulamalar arası iletişimi ve erişim denetimini sağlamaktadır. Bu katman farklı bilgisayarlardaki kullanıcıların birbirleri üzerinde bir oturum açmasını sağlar. Bir 'oturum', taşıma katmanının yaptığı gibi sıradan bir veri gönderimidir. Fakat oturum katmanında bazı uygulamalar için ileri düzey servisler de sunulmaktadır. Bir oturum uzaktaki zaman paylaşımlı bir bilgisayara erişmek veya iki bilgisayar arasında dosya transferi yapmak amacıyla kullanılabilir.

Sunum Katmanı: Sunum katmanı uygulamadan bağımsız olarak verinin geçirmesi gereken dönüşümleri (veri sıkıştırma, kod dönüşümü, şifreleme, şifre çözme vb.) gerçekleştirir. Bu katmana gelen paketler bilgi haline dönüştürülür. Yani sunum katmanı iletilen verinin sözdizimi (sentaks) ve semantiğiyle ilgilidir. EBCDIC-ASCII dönüşümleri bu katmanda gerçekleşir.

Uygulama Katmanı: Uygulama katmanı kullanıcıya en yakın katmandır. Kullanıcıların uygulama yazılımları, veri tabanları, elektronik posta, vb. programlar aracılığıyla OSI sistemine erişimini sağlar. Bu katmanda çok farklı terminallerin tanınmasını sağlayan protokoller gibi en sık kullanılan protokoller bulunur. Tüm sanal terminal yazılımları uygulama katmanı üzerinde bulunur. Dosya iletimi (FTP-File Transfer Protocol), e-posta, ağ yönetimi (SNMP-Simple Network Management Protocol) uygulamaları bu katmanda gerçekleşir.

Her katmanda bir ağ yazılımı belli ağ işlevlerini daha önceden belirlenmiş protokollere göre gerçekleştirir. Veri bir katmandan diğerine geçirilmeden (yukarıdan aşağıya) önce paketlere bölünür. Paketler bir katmandan diğerine sırasıyla geçirilirken o katmana ait başlıklar paketlerin önüne eklenir.



Şekil 2.2 OSI referans modelinde katmanlar aracılığı ile veri aktarımı (Baykal, 2001)

Alıcı tarafında paketler ters yönde ilerlerler (aşağıdan yukarıya). Her katmandaki yazılım paket üzerindeki bilgileri işler, ve üst katmana gönderir (Şekil 2.2). Paket uygulama katmanına ulaştığında alıcı tarafında anlaşılabilen özgün formuna dönmüş olur. Tüm bu işlemlere verinin kapsüllenmesi (Encapsulation) adı verilmektedir.

2.3 TCP/IP (Transmission Control Protocol/Internet Protocol) Referans Modeli

İnternet, 1973 yılında Amerika'nın İleri Savunma Araştırma Projeleri Ajansı (DARPA-Defense Advanced Research Projects Agency) tarafından bir araştırma projesi olarak başlamıştır. Buradaki amaç savunma ile ilgili projelerde bilgisayarların farklı ağlardaki diğer bilgisayarlarla haberleşebilmesini sağlamaktır. Bu amaçla ARPANET (Advanced Research Projects Agency Network) geniş alan ağı oluşturulmuş ve bu sayede Yerel Alan Ağlarının (LAN-Local Area Network) Geniş Alan Ağlarına (WAN-Wide Area Network) bağlanması kavramı ortaya çıkmıştır. Bu ağlar arasındaki uyumluluğu sağlamak amacıyla da TCP/IP (Transmission Control Protocol/ Internet Protocol) standardı geliştirilmiştir.

TCP/IP, farklı topoloji ve protokollere sahip ağları birbirlerine bağlamak için kullanılan bir

protokoller dizisidir. Sistem, İletim Denetim Protokolü (TCP) ve İnternet Protokolü (IP) temellerine dayandığı için bu ismi almıştır. Bu protokol mimarisi internet üzerinden ses iletimi gibi birçok uygulama ve servisler için temel oluşturmaktadır.

İnternet, birbirine bağlı çok sayıda bağımsız bilgisayar ağından oluşur. İnternet'te TCP/IP grubu protokoller kullanılır. Herhangi bir ağ üzerindeki kullanıcı, diğer ağdaki bir başka kullanıcıya bir ileti göndermek istediğinde, bu ileti alıcısına ulaşmadan önce birçok ağ üzerinden geçer. İletiyi gönderen kullanıcının bu geçişlerden haberi olmaz. Kullanıcının bilmesi gereken, yalnızca alıcının internet adresidir.

TCP/IP, OSI referans modeli gibi katmanlardan oluşmuş bir protokoldür. Bununla birlikte TCP/IP protokolü, OSI modelinde bulunan her katmanı içermez, ağ katmanı, ulaşım katmanı ve üzerlerindeki protokolleri tanımlar. Örneğin, OSI modelinin sunum ve oturum katmanları, TCP/IP protokolünde uygulama katmanı içinde yer alır. Şekil 2.3'de TCP/IP katmanları gösterilmektedir.

Uygulama	STMP	RLOGIN	FTP	TELNET	DOMAIN	TFTP
Ulaşım	TCP				UDP	
Yönlendirme (IP)	IP			ICMP		
Fiziksel (Ağ Ulaşım)	IEEE 802.2/LAPB/HDLC Ethernet, X.25, andaçlı halka, çevirmeli ağ vb.					

Şekil 2.3 TCP/IP katmanları (Baykal, 2001)

Bu protokoller kümesinde, fiziksel katman ve veri-bağlantı katmanı için herhangi bir tanım yapılmamıştır. Ağ içinde kullanılan diğer alt katman tanımlamaları geçerlidir. Örneğin bu katmanda IEEE 802 protokolleri, IBM andaçlı halka veya Ethernet protokolleri (10BASE-T, FDDI, ATM) kullanılabilir. Bu esneklik, kullanılan iletişim ortamına da yansır. Böylece herhangi bir fiziksel ortam, kablo kullanılmasına olanak tanır.

TCP/IP referans modelinin veri bağlantı ve fiziksel katmandan bağımsız olması, bu kadar sık kullanılmasının ve yaygınlaşmasının en önemli nedenlerinden biridir. Ayrıca, günümüzde UNIX gibi birçok işletim sistemi de TCP/IP protokol gruplarını hazır olarak içermektedir.

Sonuç itibariyle TCP/IP uygulamalarında 4 ayrı katman kullanılmaktadır:

- Uygulama protokolü (bunlar FTP, SMTP, Telnet gibi uygulama protokolleridir).
- TCP protokolü.
- IP protokolü.
- Fiziksel katman (Ağ ulaşım katmanı).

2.3.1 Aktarım Denetim Protokolü (TCP-Transmission Control Protocol)

TCP/IP referans modeline ismini veren TCP protokolü, bağlantılı (connection-oriented) ve güvenilir (reliable) bir iletişim sağlamaktadır. Buradaki "bağlantılı" ifadesi şu anlama gelmektedir: Bilgisayarlar iletişime geçmeden önce aralarında bir oturum açarlar. Oturumun açılması sırasında bilgisayarlar kendi iletişim parametrelerini birbirlerine iletirler. İletişim sırasında bu parametrelere göre hareket edilir. Güvenilir iletişim ise şu anlama gelmektedir: Bir bilgiyi karşı tarafa gönderdiğimizde karşı tarafın eline ulaştığından emin oluruz. Bu da gönderdiğimiz bilginin alındığına ilişkin bir onay mesajının (acknowledgement) bize gelmesi ile olmaktadır. Eğer belli bir süre içinde bu mesajı alırsak bizden çıkan bilgi karşı tarafın eline geçmiş demektir. Ancak eğer belli bir süre içinde bu mesajı alamazsak gönderdiğimiz bilgi karşı tarafa ulaşmadı demektir. Bu durumda bilgi tekrar gönderilir.

TCP protokolünün başlıca görevleri şu şekildedir:

- Alıcı tarafa yollanan verilerin kayıtlarını tutmak.
- Uygulama katmanından gelen bilgiyi parçalara ayırmak.
- İletişim ortamında kaybolan veya hatalı yollanan verileri yeniden göndermek.
- Alıcıya ayrı sıralar halinde gelebilen parçaların doğru sırada ve hatasız olarak ulaşmasını sağlamak.

Bu protokol, kısaca parçaların alıcıya hatasız ve sıralı olarak ulaştırılmasından sorumludur. TCP, OSI referans modelinde anlatılan ulaşım katmanının işlevlerini yerine getirir. Bu katman, uçtan uca bağlantının sağlandığı ilk katmandır. TCP protokolü, iletiyi parçalara ayırdıktan sonra her birinin başına bir başlık ekler. Bu başlık gönderici kapısı, alıcı kapısı, sıra numarası, alındı onayı, vb. gibi çeşitli alanlar içerir (Şekil 2.4).

Kaynak Kapı Numarası				Alıcı Kapı Numarası				
Sıra Numarası								
Onay (Acknowledgement)								
Veri Offset	Ayrılmış	U R G	A C K	P S H	R S T	S Y N	F I N	Pencere (Window)
Sağlama Toplamı		Acil işareti (Urgent Pointer)						
Bilgi diğer 500 oktet								

Şekil 2.4 TCP segmenti

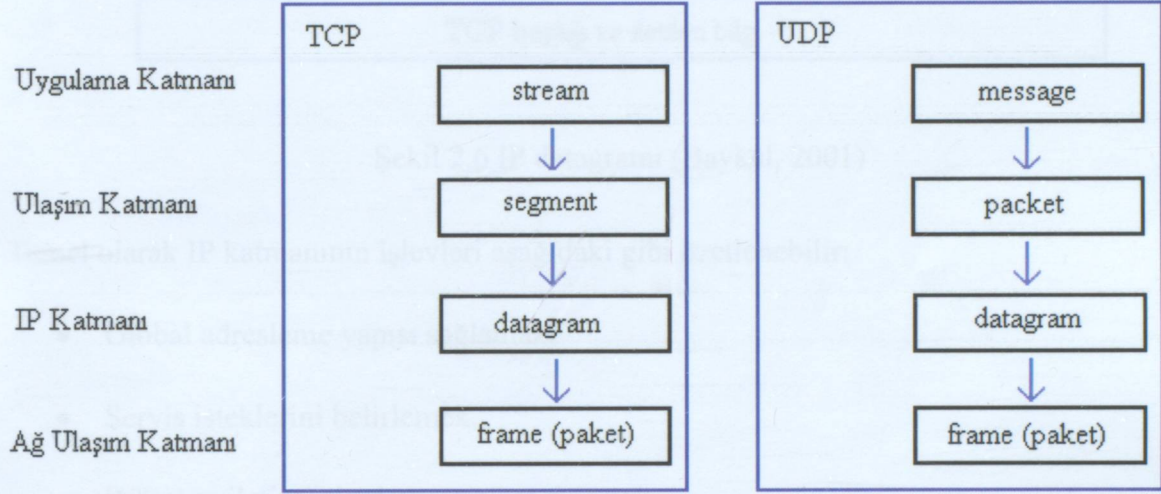
Kaynak kapı numarası, paketler gönderilmeden önce TCP protokolü tarafından her kullanıcıya verilmiş numaradır. Alıcı kapı numarası ise, iletişim kurulduğu zaman alıcı tarafındaki TCP tarafından verilen numaradır. Bu sayının, gönderici TCP tarafından bilinmesi gerekir. Bu nedenle iki nokta arasında iletişim kurulduğunda, kaynak noktasındaki TCP bu numarayı alıcıdan öğrenir ve parça başlıklarına yazar. Sıra numarası alanı ile her parçaya bir sıra numarası verilir. Bu numara ile karşı taraf, doğru parçayı eksiksiz alıp almadığını anlayabilir. Sağlama toplamı, parça içindeki tüm sekizliler (octet) toplanarak bulunur. Alıcı taraftaki TCP sağlama toplama hesabını yeniden yapar, eğer bilgi yolda bozulmamışsa kaynak noktasında hesaplanan sayı ile alıcıda hesaplanan sayı aynı çıkar.

2.3.2 Kullanıcı Datagram Protokolü (UDP-User Datagram Protocol)

TCP protokolü, bilgiyi parçalara bölen ve bu parçaları alıcı tarafında birleştiren bir protokoldür. Bazı uygulamalarda iletilen bilgiler, tek bir datagram içine sığabilecek büyüklüktedir. Bu tür uygulamalara örnek olarak, adres denetimini verebiliriz. Kullanıcılar, internet üzerindeki bir bilgisayara ulaşabilmek için o bilgisayarın adını kullanabilir. Sistem bağlantı kurmadan önce bu bilgisayar adını internet adresine çevirmek durumundadır, internet adreslerinin hangi adlara karşılık geldiği, belli bilgisayarlarda tablolar halinde tutulmaktadır, internet adresi, bu tablolardan sorgulanarak öğrenilebilir. Böyle bir sorgulama tek bir parçaya sığdırılabileceği için, TCP katmanının kullanılması gereksizdir. Bu gibi durumlarda en sık kullanılan protokol UDP'dir. UDP, uygulamalara bağlantı kurulmayan bir ulaşım katmanı işlevi sunar. Dolayısıyla TCP protokolündeki çoğu mekanizma UDP'de yoktur (bağlantı kurulumu, alındı bildirimi, tıkanıklık denetimi, vb.).

UDP, datagramların belirli sıralara konmasının gerekmediği uygulamalarda kullanılır. UDP protokolünün de kullandığı bir başlık vardır. Bu başlık, gönderilecek bilginin başına konur ve IP katmanına gönderilir. IP katmanı kendi başlık bilgisini ve protokol numarasını ekleyerek gönderir. UDP protokolünün TCP protokolünden farkı şu şekildedir: Bilgi datagramlara bölünmez ve yollanan paketlerin kaydı tutulmaz.

Şu ana dek anlatılan katmanları ve bilgi akışını Şekil 2.5'den görebiliriz.



Şekil 2.5 Katmanlar arası bilgi akışı (Baykal, 2001)

2.3.3 İnternet Protokolü (IP-Internet Protocol)

IP katman protokolü, datagramların yönlendirilmesinden sorumludur. OSI referans modelinin ağ katmanına karşılık gelir. Bu katman, ağlar arasında veri gönderiminin gerçekleştirilmesini sağlayan protokolleri içerir.

TCP katmanında parçalara ayrılan bilgi yönlendirilmek üzere IP katmanına yollanır. Bu katman parçanın içeriğiyle ilgilenmez, yalnızca bu parçayı gideceği adrese yollamakla yükümlüdür. Bunun için, öncelikle bir yol (rota) bulur. Yolun saptanmasından sonra kendi başlığını TCP'den gelen parçaya ekler. Bu başlığın da eklenmesiyle parça artık datagram olarak adlandırılır (Şekil 2.6). 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.

Sürüm	IHL	Servis tipi	Toplam uzunluk	
Tanımlama			Bayrak	Parça offset
Yaşam süresi (TTL)	Protokol		Başlık kontrol programı	
Kaynak adresi				
Varış adresi				
TCP başlığı ve iletilen bilgi				

Şekil 2.6 IP datagramı (Baykal, 2001)

Temel olarak IP katmanının işlevleri aşağıdaki gibi özetlenebilir:

- Global adresleme yapısı sağlamak.
- Servis isteklerini belirlemek.
- Parçaları iletim için datagramlara ayırmak.
- Alıcıda datagramları tekrar birleştirerek parçalar oluşturmak.

2.3.4 Gerçek Zamanlı Taşıma Protokolü (RTP-Real Time Transport Protocol)

RTP, gecikmeye karşı duyarlı olan gerçek zamanlı ses ve görüntü datalarını paket anahtarlama ağılarda taşımak amacıyla geliştirilmiş bir standarttır. RTP protokolü ilk defa 1996 yılında standartlaştırılmış ve 2001 yılında son halini almıştır.

RTP protokolü ses datalarını UDP protokolü üzerinden taşımaktadır yani, UDP portlarını ve UDP'nin çağullama ve başlık kontrol mekanizmalarını kullanmaktadır. RTP'nin diğer bir önemli özelliği ise çoklu ortam (multicast) uygulamalarında birden çok kullanıcının data transfer işlemini gerçekleştirebilmesidir.

RTP protokolünün sağladıkları başlıca şu şekildedir:

- Sıraya sokma.
- Zaman etiketleme.
- Kaynak belirleme.

RTP, UDP gibi bağlantısız (connectionless) 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. Şekil 2.7’de RTP başlığı ve mesaj formatı verilmiştir.

0	1	2	3	4-7	8	9	10-14	15	16	17-30	31
V=2	P	E		CC	M		PT			Dizi Numarası	
Zaman Damgası											
Senkronizasyon Kaynak Tanımlayıcısı (SSRC)											
Ek Kaynak Tanımlayıcısı (CSRC) (Değişken)											
Veri (Değişken)											

Şekil 2.7 RTP mesaj formatı

- **Versiyon (V):** RTP’nin sürüm numarasını belirtmektedir.
- **Dolgu (P):** Bu kısmın 1 olması çeşitli bit ekleme sekizlilerinin bulunduğunu gösterir.
- **Uzantı (E):** RTP başlığından sonra başka bir başlığın bulunduğunu gösterir.
- **Katılımcı Kaynağı Tanımlayıcısı (CC):** Mesajdaki ek kaynak tanımlayıcılarının sayısıdır.
- **İşaretleyici (M):** Veri akışının sınırlarını belirlemek için kullanılır.
- **Yük Tipi (PT):** Taşınan yükün türünü (G.729, JPEG gibi) belirtir.
- **Dizi Numarası:** Her RTP paketi yollandığında değeri 1 artan bir numaradır. Alıcı tarafta paketlerin tekrar sıralı bir şekilde birleştirilmesini sağlamaktadır.
- **Zaman Damgası:** Senkronizasyon ve jitter hesaplamaları için kullanılır.
- **Senkronizasyon Kaynak Tanımlayıcısı (SSRC):** Senkronizasyon kaynağını belirtir. Aynı oturumdaki senkronize olacak her kaynağın SSRC numarası farklıdır.
- **Ek Kaynak Tanımlayıcısı (CSRC):** CSRC listesi paket yüküne katkıda bulunan kaynakları tanımlar. Bu kaynakların sayısı CC alanında verilir. Eğer 15’den fazla ek katkı kaynağı varsa o durumda sadece 15 katkı kaynağına yer verilir.

RTP yapısını kısaca özetlemek gerekirse, her kaynağın bir SSRC numarası vardır. Eğer bu kaynaklar bir karıştırıcı yardımıyla tek bir veri akımına aktarılırlarsa bu veri akımı tek bir kaynak gibi davranacak ve tek bir SSRC numarasına sahip olacaktır. Bu veri akımında bulunan verilerin hangi kaynaklara ait olduğunu belirten kısım ise CSRC numaralarının bulunduğu CSRC listesidir ve bu listedeki kaynakların sayısı CC alanına yazılır. Böylece mesajların sonradan paketlere ayrıştırılması ve tekrardan birleştirilip doğru kaynağa yönlendirilmeleri de kolaylaşmış olur. Bu duruma ek olarak orijinal RTP kaynağının belirlenmesi amacıyla zaman damgası ve dizi numarası kullanılır. Böylece trafik uygun sırayla akacak ve eğer bir veya birden fazla PDU hatta kaybolursa senkronizasyon bozulmadan devam edebilecektir.

2.3.5 Gerçek Zamanlı Taşıma Kontrol Protokolü (RTCP-Real-time Transport Control Protocol)

RTCP protokolü, kontrol paketlerinin zaman zaman özel bir RTP oturumuna ilişkin paylaşımcılara iletimi için kullanılır. Bu kontrol paketleri paylaşımcılar hakkında (isimleri, genel adresleri gibi) 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).
- Taşıma denetleme.

RTCP protokolü başarımlı 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 Service) geri beslemesi yaptırabilir.

3. İNTERNET PROTOKOLÜ ÜZERİNDEN SES İLETİMİ (VOICE OVER IP)

VoIP (eş anlamlı olarak, IP Telefonculuğu) hizmeti, paket anahtarlama olarak internet üzerinden iletilen veri halindeki ses hizmetini kapsamakta ve bir veri iletişimi hizmeti olarak kabul edilmektedir. Bir diğer deyişle VoIP, PSTN (Public Switched Telephone Network) tabanlı geleneksel ses iletişimi yerine, sesin IP paketlerine dönüştürülerek IP tabanlı şebekeler üzerinden veri halinde iletilmesi hizmetidir. Her ne kadar teknolojinin ismi “ses”le bağdaşsa da genelde “ses ve çoklu-ortam” olarak genişletilmekte; sesi olduğu kadar faks, video konferans gibi çoklu ortam uygulamalarını da gerçek zamanlı olarak karşılamaktadır.

Bundan 30 yıl öncesine kadar yani, internet henüz yaygın değilken etkileşimli (interactive) iletişim sadece PSTN şebekesi üzerinden yapılabiliyordu. Veri iletimi özellikle uzun mesafeler için oldukça pahalıydı ve henüz kimse görüntülü iletişimi hayal bile edemiyordu. PSTN şebekeleri kullanıcılara her çağrı için uçtan uca bir devre bağlantısı sağlamaktadır. Arayan ve aranan tarafların numarasına göre, arayan tarafın bağlı olduğu santralden başlayarak, aradaki santraller ve diğer uçtaki santrale 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. PSTN trafiği her geçen gün daha fazla veri içerikli olamaya yüz tuttukça ses ve veri şebekelerinin birleşmesi yani tek bir platforma indirgenmesi ihtiyacı daha fazla belirgin hale gelmiştir. Bu nedenle internet servis sağlayıcıları ve ekipman üreticileri IP temelli olarak ses/veri iletimine yönelmişlerdir.

1995’lerde IP ağları üzerinden ses transferi teknik olarak mümkün hale geldi. Uygulamalar yaygın olarak kullanılmamakla birlikte standartlaştırma çalışmaları 1995 yılında başladı. 1996’da ilk VoIP standartları kabul edildi. Düşük kapasiteli H.323 ağ geçitleri (gateway) gibi ilk öncü ürünler aynı yıl geliştirildi. Ağ geçitlerinin ortaya çıkması ve kullanımı VoIP tarihinde anahtar bir rol oynamıştır. Ağ geçitleri birbirinden farklı PSTN ve IP ağları arasında iletişimi sağlamak için kullanılmaktadırlar. Kendi aralarında birbirlerinden oldukça farklı protokollerle konuşan iki ağı birleştirmek, konuşturmak ve birinden diğerine veri akışını sağlamak gibi zor bir görev üstlenmişlerdir. Nihayetinde bütün bu gelişmeler ilk internet üzerinden telefonda telefona görüşme ile sonucunu verdi.

İnternet’in gelişerek yaygınlaşmasıyla birlikte ses iletişiminin paket anahtarlama IP ağları üzerinden iletimi günümüzde son derece ekonomik ve cazip görünmektedir. Nitekim

paketlenerek IP trafiğı üzerine oturtulmuş ses verilerinden oluşan telefon faturaları, özellikle deniz aşırı konuşmalar dikkate alındığında ciddi bir ucuzlama sağlamaktadır.

3.1 VoIP'in Kullanım Alanları ve Entegrasyonu

Geniş alanlara yayılmış orta ve büyük ölçekli şirketlerdeki yüklü telefon faturaları ses ve veri entegrasyonu zorunlu hale getirmiştir. VoIP sayesinde düşürülen iletişim maliyetleri bir çok işletmenin ilgisini çekmiştir. VoIP teknolojisinin gelişmesinden önce şirketlerin telefon görüşmelerini geleneksel telefon şebekeleri üzerinden veri iletişimini ise kiralık hatlar üzerinden yapma zorunluluğı vardı. Bu iki hizmet için ayrı ayrı ücret ödemek zorundaydılar.

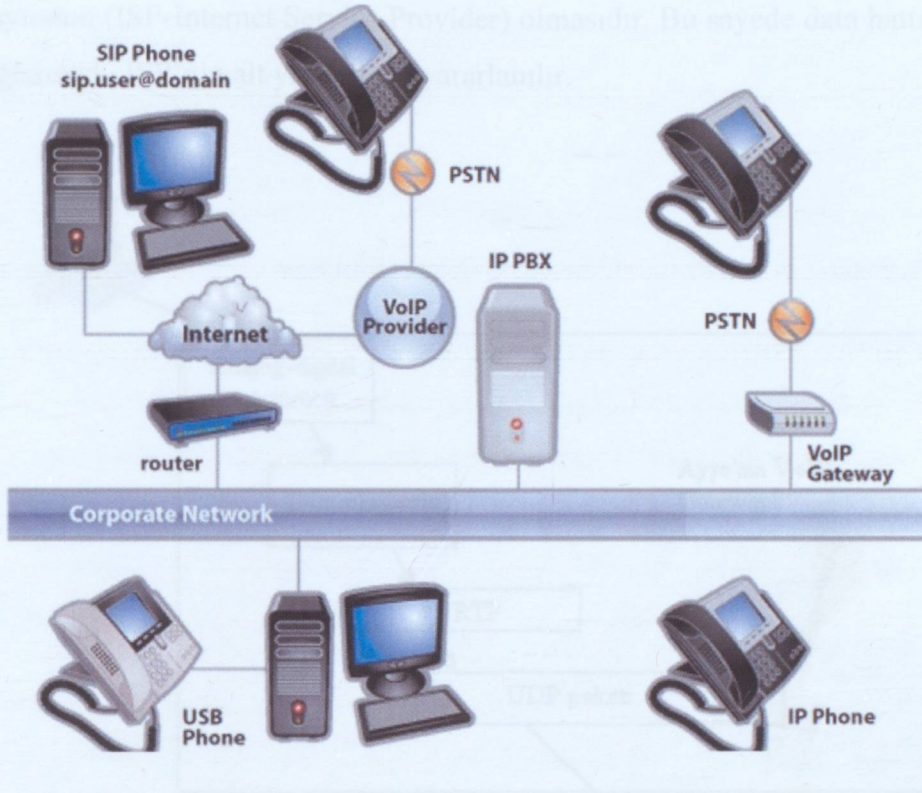
VoIP'in uygulama alanları gün geçtikçe artmaktadır. Uygulama alanları arttığından bu teknolojinin kullanılması kaçınılmazdır. Gelecekte PSTN şebekesinin önemi azalmayacaktır ama VoIP iki nokta arasındaki sesli iletişiminden tutunda karmaşık video konferanslara kadar her türlü ses iletişimine olanak sağlandığından esnek ve ucuz bir alternatif olacaktır.

Geniş alanlarda şubeleri bulunan ve merkezi ile sürekli çevrimiçi (online) çalışması gereken bir şirketi düşünelim. Bu şirket şubeleri ile bağlantı kurmak için hat kiralamak ve bunun için fatura ödemek zorundadır. Ayrıca şubeler arasındaki telefon görüşmeleri için de fatura ödeme zorunluluğı vardır. Böyle bir durumda şirketin imdadına VoIP yetişmektedir. VoIP ile birlikte ses ve veri entegrasyonunu sağlayarak mevcut veri iletişimini sağlayan data hatları üzerinden ses ve video iletişimi de sağlanabilmektedir.

Bir şirketin ofis içi ve ofisler arası ses iletişimini sağlaması için her ofisinde mutlaka bir telefon santrali vardır. Bu telefon santralleri PSTN hatlarında kullanılıyordur. VoIP teknolojisi kullanılarak bu santrallere yapılan birkaç eklemeler ile IP şebekesi üzerinden ofislerdeki santrallerin birbirlerine bağlanması sağlanabilmektedir. Bu sayede şirketin şirket içi telefon görüşmeleri maliyeti sıfır olacaktır. Bu da bir şirket için büyük bir ölçüde tasarruf demektir.

VoIP teknolojisi şirket içi telefon görüşmeleri haricinde internet kullanıcıları için de kullanabilmektedir. İnternette bulunan iki kullanıcı bu teknolojiyi kullanarak ücretsiz telefon görüşmesi yapabilmektedir. Evlerde bulunan standart telefonlar ile araya bir VoIP ağ geçidi koyarak ya da PC üzerinde çalışabilen bir yazılımsal telefon (softphone) ile VoIP teknolojisi kolaylıkla kullanılabilir ve internet üzerinden telefon görüşmesi yapılabilir (Şekil 3.1). Ayrıca internet kullanıcıları internetteyken kendilerine gelen telefon çağrılarını yanıtlayabilir ve hoparlör ve mikrofon ile telefon görüşmesi yapabilmektedir. Bu sayede

özellikle uzak noktalarla yapılan telefon/faks iletişimi çok ucuzlamakta hatta bedava olmaktadır.

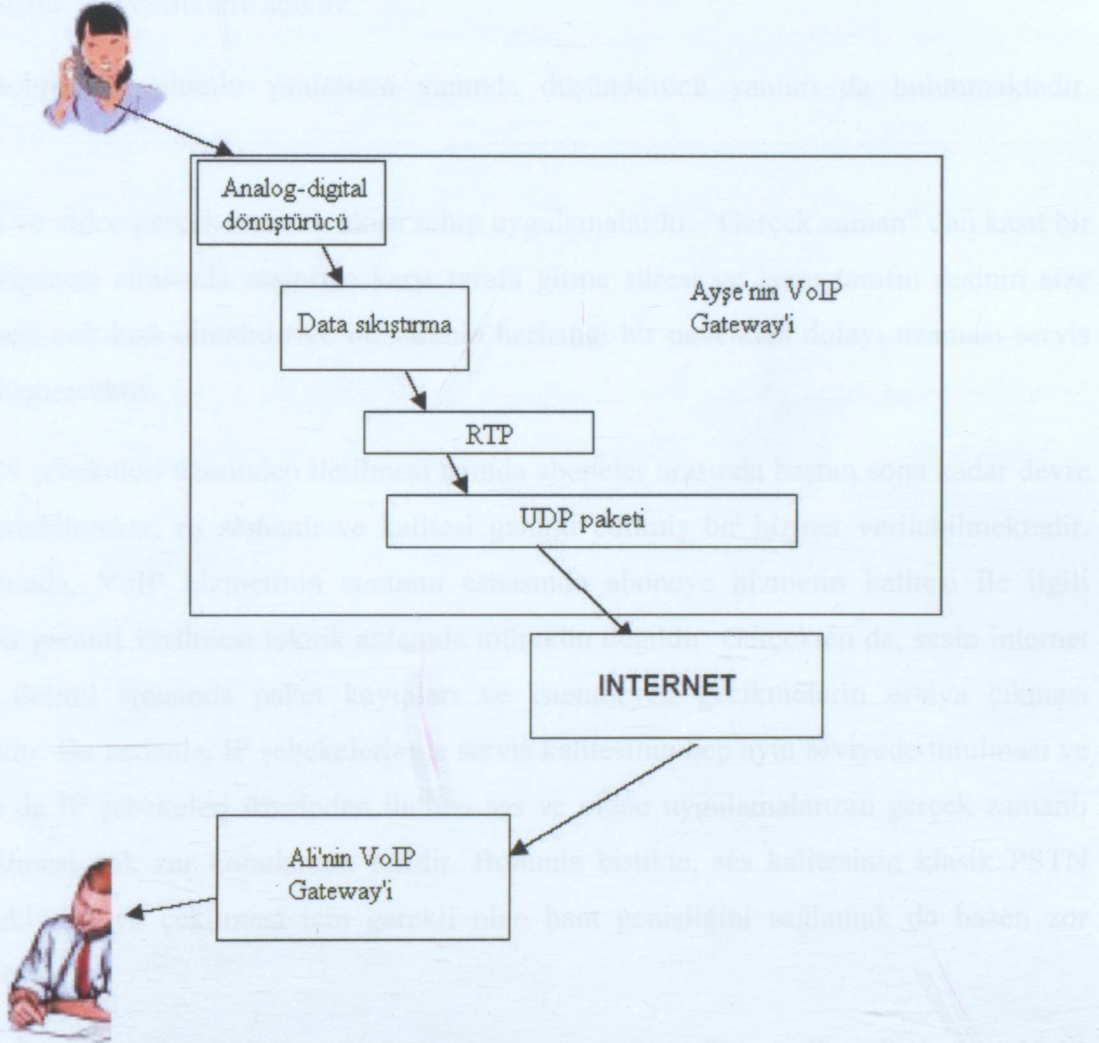


Şekil 3.1 VoIP bileşenleri ve entegrasyonu (Won, 2006)

Telefon görüşmelerinin mevcut data hattı üzerinden yapılması özellikle milletlerarası ve şehirlerarası telefon görüşmelerinde önemli ölçüde bir tasarruf sağlamaktadır. Bunu sağlamanın en basit ve en hızlı yöntemi data şebekesine bağlı olan her noktaya birer adet VoIP cihazının yerleştirilmesidir. VoIP cihazları çözümlerinde mevcut IP ağı cihazlarında ve telefon santralinde herhangi bir değişiklik yapmadan VoIP cihazı çok kısa bir süre içinde sisteme entegre edilebilmektedir. VoIP cihazları özel bir santrale veya belli marka bir yönlendiriciye (router) bağımlı değildir. Her yönlendirici ve santral ile çalışabilir. Bu da VoIP yatırımı maliyetini azaltan çok önemli bir faktördür. VoIP cihazının bir ucu mevcut data hattına bağlanır cihazın diğer ucuna ise ya bir telefon santrali ya da direkt bir telefon ya da bir faks cihazı bağlanabilmektedir. Böylece telefon ve faks iletişimi sanki aynı ofis içinde yapılıyormuş gibi ücretsiz ve kolay olmaktadır.

Bu iletişimde çok basit bir mantık vardır. Burada ses önce VoIP cihazına ulaşarak sayısal dataya çevrilir, data hattı üzerindeki yönlendirici ve modem aracılığıyla karşı noktaya gönderilir. Karşı noktada da yine modem ve yönlendirici aracılığıyla alınır ve VoIP cihazına

iletilir. Buradaki cihazda karşı tarafta yapılan işlemin tersi yapılarak data paketi halinde gelen ses işareti analog sese çevrilir ve telefona aktarılır (Şekil 3.2). İnternet üzerinden gerçekleştirilen iletişimde de yapılan işlem daha farklı değildir. Tek fark arada bir internet servis sağlayıcının (ISP-Internet Service Provider) olmasıdır. Bu sayede data hattı ofis ile ISP arasında sağlanarak, ISP'nin alt yapısından yararlanılır.



Şekil 3.2 IP üzerinden ses iletim aşamaları (Kuhn ve Thomas, 2005)

Özetle, gelecekte PSTN şebekelerinin yerini alacağına kesin gözüyle bakılan bu yeni teknoloji bir çok avantaja sahiptir. Bu avantajları maddeler halinde sıralarsak:

- Ses ve veri hizmetlerinin bir arada verilebilmesi.
- Varolan internet altyapısı üzerine kurulabilmesi.
- İletişim yatırım maliyetlerinin çok büyük oranda düşmesi.

- Bakım onarım giderlerinin düşmesi.
- Hareketliliği (Mobility) arttırması ve dünyanın her yerinden erişilebilirlik.
- Kurulum maliyetlerinin düşmesi.
- Operasyon maliyetlerinin düşmesi.
- Gelişme ve yeniliklere açıklık.

VoIP teknolojisinin olumlu yanlarının yanında düşündürücü yanları da bulunmaktadır.

Bunlar:

Kalite: Ses ve video gerçek zamanlı akışa sahip uygulamalardır. “Gerçek zaman” dan kasıt bir telefon görüşmesi sırasında sesinizin karşı tarafa gitme süresi ve karşı tarafın sesinin size ulaşma süresi çok kısa olmalıdır ve bu sürenin herhangi bir nedenden dolayı uzaması servis kalitesini düşürecektir.

Sesin PSTN şebekeleri üzerinden iletilmesi anında aboneler arasında baştan sona kadar devre tahsisi yapılabilmekte, eş zamanlı ve kalitesi garanti edilmiş bir hizmet verilebilmektedir. Bunun yanında, VoIP hizmetinin sunumu esnasında aboneye hizmetin kalitesi ile ilgili herhangi bir garanti verilmesi teknik anlamda mümkün değildir. Gerçekten de, sesin internet ortamında iletimi sırasında paket kayıpları ve istenmeyen gecikmelerin ortaya çıkması kaçınılmazdır. Bu nedenle, IP şebekelerimde servis kalitesinin hep aynı seviyede tutulması ve dolayısıyla da IP şebekeleri üzerinden iletilen ses ve video uygulamalarının gerçek zamanlı olarak iletilmesi çok zor konulardan biridir. Bununla birlikte, ses kalitesinin klasik PSTN sistemlerdeki çizgiye çekilmesi için gerekli olan bant genişliğini sağlamak da bazen zor olabilmektedir.

Güvenlik: Popülaritesi gittikçe artmakta olan ve gün geçtikçe gelişmekte olan VoIP teknolojisi beraberinde aynı hızda gelişen bir güvenlik problemini de getirmektedir. Sonuçta VoIP trafiği de aynı diğer veri akışlarında olduğu gibi bir yönlendiriciden diğerine giden trafik olarak değerlendirilmelidir. Bu durumda VoIP trafiği kötü niyetli biri tarafından kesilebilir, kopyalanabilir, engellenebilir, yavaşlatılabilir veya değiştirilebilir.

Günümüzde VoIP teknolojisinin yaygınlaşmasıyla birlikte yukarıda bahsedilen kalite ve güvenlik konuları üzerinde birçok araştırmalar ve beraberinde birçok geliştirmeler yapılmıştır. Kalite konusunda bugün PSTN şebekelerine çok yakın kalite seviyelerine ulaşılabilmekte ve güvenlik konusunda da geliştirilen güvenlik protokolleri sayesinde çağrının güvenli bir

şekilde kurulması sağlanabilmektedir. İleriki bölümlerde bu konuya ayrıntılı olarak değinilecektir. Şimdi VoIP teknolojisinde yaygın olarak kullanılan protokollere değinelim.

3.2 H.323 Protokolü

H.323, IP temelli ağlar üzerinden ses, görüntü ve data iletimini sağlamak amacıyla ITU-T (International Telecommunication Union-Telecommunication Standardization Sector) tarafından geliştirilmiş bir protokoldür. Önceleri yerel ağlar üzerinde çoklu ortam konferansları için geliştirilmiş, fakat sonradan IP üzerinden ses uygulamasını kapsayacak şekilde genişletilmiştir. H.323 protokolü, internet telefonculuğu amacıyla kullanılan en geniş ve en etkin standartlardan birisidir. Ses ile beraber data, video ve resim gibi tüm çoklu ortam uygulamalarını desteklemektedir.

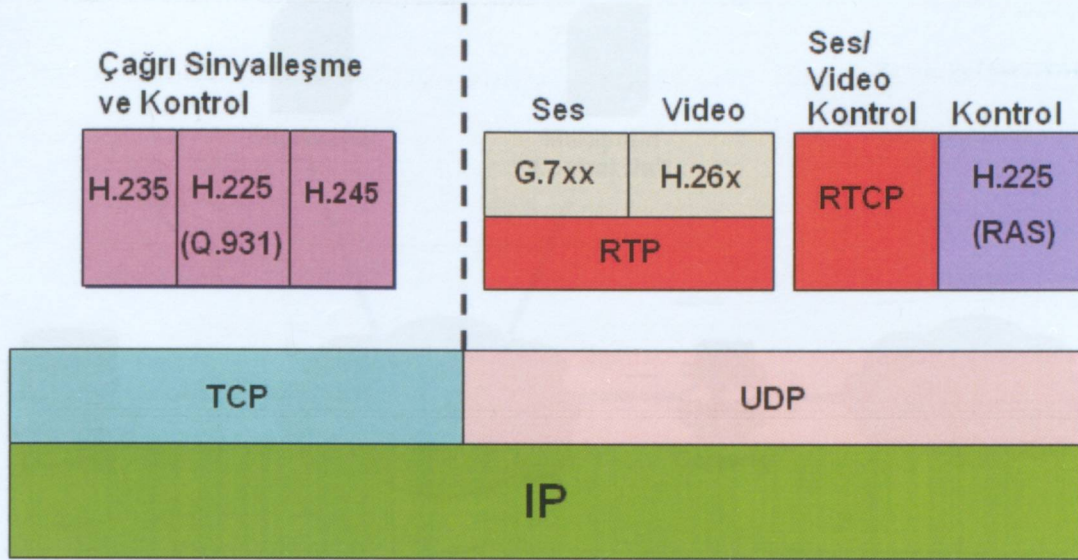
Genellikle bir işaretleşme standardı olarak görülen H.323 aslında bir çok protokolün birleşerek oluşturduğu bir protokoldür. H.323 ses, veri ve görüntünün birleşik bir şekilde IP bazlı şebekelerden nasıl iletilmesi gerektiğini açıklayan kuralları barındıran bir protokoldür.

3.2.1 H.323 Protokol Yığını

H.323 protokol yığını aşağıdaki temel bileşenlerden oluşmaktadır.

- İşaretleşme ve kontrol protokolleri: H.245, H.225, RTCP
- Ses kodlayıcıları: G.7xx (G.711, G.723, G.726, G.729, vb.)
- Görüntü kodlayıcıları: H.26x (H.261, H.263)
- Çoklu ortam haberleşmesi protokolü: T.120
- Taşıma protokolü: RTP

Şekil 3.3'de H.323'de hangi protokollerin hangi katmanlarda kullanıldığı gösterilmiştir.



Şekil 3.3 H.323 protokol yığını

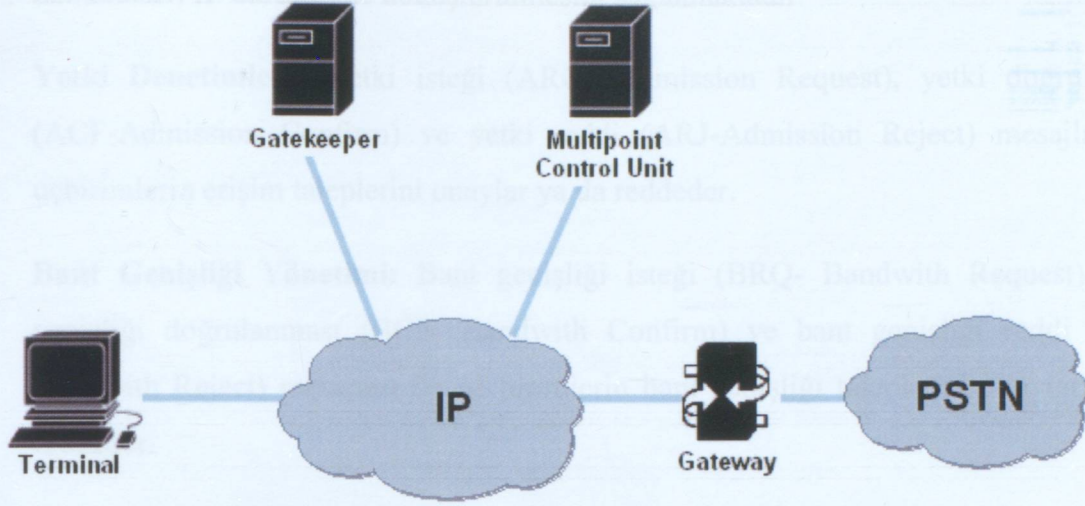
3.2.2 H.323 Bileşenleri

H.323’de tanımlı toplam 4 ayrı bileşen bulunmaktadır (Şekil 3.4). Bunlar:

- Terminal.
- Ağ Geçidi (GW-Gateway).
- Geçit Sorumlusu (GK-Gatekeeper).
- Çok Nokta Kontrol Birimi (MCU-Multipoint Control Unit).

Terminal: Terminaller uç noktalarda gerçek zamanlı çift yönlü haberleşme sağlayan, hem GW’ler hem de MCU’larla haberleşme yeteneğine sahip olan yerel ağ istemcileridir. Bir terminal diğer bir terminali arama yeteneğine sahip olduğu gibi bu arama işlemi bir GW ya da bir GK üzerinden de yapılabilir. Tüm H.323 terminalleri H.245, Q.931, RAS ve RTP protokollerini desteklemektedir.

H.245, kanal kullanım izni için; Q931, çağrı kurulması ve sinyalleşme için; RTP, gerçek zamanlı olarak ses paketlerinin taşınması için; RAS (Registration Admission Status) ise GK ile haberleşme için kullanılan protokollerdir.



Şekil 3.4 H.323 bileşenleri

Ağ Geçidi (GW-Gateway): Ağ geçitleri, PSTN ağları ile IP ağları arasında arayüz olarak görev yapan, diğer bir deyişle ağlar arası geçiş fonksiyonlarını sağlayan modüllerdir. Bu tür ağ geçitleri hem SS7 hem SIP hem de H.323 protokollerini desteklemektedirler. IP şebekesi ile PSTN şebekesi arasındaki çağrı kurulumu ve sonlandırılması işlemlerini ağ geçitleri üstlenmektedir. Ses, data ve görüntü arasındaki dönüşümler de ağ geçitleri vasıtasıyla gerçekleşmektedir.

Bir ağ geçidi, IP ağı üzerindeki H.323 uyumlu terminallerin geleneksel PSTN şebekesine entegrasyonunu sağladığı gibi IP ağı üzerindeki farklı terminallerin de haberleşmesini sağlamaktadır.

Geçit Sorumlusu (GK-Gatekeeper): GK, terminallerin ve GW'lerin kayıt, kabul ve durum (RAS-Registration, Admission and Status) takibinden sorumlu olan bir ağ modülüdür. Ayrıca bölge (zone) yönetimi ve çağrı işleme işlevlerini de yerine getirmektedir.

GK'ler şebekedeki adres tercüme işlemlerini gerçekleştiren cihazlardır. Ayrıca terminallerin, ağ geçitlerinin ve MCU'ların birbirlerine erişimlerini kontrol eden cihazlardır. Zaman zaman, GW'ler diğer GW'lere ulaşmak istediklerinde eğer hedef ağ geçidinin fiziksel konumu veya IP adresi belli değilse bunu geçit sorumlusuna sorarak öğrenirler. Bu bakımdan GK'lerin şebeke üzerinde büyük bir hakimiyetleri bulunmaktadır.

H.323 sistemindeki bir GK'nin başlıca görevleri şu şekildedir:

- **Adres Dönüşümleri:** Ağdaki uçbirimlerin E.164 adreslerinin (standart telefon

numaraları) IP adreslerine dönüştürülmesini sağlamaktadır.

- **Yetki Denetimleri:** Yetki isteği (ARQ- Admission Request), yetki doğrulaması (ACF-Admission Confirm) ve yetki reddi (ARJ-Admission Reject) mesajları ile uçbirimlerin erişim taleplerini onaylar ya da reddeder.
- **Bant Genişliği Yönetimi:** Bant genişliği isteği (BRQ- Bandwith Request), bant genişliği doğrulanması (BCF- Bandwith Confirm) ve bant genişliği reddi (BRJ- Bandwith Reject) mesajları ile uç birimlerin bant genişliği taleplerini onaylar ya da reddeder.
- **Bölge Yönetimi:** Tek bir GK tarafından yönetilen terminallerin, GW'lerin, ve MCU'ların toplamı "bölge (zone)" olarak adlandırılır. GK, yukarıda anlatılan bütün fonksiyonları kendi yönetimindeki bölge için sağlamaktadır.

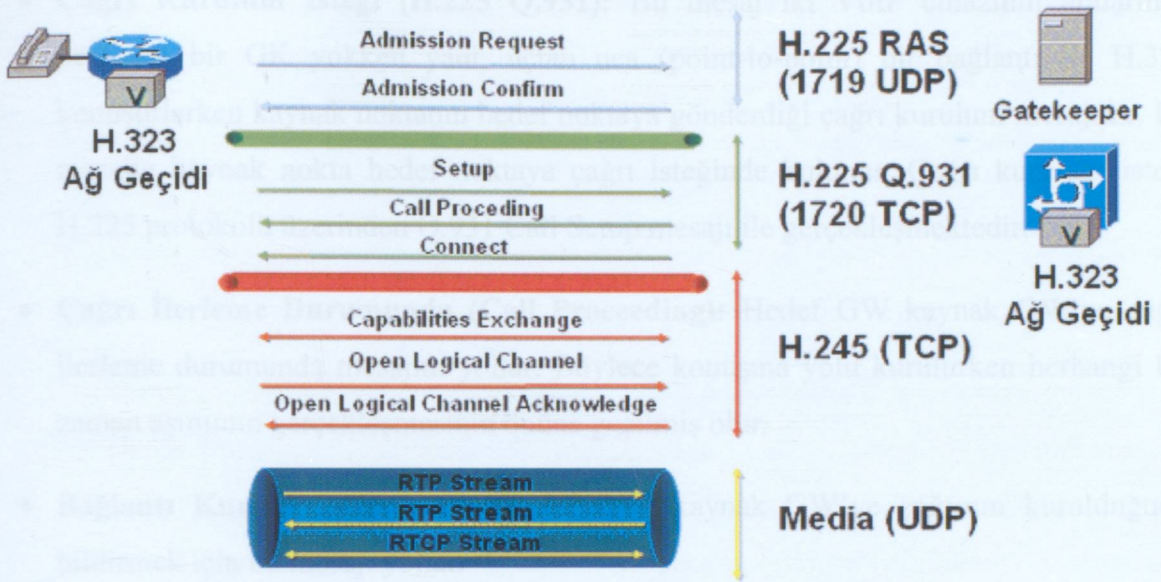
Ayrıca bir GK; çağrı kontrol sinyalleşmesi, çağrı yetkilendirme ve çağrı yönetimi gibi fonksiyonları da desteklemektedir.

Çok Nokta Kontrol Birimi (MCU-Multipoint Control Unit): MCU, ağdaki üç veya daha fazla terminalin ya da GW'nin çoklu bir konferansa katılımlarını sağlayan bir ekipmandır. MCU iki kısımdan oluşmaktadır. Bunlar MC (Multipoint Controller) ve MP (Multipoint Processor)'dir. Bunlardan MC bulunması zorunlu bir ekipman iken MP'nin bulunması zorunlu değildir. MC, konferansa katılacak bütün terminallerin ortak iletişim seviyelerinde bulunmalarını sağlamak amacıyla iletişim parametreleri üzerinde uzlaşmalarını sağlamaktadır. MP ise MC'nin denetiminde medya akışlarının işlenmesi görevlerini (karıştırma, anahtarlama, vb.) yürütmektedir.

3.2.3 H.323 Mesajları

H.323'de konuşma yolunun kurulması esnasında çeşitli mesajlar kullanılmaktadır (Şekil 3.5). Bu mesajlar aşağıda verilmiştir.

H.225 Mesajları: H.323 protokolünde çağrı kurulumu H.225 protokolü vasıtasıyla 1719 UDP ya da 1720 TCP portları üzerinden gerçekleşmektedir. Eğer bir terminal herhangi bir GK'ye çağrı kurulum talebinde bulunursa 1719 UDP portunu kullanırken; terminaller arasındaki uçtan uca çağrı kurulum talepleri ise 1720 TCP portu üzerinden gerçekleşmektedir. Başlıca H.225 mesajları aşağıda verilmiştir.



Şekil 3.5 H.323 mesajları ve çağrı kurulumu

- **Çağrı Kurulum İsteği (H.225 RAS):** Bu mesajla kaynak nokta GK'ye çağrı isteğinde bulunur. Çağrı kurulum isteği H.225 RAS mesajları ile gerçekleşmektedir. RAS mesajlarından bazıları şu şekildedir:
 - ✓ **ARQ (Admission Request):** GW'nin GK'ye hedef noktasındaki uç birim ile bağlantının nasıl yapılacağını sorduğu çağrı kurulum mesajdır.
 - ✓ **ACF (Admission Confirm):** GK'nin kaynak uç birimin hedef uç birimdeki GW ile bağlantının kurulmasına izin verdiğini belirten ve kaynağa hedef GW'nin adresinin iletildiği mesajdır.
 - ✓ **ARJ (Admission Reject):** GK tarafından gönderilen ve GW'nin çağrı kurulum talebini reddettiğini bildiren mesajdır.
 - ✓ **RRQ (Registration Request):** GW'nin GK'ye kayıt olmak için gönderdiği mesajdır.
 - ✓ **RCF (Registration Confirm):** GK tarafından uç terminale gönderilen ve kayıt işleminin gerçekleştiğini bildiren mesajdır.
 - ✓ **RRJ (Registration Reject):** GK'nin kayıt işlemini reddettiğini bildiren mesajdır.

- **Çağrı Kurulum İsteği (H.225 Q.931):** Bu mesaj iki VoIP cihazının aralarında herhangi bir GK yokken yani, uçtan uca (point-to-point) bir bağlantı ile H.323 konuşurlarken kaynak noktanın hedef noktaya gönderdiği çağrı kurulum mesajıdır. Bu mesajla kaynak nokta hedef noktaya çağrı isteğinde bulunur. Çağrı kurulum isteği H.225 protokolü üzerinden Q.931 Call Setup mesajı ile gerçekleşmektedir.
- **Çağrı İlerleme Durumunda (Call Proceeding):** Hedef GW kaynak GW'ye çağrı ilerleme durumunda mesajını yollar. Böylece konuşma yolu kurulurken herhangi bir zaman aşımının gerçekleşmesinin önüne geçilmiş olur.
- **Bağlantı Kuruldu (Connect):** Hedef GW, kaynak GW'ye çağrının kurulduğunu bildirmek için bu mesajı yollar.

H.245 Mesajları: H.323 protokolünde H.225 protokolü üzerinden çağrı kurulumu tamamlandıktan sonra katılımcılar arasında H.245 kontrol mesajları gidip gelmektedir. Bu mesajların amacı katılımcıların sorunsuz bir H.323 oturumu kurabilmeleri için gerekli parametreler konusunda mutabakata varmalarıdır. Bu parametreler arasında; kanal durumu, zaman parametreleri, katılımcıların destekledikleri kodlayıcılar, ses veya video parametreleri, vb. bulunmaktadır. H.245 mesajları TCP portu üzerinden iletilmektedir. H.245 mesajları aşağıdaki gibidir.

- **TCS (Terminal Capability Set):** Bu mesaj sayesinde GW'ler destekledikleri parametreleri (kodlayıcılar gibi) karşı tarafa iletirler.
- **OLC (Open Logical Channel):** Kaynak GW'nin hedef GW ile mantıksal kanal açılması amacıyla yolladığı mesaj türüdür.
- **ACK (Acknowledgement):** TCS mesajını alan GW'nin bu mesajı aldığını karşı tarafa bildirmek için yolladığı mesajdır.

H.225 çağrı kurulum mesajları ve H.245 kontrol mesajları tamamlandıktan sonra artık katılımcılar arasında ses iletimi başlayacaktır. Ses iletimi RTP protokolü üzerinden gerçekleşmektedir.

3.2.4 H.323 Protokol Versiyonları

H.323 Versiyon 2 (H.323 v.2): Bu sürüm varolan H.323 protokolüne yeni özellikler eklemiştir. Bu özellikler aşağıda verilmiştir (Kuhn ve Thomas, 2005).

- **Hızlı Bağlanma (Fast Connect):** Çağrının kurulma hızını artırır. Böylece çağrı kurulum süresi kısalmır.
- **Ek Hizmetler (Supplementary Services):** H.450 serisi standartlar da sisteme entegre olmuştur. Bu standartlardan H.450.1, bu ek servislerin kontrolünü ve işaretleşmesini sağlar. H.450.2 ise katılımcılar arasında çağrı transferini mümkün kılan bir standarttır. H.450.3 ise gelen çağrının başka bir hedefe yönlendirilmesini sağlamaktadır.
- **H.235 güvenliği:** Bu özellik doğrulama, güvenilirlik, gizlilik ve reddedilmeme gibi işlemleri tanımlar. Doğrulama sadece yetkili kullanıcıların haberleşebilmesini sağlayan bir mekanizmadır. Güvenilirlik, gelen paketle kaynaktan yollanan paketin içindeki veriyle birebir aynı olmasını sağlar. Gizlilik, paketin şifreleme yoluyla sadece hedeflenen alıcı tarafından alınmasını sağlar. Reddedilmeme ise, kullanıcının bir konferans görüşmeye katılmak istediğinde onun o görüşmeye katılma isteğinin reddedilmemesini garantiler.
- **Şebeke Sorumlusu Fazlalığı (GK Redundancy):** Birincil GK hizmet dışı kaldığında kullanıcının ikincil ve üçüncül GK'ler tanımlamasına olanak verir. Böylece verilen hizmetin sürekliliği artar.
- **Servis Kalitesi (QoS-Quality of Service):** Uç noktaların kendi QoS parametrelerini belirlemelerini sağlar. Bu şekilde şebeke performansının artırılması sağlanır.

H.323 Versiyon 3 (H.323 v.3): Bu sürüm daha önceki sürümlere ek olarak, hızlı bağlantı kurulması için TCP yerine UDP üzerinden işaretleşmenin yapılmasını sağlar. Tabi ki bu teknik küçük şebekelerde işe yarayan bir tekniktir. Binlerce çağrının üzerinden geçtiği şebekelerde UDP uzun çağrı kurulum süreleri oluşmasına neden olur. H.323 v.3, SS7 işaretleşmesinin olduğu PSTN şebekelerine de entegre olmuştur ve dört adet yeni ek servise destek vermeye başlamıştır. Bunlar H.450.4 ile o anda etkin olan çağrıyı belirli bir süre bekletip diğer gelen çağrıya bakılmasını, H.450.5 ile gelen bir çağrının belirli bir süre bekletilip; daha sonra önceden belirlenmiş farklı telefonlar tarafından karşılanabilmesini sağlar. Aynı şekilde bir çağrının farklı telefonlardan aynı şekilde çıkarılmasını sağlar. H.450.6 ile aranan tarafın meşgul olduğu durumlarda gelen çağrının bekletilmesi sağlanır. H.450.7 kullanıcıya kendisini bekleyen mesajların olduğu bildirilir. Ayrıca H.323 v.3, H.246C desteğidir. Bu destek ise ISUP ile H.226 konuşabilmesini sağlar.

H.323 Versiyon 4 (H.323 v.4): H.323'ün dördüncü sürümü diğer sürümlere göre daha geniş şebekeler için geliştirilmiştir. İlk üç sürümde ağ geçitleri bütün işleri hallederlerdi. Yapılan bu işler, işaret dönüşümü, çağrı kontrolü ve çeşitli çoğul ortam kodlayıcıları arasında dönüşümleridir. Bütün bu görevlerin ağ geçitlerinin üzerine bindirilmesi ise şebeke büyüdüğü zaman ölçeklenebilirlik açısından sıkıntılara yol açmaktadır.

H.323 v.4 geniş şebekelerdeki ölçeklenebilirlik problemini GW'leri üç ayrı şebeke elemanına ayırarak çözmüştür. Bu üç eleman aşağıda verilmiştir.

- Akılsız (Dumb) Medya Ağ Geçidi (MG).
- Medya Ağ Geçidi Kontrolörü (MGC).
- İşaretleşme Ağ Geçidi.

MG'ler sadece PSTN ile veri şebekesi arasında akan sesin gideceği şebekenin formatına uygun şekle dönüştürülmesinden sorumludurlar. Böylece paket şebekesindeki RTP başlığını ve PSTN'deki taşıyıcı kanalları sonlandırma görevini üstlenmiş olurlar.

MGC'ler MG'lerin çağrıları nasıl işlemesi gerektiğini bilen ve gerekli emirleri MG'lere veren yönetim cihazlarıdır. Eğer MG ve MGC'ler farklı cihazların içinde bulunuyorlarsa yani tümleşik değilse; bu durumda birbirleriyle iletişim kurabilmeleri amacıyla Ağ Geçidi Kontrol Protokolü (GCP-Gateway Control Protocol) adlı protokolü kullanırlar. GCP'nin ITU-T tarafından H.323 v.4 için geliştirilmiş hali H.248'dir. H.248 ise IETF'nin MEGACO protokolüyle beraber çalışması için tasarlanmıştır.

SG'ler ise sistemdeki tüm işaretleşmeden sorumludurlar. Bunlar, SS7 işaretleşme mesajlarının IP şebekesi üzerinde de uygun formatta yol almalarını sağlayacak dönüşümleri yaparlar.

H.323 v.4, çoklu akış iletimine izin verir; ki bu iletim ses ile görüntü verilerinin birleştirilmiş bir şekilde aynı anda akmasını sağlar. Bu özelliğin sağladığı en büyük fayda ise ses ve görüntünün önceki sürümlere göre çok daha kolay bir şekilde senkronize olabilmesidir. Ayrıca dördüncü sürümde desteklenen ek servislerin sayısı arttırılmıştır. Bunlar:

- **H.450.8:** Kullanıcı bilgilerinin karşı taraftaki uç birim noktasına gönderilmesini sağlar. Bu hizmet PSTN şebekesinde sadece arayanın numarasını gösterme (Caller ID) şeklinde verilebilmektedir.
- **H.450.9:** Aranan taraf meşgul olduğunda veya cevap yoksa çağrının otomatik olarak

kesilmesini sağlar.

- **H.450.10:** Arayan tarafın isteğine bağlı olarak aranan taraf meşgulse, arayanın hatta tutulması ve meşgul durumun sona ermesiyle birlikte çağrının kurulmasını sağlar. Bu özellik, ülkemizde aranan tarafın devamlı meşgul olduğu, yarışma programları gibi yerlerde, kullanılmak için oldukça elverişlidir.
- **H.450.11:** Arayan A kullanıcısının, aranan B kullanıcısı C kullanıcısıyla görüşme halindeyse araya girmesini sağlar. Bu hizmet, A kullanıcısının isteğine göre verilebilir. Özellikle önceliği yüksek olan kullanıcılar (komutanlar, büyük patronlar) bu hizmetten yararlanmak isteyeceklerdir.

3.3 Oturum Başlatma Protokolü (SIP-Session Initiation Protocol)

SIP protokolü 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.

SIP protokolünün başlıca özellikleri şu şekildedir:

- Protokol HTTP protokolünden esinlenerek oluşturulmuştur. HTML'de kullanılan kodlar ufak değişikliklerle SIP protokolünde de kullanılabilir.
- 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. Standart port numarası 5060'dır.

3.3.1 SIP Bileşenleri

SIP, noktadan noktaya bir protokoldür. Her bir uç "Kullanıcı Ajansı (UA-User Agent)" olarak isimlendirilir. UA'lar SIP ağında aşağıdaki görevlerden birini yerine getirirler:

- **Kullanıcı tarafı kullanıcı ajansı (UAC-User Agent Client):** SIP isteklerinin başlatıldığı noktalardır. Ağ geçitleri, IP telefonlar, Yazılımsal SIP telefonlar (softphone), vb. UAC olarak davranırlar.
- **Sunucu tarafı kullanıcı ajansı (UAS-User Agent Server):** UAC'den gelen istek mesajlarının alınmasından ve bu mesajların cevaplanmasından sorumludur. SIP Proxy, yönlendirme ve lokasyon sunucuları UAS olarak davranırlar.

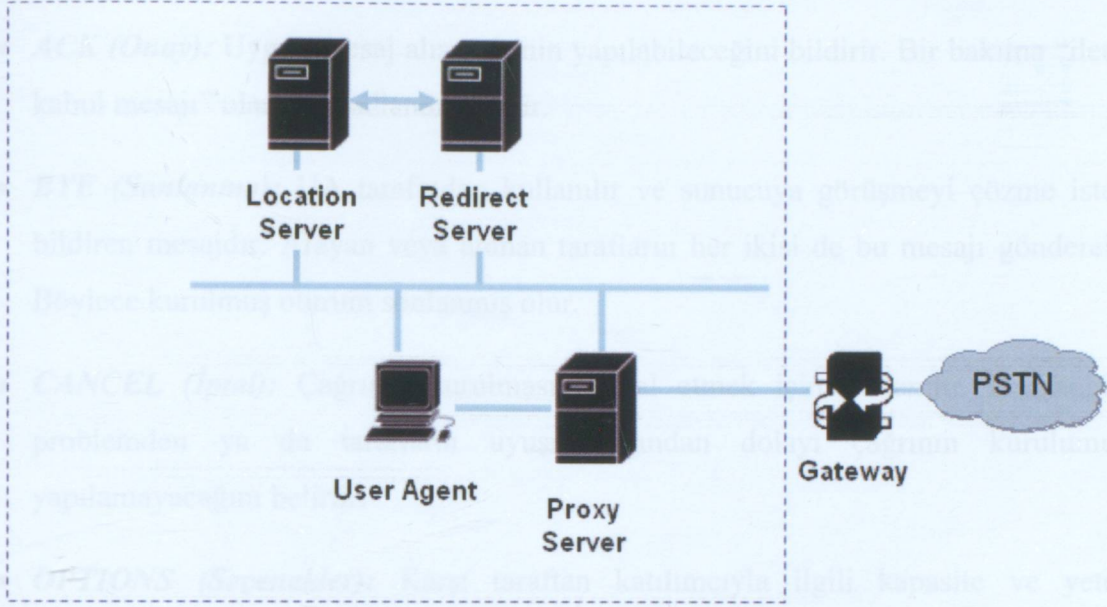
3.3.2 SIP Sunucuları

3 tip SIP sunucusu bulunmaktadır (Şekil 3.6). Bunlar:

Proxy Sunucusu: Bu sunucu, hem bir uç birim hem de yeri geldiğinde bir sunucu olarak görev yaparak, diğer uç birimlerden gelen istekleri işler. Proxy sunucusu, ağ üzerindeki VoIP cihazlarının tüm çağrı taleplerini kendi üzerinde toplayarak yönlendirme işlemlerini tek bir merkezden gerçekleştiren merkezi bir yapı sunmaktadır.

Yönlendirme Sunucusu (Redirect Server): Bu sunucu, arayan tarafa aranan taraf hakkındaki lokasyon bilgilerini iletmektedir. Bir yönlendirme sunucusuna herhangi bir çağrı geldiğinde aranan taraf kendisine kayıtlı ise doğrudan ilgili çağrıyı aranan kişiye yönlendirir. Ancak, aranan taraf kendisine kayıtlı değilse, çağrıyı aranan tarafın bulunduğu sunucuya yönlendirir. Proxy sunucuları böyle bir durumda yani aranan tarafın kendisinde kayıtlı olmadığı bir durumda çağrıyı doğrudan sonlandırmaktadır.

Lokasyon Sunucusu (Lokation Server): Bu sunucular, uç birimlerin fiziksel adreslerini tutarlar. Diğer SIP sunucuları tarafından katılımcıların konum bilgilerinin elde edilmesi amacıyla başvuru sistemleridir. Ancak günümüzde birçok proxy sunucusu lokasyon sunucusunu da kendi yapısı içerisinde barındırdığından bu tip sunucular günümüzde çok kullanılmamaktadır.



Şekil 3.6 SIP bileşenleri

3.3.3 SIP Mesajları

SIP mesajları iki gruba ayrılırlar. Kullanıcı uç birimleri tarafından gönderilen istek (request) mesajları ve sunucular tarafından bu mesajlara cevap olarak gönderilen cevap (response) mesajlarıdır. Her mesaj bir başlık alanından ve opsiyonel bir gövde alanından oluşur.

SIP İstek Mesajları:

- **INVITE (Davet):** Kullanıcının oturuma davet edilmesini sağlar. Mesajın gövdesi davet edilen yani, aranan tarafla ilgili enformasyonu içeren bir açıklama alanı içerir. Bu mesajın başlığı aşağıdaki parametreleri içerir.
 - ✓ Çağrı kimliği (Call-ID), ki bu kimlik yapılan daveti kendine has bir şekilde tanımlar.
 - ✓ Aranan ve arayan tarafların adresleri (From, To).
 - ✓ Çağrının konusu (Subject).
 - ✓ Çağrı önceliği.
 - ✓ Çağrı yönlendirme istekleri.
 - ✓ Kullanıcının yeriyle ilgili özellikler.

✓ Cevabın istenen bölüm ve özellikleri.

- **ACK (Onay):** Uygun mesaj alışverişinin yapılabileceğini bildirir. Bir bakıma “iletişim kabul mesajı” olarak da adlandırılabilir.
- **BYE (Sonlanma):** UA tarafından kullanılır ve sunucuya görüşmeyi çözme isteğini bildiren mesajdır. Arayan veya aranan tarafların her ikisi de bu mesajı gönderebilir. Böylece kurulmuş oturum sonlanmış olur.
- **CANCEL (İptal):** Çağrının kurulmasını iptal etmek için kullanılır. Herhangi bir problemten ya da tarafların uyuşmazlığından dolayı çağrının kurulmasının yapılamayacağını belirtir.
- **OPTIONS (Seçenekler):** Karşı taraftan katılımcıyla ilgili kapasite ve yetenek enformasyonu istenir. Böylece en uygun performansı sağlayan mantıksal bağlantı kurulabilir.
- **REGISTER (Kaydol):** Herhangi bir SIP sunucusuna kayıt olabilmek için kullanılır. Bu mesajın başlık alanında çeşitli bölgeler bulunmaktadır. Bu bölgeler:
 - ✓ To bölgesi: Sunucu adresi bu bölgeye yazılır.
 - ✓ From bölgesi: Arayan tarafla ilgili adres ve IP bilgileri bu alana yazılır.
 - ✓ Request-URI bölgesi: Kayıt olanın domain adı bu bölgeye yazılır.
 - ✓ Call-ID bölgesi: From başlığıyla aynı yapıdadır. Aranan tarafın adresini belirtir.

Örnek bir SIP istek mesajı Şekil 3.7’de verilmiştir.


```

INVITE sip:marconi@radio.org SIP/2.0
Via: SIP/2.0/UDP lab.high-voltage.org:5060;branch=z9hG4bKfw19b
Max-Forwards: 70
To: G. Marconi <sip:Marconi@radio.org>
From: Nikola Tesla <sip:n.tesla@high-voltage.org>;tag=76341
Call-ID: 123456789@lab.high-voltage.org
CSeq: 1 INVITE
Subject: About That Power Outage...
Contact: <sip:n.tesla@lab.high-voltage.org>
Content-Type: application/sdp
Content-Length: 158

v=0
o=Tesla 2890844526 2890844526 IN IP4 lab.high-voltage.org
s=Phone Call
c=IN IP4 100.101.102.103
t=0 0
m=audio 49170 RTP/AVP 0
a=rtpmap:0 PCMU/8000

```

Şekil 3.7 Örnek bir SIP istek mesajı

SIP Cevap Mesajları:

Bir SIP cevap mesajı bir SIP istek mesajının alınmasının ardından gönderilir. SIP cevap mesajının ilk satırı durum satırı olarak adlandırılır. Bu satır 3 haneli durum kodu ve metin öbeğinden oluşur. Durum kodu istekle ilgili sunucu tarafında neler yapıldığını belirtir. Metin öbeği kısmı ise küçük bir açıklama getirmek için kullanılır. Cevap mesajları başlıca altı gruba ayrılır.

- **1xx: Bilgilendirme Mesajları:** İstek mesajının alındığını ve işleme konduğunu bildirir.

100: Deniyor (Trying).

180: Zil çaldırılıyor (Ringing).

181: Çağrı yönlendiriliyor (Call is being forwarded).

- **2xx: Başarı Mesajları:** Arama ya da kayıt faaliyetinin başarılı bir şekilde alındığını, anlaşıldığını ve kabul edildiğini gösterir.

200: Tamam (OK).

- **3xx: Yönlendirme Mesajları:** İsteğin yerine getirilebilmesi için yeni faaliyetlerin yapılması gerektiğini bildirir.

- 301: Kalıcı olarak yer değiştirmiş (Moved permanently).
- 302: Geçici olarak yer değiştirmiş (Moved temporarily).
- 305: Proxy sunucusu kullanılmalı (Use proxy).
- **4xx: Kullanıcı Tarafı Hataları:** İsteğin kötü bir sentaksa sahip olduğunu veya şuan yerine getirilemeyeceğini bildirir.
 - 401: Gerekli izin bulunmuyor (Unauthorized).
 - 404: Bulunamadı (Not Found).
 - 415: Desteklenmeyen medya türü (Unsupported media type).
- **5xx: Sunucu Hataları:** Talep edilen çağrının sunucu tarafından yerine getirilemediğini bildirir.
 - 500: İç sunucu hatası (Internal server error).
 - 501: Uygulanamadı (Not Implemented).
 - 503: Servis dışı (Service Unavailable).
- **6xx: Global Hatalar:** Genel global hataları bildirir.
 - 600: Her yer meşgul (Busy everywhere).
 - 603: Reddedildi (Decline).
 - 606: Kabul edilemez (Not acceptable).

Örnek bir SIP cevap mesajı Şekil 3.8’de verilmiştir.

SIP/2.0 180 Ringing

Via: SIP/2.0/UDP lab.high-voltage.org:5060;branch=z9hG4bKfw19b
 ;received=100.101.102.103
 To: G. Marconi <sip:marconi@radio.org>;tag=a53e42
 From: Nikola Tesla <sip:n.tesla@high-voltage.org>;tag=76341
 Call-ID: 123456789@lab.high-voltage.org
 CSeq: 1 INVITE
 Contact: <sip:marconi@tower.radio.org>
 Content-Length: 0

Şekil 3.8 Örnek bir SIP cevap mesajı

3.3.4 SIP İsimleri ve Adresleri

SIP protokolünde kullanıcılar SIP adresleriyle tanımlıdır. Bu adresler aslında e-posta adresleriyle büyük bir benzerlik göstermektedirler. Bu adresler SIP URL olarak da bilinirler. Basit bir SIP URL adresi “*sip:kullanıcı_adi@servis_sağlayıcı*” şeklindedir.

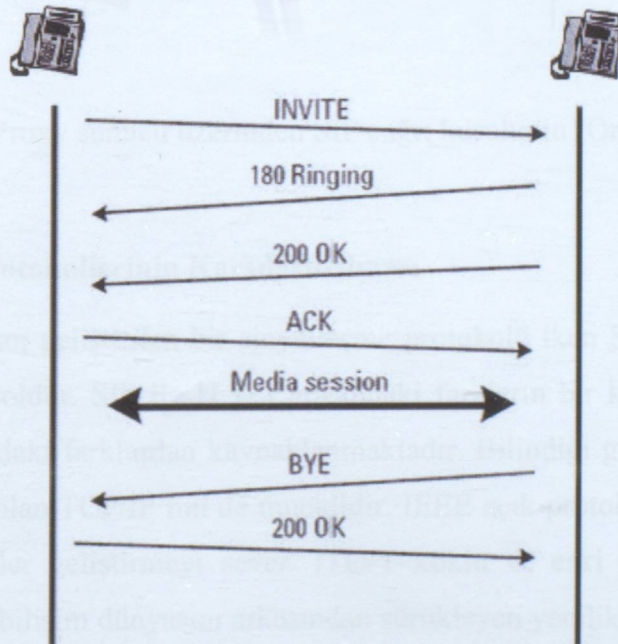
Burada; “kullanıcı_adi” bölümü bir kullanıcıya atanmış bir isim ya da bir telefon numarası olabilirken; “servis_sağlayıcı” bölümü ise, bir domain adı ya da bir IP adresi olabilmektedir. SIP URL adreslerine aşağıda birkaç örnek verilmiştir:

- 02124552525@system.com
- voip@system.com
- 02124552525@192.168.0.22

3.3.5 SIP Çağrı Kurulumu

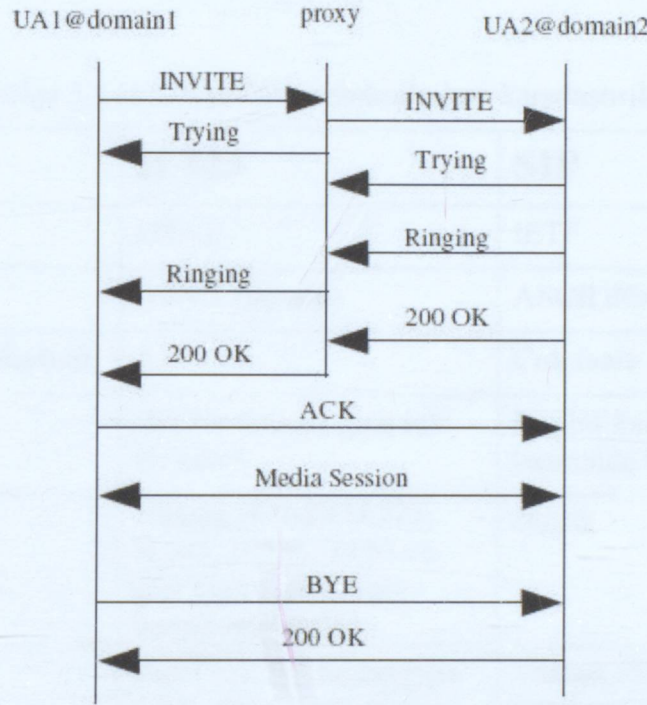
SIP çağrı kurulumu iki SIP terminali (UA-User Agent) arasında doğrudan yapılabildiği gibi arada bir proxy sunucu kullanılarak da yapılabilmektedir.

Doğrudan SIP çağrı kurulumu: SIP çağrı kurulumu doğrudan UA’lar arasında gerçekleşir. Çağrıyı başlatan UA tarafından diğer aranan UA’ya ‘invite’ mesajı gönderilir ve kabul edilirse onay mesajı sonrasında çağrı kurulur. Basit bir SIP oturumunda SIP sinyalleşmesi Şekil 3.9’deki gibi olmaktadır:



Şekil 3.9 Temel SIP çağrı kurulumu (Orrblad, 2004)

Proxy sunucu kullanılarak SIP çağrı kurulumu: Çağrıyı başlatan UA proxy sunucuya 'invite' mesajı gönderir. Proxy sunucu eğer çağrının sonlanacağı (aranan) UA'nın IP adresi kendisinde kayıtlı ise doğrudan aranan UA'ya 'invite' mesajı gönderir. Ancak eğer aranan UA'nın IP adresi kendisinde kayıtlı değilse lokasyon sunucusundan aranan UA'nın IP adresini alır ve ardından aranan UA'ya 'invite' mesajını gönderir. Eğer parametreler kabul edilirse yine proxy sunucu yardımı ile onay mesajları takası yapılır. Sonrasında taraflar arasında RTP oturumu başlar (Şekil 3.10).



Şekil 3.10 Proxy sunucu üzerinden SIP çağrı kurulumu (Orrblad, 2004)

3.4 SIP ve H.323 Protokollerinin Karşılaştırılması

H.323, ITU-T tarafından geliştirilen bir sinyalleşme protokolü iken SIP ise IETF tarafından geliştirilmiş bir protokoldür. SIP ile H.323 arasındaki farkların bir kısmı geliştiricileri olan IEEE ve ITU-T arasındaki farklardan kaynaklanmaktadır. Bilindiği gibi IEEE aynı zamanda internet'in bel kemiği olan TCP/IP'nin de mucididir. IEEE açık protokoller, ITU-T ise kapalı ve kompleks protokoller geliştirmeyi sever. ITU-T köklü ve eski bir kurum olduğundan gelenekçidir. IEEE ise bilişim dünyasını arkasından sürükleyen yenilikçi bir kurumdur.

H.323 protokolü SIP protokolüne göre daha kompleks ve daha geniş düşünülmüş, güvenilirliği daha fazla olan bir protokoldür. Yük dengeleme (load balancing) ve otomatik hata düzeltme (failover) gibi üst düzey erişilebilirlik seçenekleri ile H.323 daha fazla güven vermektedir. Ayrıca ASN.1 formatındaki ikili kodlanmış H.323 paketleri çok daha az bant genişliği tüketirken güvenlik duvarı/NAT uygulamalarında problemlere sebep olabilmektedir. SIP mesajları ise ASCII formatında olduğundan insanların okuması ve hata ayıklaması kolaydır. Fakat bu mesaj yapısı daha fazla bant genişliği tüketmektedir.

H.323 ve SIP protokollerinin karşılaştırılması Çizelge 3.1’de özet olarak verilmektedir.

Çizelge 3.1 H.323 ve SIP protokollerinin karşılaştırılması

	H.323	SIP
Mimari	ITU-T	IETF
Mesaj Formatı	ASN.1 (Binary)	ASCII düz metin
Bant Genişliği Tüketimi	Az	Çok fazla
Adres Yapısı	Her bir fiziksel giriş için bir adres.	Her bir kullanıcıya e-mail yapısında bir adres atanır.
Komplekslik	Yüksek (Çünkü H.225, H.245, H.235, T120 vb. gibi birçok protokolü barındırmaktadır)	Düşük
Ölçeklenirlik	Zayıf (Çünkü başlangıçta LAN ağları düşünülerek tasarlanmış)	Yüksek (WAN ağları için tasarlanmıştır). Zamanla yeni özellikler bu protokole kazandırılabilir
Gecikme	Kompleks sinyalleşme yapısı nedeniyle yüksek	Basit yapısı nedeniyle düşük.
Güvenlik	H.235 güvenlik profilini kullanmaktadır. Bununla birlikte TLS, IPSec vb. güvenlik protokolleri kullanılabilir	HTTPS, TLS, MIME, IPSec vb. güvenlik protokolleri kullanılabilir

4. VOIP TEKNOLOJİSİNİN GÜVENLİK AÇIKLARI

Bu bölümde VoIP sistemlerine büyük zararlar verebilecek güvenlik risklerine değinilecektir. Bir risk; bir güvenlik açığı gibi düşünülebildiği gibi bir tehdit olarak da düşünülebilmektedir. Bir tehdit bir VoIP sistemine zarar verebilecek potansiyele sahip bir takım durumları ifade ederken; bir güvenlik açığı, sistem içerisindeki zayıflıkları ifade etmektedir.

Risk problemleri daha az güvenli olan açık ağlarda karşımıza çıkabildiği gibi kapalı ağlarda da söz konusu olabilmektedir. Açık ağlar internetin olduğu her yerde ve her zaman herkesin erişebildiği ağlardır ve herhangi bir ön kayıt gerektirmez. Kapalı ağlar ise güvenliğin daha fazla olduğu ağları ifade eder. Örneğin erişimci sayısı maksimum dört kişi ile sınırlandırılan bir ağ kapalı bir ağdır. Başka bir örnek verecek olursak, firma çalışanlarının şirket ağına sadece firma içerisindeyken erişebildiği yani, şirket dışından (internet üzerinden) erişemediği bir ağ da kapalı bir ağdır. Bu yapıda çalışanlar sadece intranet adı verilen şirket içi ağda VoIP görüşmesi yapabilirken internet üzerinden yapamamaktadır.

Bu bölümde kapalı bir ağ yapısındaki riskleri ve muhtemel saldırıları tanımlamak için üç soru cevaplanacaktır. Bu sorular:

- VoIP ile birlikte şirketler hangi tehditlere maruz kalabilmektedir?
- Bir VoIP görüşmesi hangi güvenlik açıklarını da beraberinde getirmektedir?
- VoIP sistemlerine karşı gerçekleştirilen atakların muhtemel sonuçları nelerdir?

4.1 Servis Reddi Saldırıları (DoS- Denial of Service Attacks)

DoS saldırıları genelde TCP/IP protokol yapısındaki açıklardan faydalanıp bir sunucuya çok sayıda istek yönelterek onu tıkamaya sebep olan saldırılardır.

VoIP sistemleri QoS gereksinimlerinden dolayı diğer data sistemleri ile karşılaştırıldığında DoS saldırılarına karşı çok daha savunmasızdır. VoIP gerçek-zamanlı bir uygulamadır ve dolayısıyla da ses paketlerinin kısa zaman periyodu içerisinde iletimi çok önemlidir. Örneğin iki VoIP terminali arasındaki 150 ms'nin üzerindeki bir gecikme VoIP görüşmesinin kabul edilemez bir hale gelmesine sebep olacaktır.

DoS saldırılarının amacı bir sisteme yetki dahilinde olunmadığı halde ulaşmak değildir. Bunun aksine, yetkili kullanıcıların mevcut sisteme ve servislere erişmesini engellemektir. Burada saldırganın amacı saldırılar sayesinde rakiplerinin sistemlerini çökertmek ya da QoS

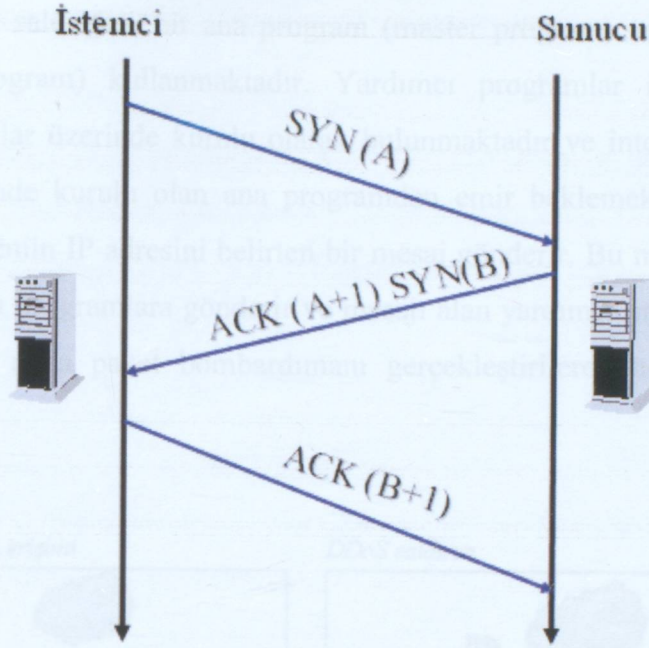
oranını azaltarak sistemlerin istenildiği gibi çalışmamasına sebep olup, müşteri memnuniyetini olumsuz yönde etkilemek olabilmektedir.

Bir DoS saldırısını gerçekleştirmenin birden fazla yolu bulunmaktadır. Örneğin bir saldırgan, bir hedef VoIP sistemine paketler göndererek sistemin çökmesine ve görevlerini yerine getirememesine sebep olabildiği gibi sistemin data yoğunluğunun artmasına ve yasal kullanıcılardan gelen çağrı isteklerini reddetmesine de sebep olabilmektedir. Bir VoIP sistemin sınırlı bir kapasitesi bulunmaktadır. Herhangi bir saldırı olmaksızın yasal kullanıcılardan gelen isteklerin bu kapasiteyi zorlaması dahi bir DoS saldırısı etkisi yaratabilmekte ve sistemi olumsuz yönde etkileyebilmektedir. Başlıca DoS saldırıları aşağıda verilmiştir:

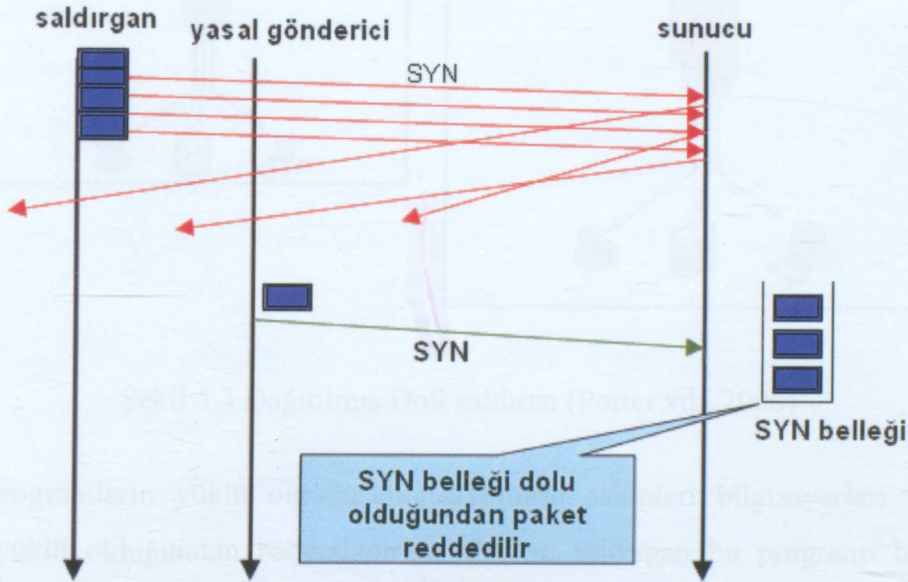
Tampon taşması (Buffer overflow): Tampon taşması saldırısı çok bilinen ve saldırganlar tarafından çok kullanılan bir DoS saldırı çeşididir. Tampon taşması, bir program ya da işlemin tamponuna istenilenden çok daha fazla datayı yüklemeye çalışmasından kaynaklanmaktadır. Bir tampon sınırlı bir data kapasitesine sahiptir. Bu tampona kapasitenin üzerinde ekstra datanın yüklenmeye çalışılması sistemin çökmesine sebep olacaktır. Bu saldırının amacı VoIP sistemlerine aşırı data yollayarak işlem tamponunun kapasitesinin dolmasına ve sistemin çalışmamasına neden olmaktır.

Senkronizasyon baskını (SYN flood): Bilindiği üzere bir TCP bağlantısı üç-yollu bir anlaşma (three-way handshake) ile gerçekleşmektedir (Şekil 4.1). Bir sunucu herhangi bir TCP paketi aldığı anda, ki bu pakette istemcinin set edildiği senkronizasyon bayrağı (SYN flag) bulunmaktadır, sunucu bağlantı için belirli bir bellek ayırarak istemciye SYN ve ACK bayraklarını içeren bir TCP paketi gönderecektir. Ayrılan bellek, istemcinin bir ACK paketi göndererek üç-yollu anlaşmayı sonlandırmasıyla serbest bırakılır.

SYN baskını saldırısında, bir saldırgan sahte bir kaynak IP adresi ile hedef sisteme ya da sunucuya birden fazla TCP SYN paketi gönderir (Şekil 4.2). Sunucu bu sahte kaynak IP adresinden hiçbir zaman ACK paketi almayacaktır. Bu nedenle de sunucu tarafından ayrılmış olan bellek hiçbir zaman serbest bırakılmayacaktır. Bu yarı açık kalmış TCP bağlantılarının sayısının çok sayıda olması durumunda sunucu belleği tamamen dolacaktır. Bu durum da sunucuya sonrasında gelecek olan yasal TCP bağlantılarının kurulamamasına sebep olacaktır.



Şekil 4.1 TCP bağlantısının kurulması

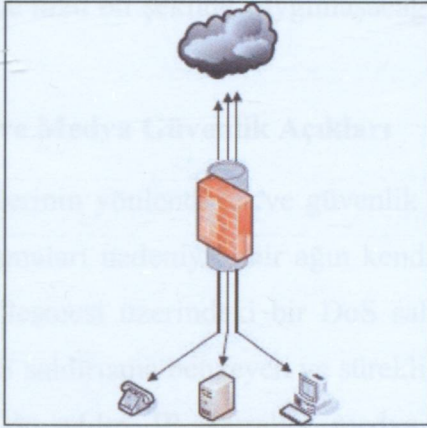


Şekil 4.2 SYN baskını saldırısı

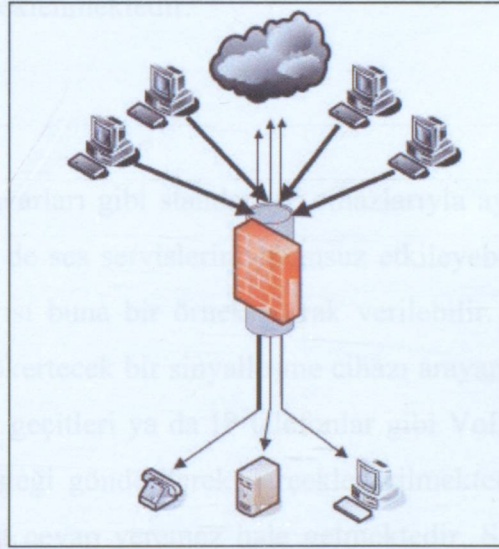
Dağıtılmış DoS (DDoS-Distributed DoS DDoS): Adından da anlaşılacağı üzere bu saldırı çeşidinde saldırı, saldırıları gerçekleştirmek için dağıtılmış teknikleri kullanmaktadır. DDoS saldırısı belirli bir sistem üzerine eşzamanlı olarak birden fazla DoS saldırısının gerçekleştirilmesi anlamına gelmektedir (Şekil 4.3). İnternetteki birden çok bilgisayar üzerinden eş zamanlı olarak bir sistem üzerine yapılan SYN baskınları buna örnek verilebilmektedir.

Bu saldırı çeşidinde saldırgan, bir ana program (master program) ve birden fazla yardımcı program (slave program) kullanmaktadır. Yardımcı programlar internette birden fazla noktadaki bilgisayarlar üzerinde kurulu olarak bulunmaktadır ve internet üzerinde herhangi bir bilgisayar üzerinde kurulu olan ana programdan emir beklemektedirler. Saldırgan ana programa hedef sistemin IP adresini belirten bir mesaj gönderir. Bu mesajı alan ana program aynı mesajı yardımcı programlara gönderir ve mesajı alan yardımcı programlar vasıtasıyla da hedef sisteme aynı anda paket bombardımanı gerçekleştirilerek hedef sistemin çökmesi sağlanır.

Tipik internet erişimi



DDoS saldırısı



Şekil 4.3 Dağıtılmış DoS saldırısı (Porter vd., 2006)

Yardımcı programların yüklü olduğu bilgisayarların sahipleri bilgisayarları üzerinde bu programın yüklü olduğundan habersizdirler. Çünkü, saldırgan bu programı bilgisayarlara sahiplerinin haberi olmadan virüs olarak yüklemiştir. Ana programdan yardımcı programlara mesaj gönderilirken kullanılan ve ana programı ifade eden kaynak IP adresi genellikle sahte olmaktadır. Bu durum ana programın yüklü olduğu bilgisayara ulaşmayı imkansız hale getirmektedir. Ancak, saldırıları gerçekleştiren yardımcı programların hedef sisteme doğru gönderdiği paketlerdeki kaynak IP adresleri sayesinde yardımcı programların yüklü olduğu bilgisayarlara ulaşmak mümkündür.

4.2 İnternet Telefonculuğu Üzerinden Spam (SPIT-Spam over Internet Telephony)

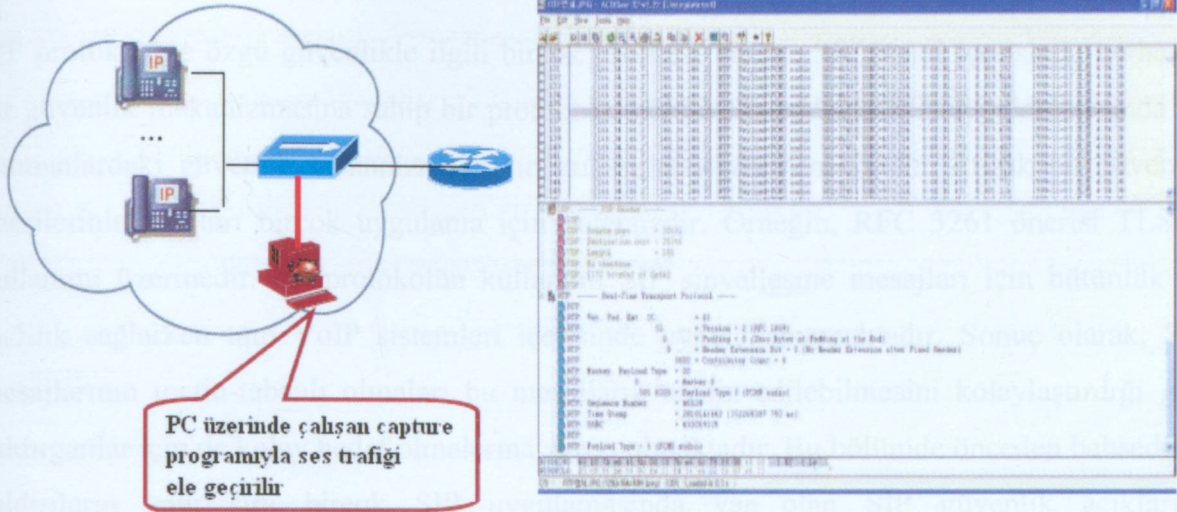
SPIT saldırıları internet üzerinden istenilmeyen çağrıların taşınması yani kullanıcılara boş çağrıların iletilmesi şeklinde ifade edilebilir. SPIT çağrıları e-mail spam'lerine benzemektedir. Bu saldırılar sayesinde aranan kişilere boş çağrılar iletilerek gereksiz data yoğunluğu oluşturulmaktadır. SPIT çağrılarının yoğun olarak gönderilmesi durumunda tüm telefonların meşgul edilerek daha sonraki yasal çağrıların ulaşılamamasına bu nedenle de müşteri memnuniyetinin düşmesine sebep olmaktadır.

SPIT çağrılarını filtrelemek e-mail spam'lerini filtrelemekten çok daha zordur. Çünkü gelen çağrılar yasal olup olmadığının anlaşılması hemen hemen imkansızdır. SPIT saldırılarının günümüzde hızlı bir şekilde yaygınlaşacağı beklenmektedir.

4.3 Ağ ve Medya Güvenlik Açıkları

Ses paketlerinin yönlendirici ve güvenlik duvarları gibi standart IP cihazlarıyla aynı fiziksel ağı paylaşmaları nedeniyle, bir ağın kendisi de ses servislerini olumsuz etkileyebilmektedir. Ses sinyalleşmesi üzerindeki bir DoS saldırısı buna bir örnek olarak verilebilir. Bu saldırı klasik DoS saldırısına benzeyen ve sürekli çökertecek bir sinyalleşme cihazı arayan bir saldırı çeşididir. Bu saldırı, IP santraller, medya ağ geçitleri ya da IP telefonlar gibi VoIP cihazları üzerine bir yığın sürekli ses sinyalleşme isteği gönderilerek gerçekleştirilmektedir. Saldırı sonrasında hedef VoIP cihazı yasal isteklere cevap veremez hale gelmektedir. Saldırganlar eğer VoIP hizmetinin de mevcut olduğu bir ağa erişim imkanı bulduysa, bu imkan sayesinde ağ içerisindeki VoIP cihazlarına yüksek boyutlu RTP paketlerini kolayca ulaştırabilmektedir.

Medya üzerindeki diğer bir önemli güvenlik açığı ise gizli dinlemedir (eavesdropping). Her ne kadar bazı VoIP çağrıları şifrelense de, bir çok kullanıcı ses paketlerinin şifrlenmesi için herhangi bir metot kullanmamaktadır. Hatta, eğer güçlü bir doğrulama mekanizması kullanılmazsa, ses paketlerinin şifrlenmesi bile gizli dinleme problemini garanti edemez. Gizli dinleme genellikle ortadaki adam (man-in-the-middle) adı verilen bir saldırı metoduyla gerçekleştirilir. Eğer saldırgan bir şekilde şifrelenmiş bir medyaya ulaşırsa, bu şifreli medyayı çeşitli programlar kullanarak kolaylıkla normal şifrelenmemiş ses dosyası haline getirebilmektedir (Şekil 4.4).



Şekil 4.4 Gizli dinleme (Won, 2006)

4.4 IP ve Yazılımsal Telefonların (Softphone) Güvenlik Açıkları

IP telefonlar ve yazılımsal telefonlar VoIP ağının en az kritik bileşenleri olmalarının yanı sıra en çok kullanılan ve en az kontrol edilebilir bileşenleridir. IP telefonların ve yazılımsal telefonların temel fonksiyonellikleri IP ağı üzerinden ses hizmeti sağlamalarıdır. Bu bileşenler üzerine gerçekleştirilen saldırılar oldukça sıktır. Çünkü bir saldırgan için bir IP telefon satın alıp kullanmak ve farklı tip saldırı ataklarını tecrübe etmek hem çok ucuz hem de çok basittir. IP telefonların ve yazılımsal telefonların temel güvenlik açıkları aşağıda belirtilmiştir:

DoS: IP/yazılımsal telefonlar üzerine gerçekleştirilen DoS saldırıları telefonların kendilerini kapatmalarına ya da konfigürasyonlarının değişmesine bu sayede de telefonların kullanılamamasına sebep olmaktadır.

İzinsiz Erişim: Saldırganlar çeşitli saldırılarla IP/yazılımsal telefona erişim imkanı bulursa telefondan gerçekleşen tüm görüşmeleri dinleyebilir, telefon üzerinden istediği görüşmeleri gerçekleştirebilir ya da telefonu kullanılamaz hale getirebilir. Bu tarz saldırılara ortadaki adam saldırısı örnek olarak verilebilir. Saldırgan telefonlar üzerinden gerçekleşen tüm görüşmeleri kendi sunucusuna yönlendirerek bu saldırıyı gerçekleştirir.

Virüsler: Özellikle bilgisayarlarda yazılımsal telefonların kullanılması, internet üzerinden çeşitli virüslerin bilgisayara ulaşmasını sağlayan açık bir kapı olarak görülebilmektedir. Bilgisayar üzerinde eğer herhangi bir güvenlik programı yüklü değilse, virüsler bilgisayarlara oldukça önemli zararlar verebilmektedir.

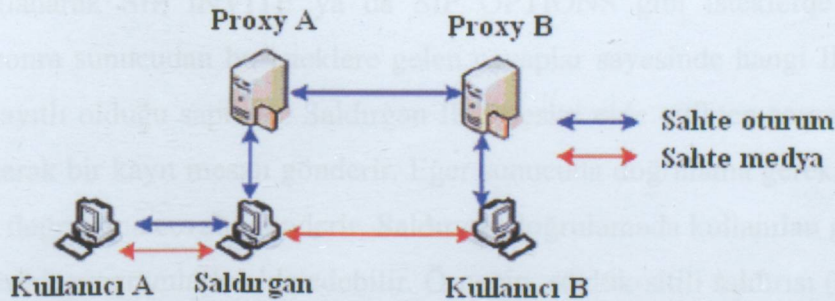
4.5 SIP Protokolü Güvenlik Açıkları

SIP protokolüne özgü güvenlikle ilgili birçok problem vardır. SIP kendi içerisinde herhangi bir güvenlik mekanizmasına sahip bir protokol değildir. Bu nedenle SIP uygulamalarında alt katmanlardaki güvenlik mekanizmalarının kullanılması önerilmektedir. Ancak bu güvenlik önerilerinin bazıları birçok uygulama için yetersizdir. Örneğin, RFC 3261 önerisi TLS'in kullanımı üzerinedir. Bu protokolün kullanımı SIP sinyalleşme mesajları için bütünlük ve gizlilik sağlarken tüm VoIP sistemleri içerisinde uygulanamamaktadır. Sonuç olarak, SIP mesajlarının metin-tabanlı olmaları bu mesajların analiz edilebilmesini kolaylaştırdığı gibi saldırganlar için de kolay hedef olmalarına sebep olmaktadır. Bu bölümde önceden bahsedilen saldırıların yanı sıra birçok SIP uygulamasında var olan SIP güvenlik açıklarına değinilecektir. Bunlardan en yaygın olanları şu şekildedir (Kultti, 2005):

- Kayıt Sahteciliği (Registration Hijacking).
- Proxy Taklit Etme (Proxy Impersonation).
- Mesaj Değiştirme (Message Tampering).
- Oturum Sonlandırma (Session Tear Down).

4.5.1 Kayıt Sahteciliği (Registration Hijacking)

SIP protokolünde tüm katılımcılar (IP telefonlar, VoIP ağ geçitleri, vb.) bir proxy sunucusuna kayıt olurlar. Bu sayede herhangi bir katılımcıya gelen tüm çağrılar bu sunucu üzerinden iletilir. Kayıt sahteciliğinde bir saldırgan geçerli bir katılımcıyı taklit ederek kendi adresi ile yasal katılımcının yerini alır ve SIP proxy sunucusuna kayıt olur (Şekil 4.5). Bu durum tüm gelen çağrıların sunucu tarafından yasal kullanıcı yerine sahte kullanıcıya iletilmesine sebep olmaktadır. Böylece saldırgan görüşmeleri dilediği gibi dinleyebilir ve kaydedebilir.



Şekil 4.5 Kayıt sahteciliği (Luthra ve Ashraf, 2005)

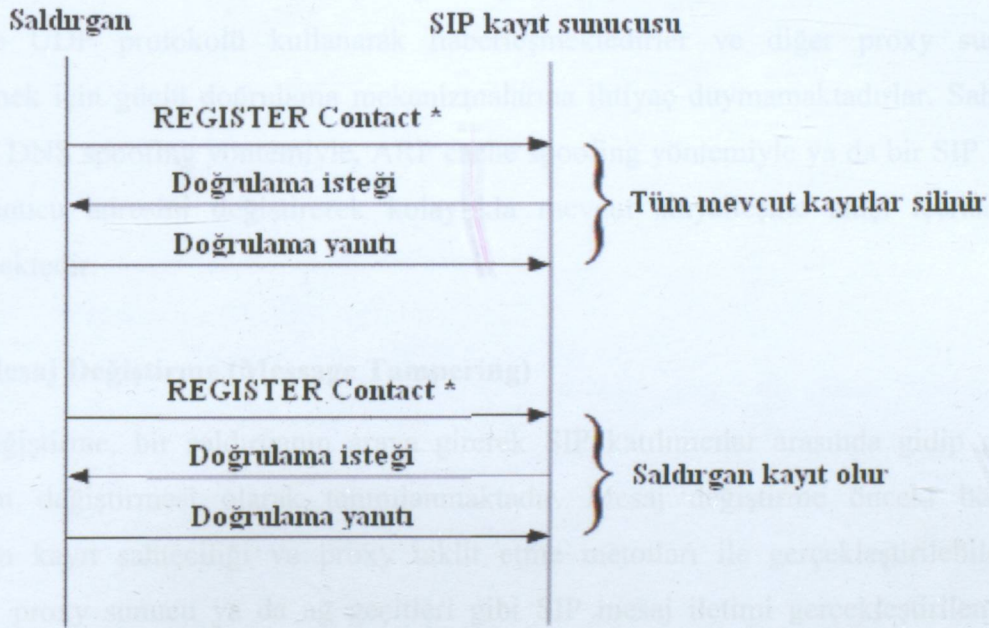
Kayıt işlemi genellikle güvenli olmayan UDP protokolü üzerinden gerçekleştirildiğinden dolayı işlem sırasında herhangi bir güvenlik mekanizması uygulanmamaktadır. Bu nedenle de kayıt sırasındaki mesajların taklit edilmesi çok kolaydır. Ayrıca, birçok SIP sunucusunda kayıt isteklerinin doğrulanması gerçekleştirilmemektedir ve hatta doğrulama kullanıldığı durumda da katılımcıya atanan kullanıcı adı ve şifre bilgilerinin basit bir şifreleme metodu kullanılarak iletilmesi çok sağlıklı bir metot olmamaktadır.

Genelde SIP kayıt işlemleri için ileriki bölümlerde ayrıntılı olarak değinilecek olan MD5 tek yönlü özetleme algoritması kullanılması önerilmektedir. Bu algoritma bir SIP kayıt mesajı gibi bir girdiyi alır ve bu girdiye özel şifrelenmiş tek bir çıktı oluşturur. Bu çıktıyı parmak izi gibi düşünebiliriz. Girdideki tek bir bitin değişmesi tamamen farklı bir parmak izinin oluşmasına sebep olacaktır. MD5 algoritmasında kullanılan zaman (nonce) parametresi sayesinde aynı girdi için farklı zamanlarda farklı parmak izlerinin oluşturulması sağlanır. Bu da güvenliği artırır. Normalde karma çakışmalarının olması yani iki farklı mesaj için aynı parmak izinin oluşturulması çok zordur. Bir saldırgan standart bir bilgisayar ile birkaç saat içerisinde bir karma çakışması oluşturabilir. Ancak, belirli bir mesaj yazmak ve bu mesajı belirli bir parmak izi ile atamak çok zaman gerektiren bir işlemdir. SIP için tanımlanmış mevcut RFC 3261 modeli, kayıt doğrulamasında MD5 metodunun kullanılmasını önermektedir ve sadece bu metoda izin vermektedir. Bir önceki model olan RFC 2543 modelinde olduğu gibi kullanıcı adı ve şifre bilgilerinin açık metin olarak iletildiği basit metotların kullanılması önerilmemektedir.

Kayıt sahteciliğinin ilk adımında SIP proxy sunucusunda kayıtlı bir IP adresi bulunur. Bu işlem sunucuya kayıtlı adreslerin yapısını bilen içerdeki kullanıcılar için çok kolaydır. Dışarıdaki saldırganlar için ise bu işlem ancak tarama programları gibi bazı bilgisayar programları ile mümkün olmaktadır. Bir tarama programı tek bir istek gönderebildiği gibi aynı anda birden fazla istek de gönderebilir. Tarama programı SIP sunucusuna farklı IP adreslerini kullanarak SIP INVITE ya da SIP OPTIONS gibi isteklerde bulunur. İstek gönderdikten sonra sunucudan bu isteklere gelen cevaplar sayesinde hangi IP adreslerinin o an sunucuda kayıtlı olduğu saptanır. Saldırgan IP adresini elde ettikten sonra sunucuya o IP adresini kullanarak bir kayıt mesajı gönderir. Eğer sunucuda doğrulama gerekiyorsa sunucu o IP adresine bir doğrulama cevabı gönderir. Saldırgan doğrulamada kullanılan geçerli kullanıcı adı ve şifreyi farklı programlarla elde edebilir. Örneğin, sözlük-sitili saldırısı (dictionary-style attack) adı verilen bir metot ile saldırgan farklı kullanıcı adı ve şifreler üreterek teker teker tüm olasılıkları alfabe sırasına göre dener. Ancak bu metot çok zaman alan bir metottur.

Bunun dışında daha az zaman alan daha farklı mantıkla çalışan daha hızlı programlar da mevcuttur. Ayrıca bu tarz bir deneme-yanılma uygulamasında VoIP sisteminin yönetici tarafından gözlenmesi gerekmektedir. Bu sayede yönetici bu yoğun hata mesajlarını fark edecek ve gerekli önlemleri alacaktır.

Hedef adres belirlendikten sonra, artık hedefin yerine sahte kayıt işlemi gerçekleştirilebilir. Saldırganın ilk yapacağı şey yasal katılımcının SIP sunucudan silinmesini sağlamaktır. Sonrasında ise kendisi yasal sunuymuş gibi davranıp SIP sunucusuna kayıt olur. Saldırgan sunucunun tüm varolan kayıtları silmesi için sunucuya hileli bir Kayıt (Register) mesajı gönderir. Bu mesajda IP adresi bilgisini içeren “Contact” başlığı yıldız (*) simgesinden oluşmaktadır. Bununla birlikte kayıt geçerlilik süresini gösteren “Expires” başlığı ise 0 olarak tanımlanmaktadır. Bu kayıt mesajını alan sunucu tüm kayıtlı katılımcıların kaydını siler. Bu andan itibaren saldırırganın yapacağı ikinci şey hazır yasal katılımcı sunucuya kayıtlı değilken sunucuya sahte bir kayıt mesajı göndererek yasal katılımcı adına sunucuya kayıt olur (Şekil 4.6).

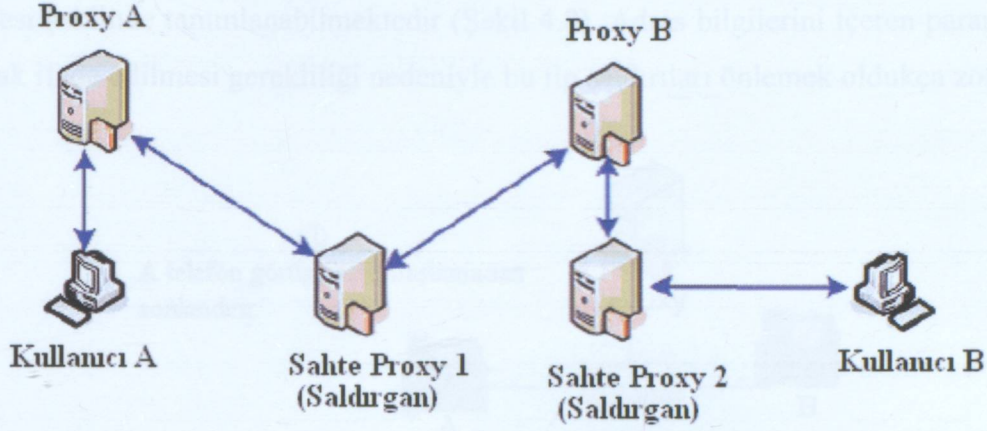


Şekil 4.6 Kayıt sahteciliğinde saldırırganla SIP sunucusu arasındaki mesajlaşma

4.5.2 Proxy Taklit Etme (Proxy Impersonation)

Proxy taklit etme, bir saldırırganın kendi yasal olmayan proxy sunucusunu kullanarak yasal bir katılımcıdan yasal SIP proxy sunucusuna gönderilen çağrılarını kendisine yönlendirmesi olarak tanımlanabilmektedir (Şekil 4.7). Saldırgan yasal proxy sunucuyu taklit ederek tüm SIP

mesajlarına erişim imkanını elde edebilmekte ve çağrılarının tüm kontrolünü ele geçirebilmektedir. Saldırgan yasal katılımcıları ve yasal proxy sunucuyu kendi yasal olmayan proxy sunucusu ile haberleşmesini sağlayacak şekilde kandırabilir.



Şekil 4.7 Proxy taklit etme (Luthra ve Ashraf, 2005)

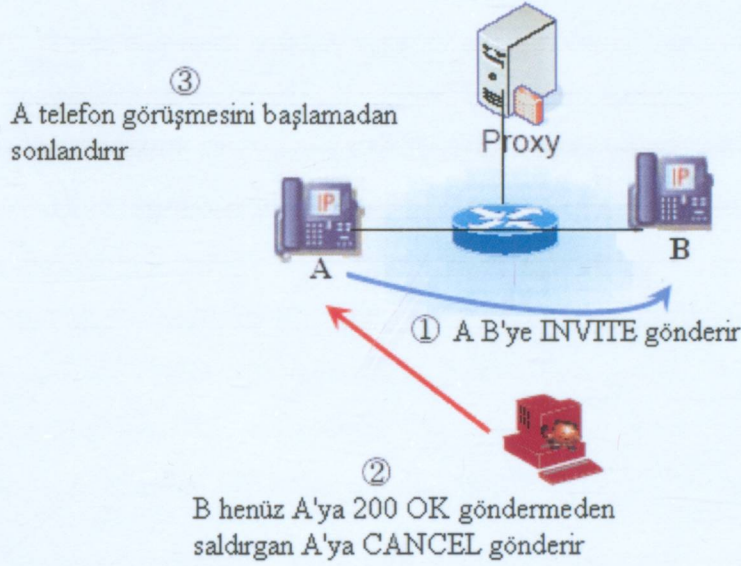
Bir proxy taklit etme saldırısı birçok yolla gerçekleştirilebilir. Katılımcılar ve sunucular genellikle UDP protokolü kullanarak haberleşmektedirler ve diğer proxy sunucularla haberleşmek için güçlü doğrulama mekanizmalarına ihtiyaç duymamaktadırlar. Sahte proxy sunucusu DNS spoofing yöntemiyle, ARP cache spoofing yöntemiyle ya da bir SIP cihazının proxy sunucu adresini değiştirerek kolaylıkla mevcut sinyalleşme akışı içerisine dahil edilebilmektedir.

4.5.3 Mesaj Değiştirme (Message Tampering)

Mesaj değiştirme, bir saldırıncının araya girerek SIP katılımcılar arasında gidip gelen ses paketlerini değiştirmesi olarak tanımlanmaktadır. Mesaj değiştirme önceki bölümlerde bahsedilen kayıt sahteciliği ve proxy taklit etme metotları ile gerçekleştirilebildiği gibi doğrudan proxy sunucu ya da ağ geçitleri gibi SIP mesaj iletimi gerçekleştirilen cihazlar üzerine yapılan saldırılar vasıtasıyla da gerçekleştirilebilmektedir. Bu tip saldırıları engellemek için şifreleme ve doğrulama yoluyla SIP mesajları gibi düz metin yapısındaki mesajların güvenliğini sağlayabilen S/MIME metodu kullanılabilir. Ancak, S/MIME metoduna rağmen SIP mesajlarının düz metin yapısında olması nedeniyle bir saldırıncı yönlendirme bilgisi sayesinde kolayca bu saldırıyı gerçekleştirebilir.

4.5.4 SIP Oturumu Sonlandırma (SIP Session Tear Down)

SIP oturumu sonlandırma, bir saldırganın SIP mesajları içerisindeki 'To' ve 'From' gibi arayan ve aranan katılımcıları belirten bazı oturum parametrelerini gözlemlemesi ve araya bir BYE , CANCEL ya da RE-REGISTER gibi oturumun sonlanmasına sebep olan bir mesaj göndermesi şeklinde tanımlanabilmektedir (Şekil 4.8). Adres bilgilerini içeren parametrelerin açık olarak ifade edilmesi gerekliliği nedeniyle bu tip saldırıları önlemek oldukça zordur.



Şekil 4.8 SIP oturumu sonlandırma saldırısı (Won, 2006)

4.6 H.323 Protokolü Güvenlik Açıkları

H.323 yıllardır kullanılan bir VoIP protokolüdür ve H.235 güvenlik mekanizmalarının ilave edilmesinden bu yana güvenli bir protokol olarak bilinmektedir. H.323 protokolünde güçlü doğrulama mekanizmaları kullanıldığından ve aynı zamanda medya akışının da güvenli olmasından dolayı SIP için bahsedilen güvenlik problemleri H.323 protokolünün sadece bazı uzantıları için geçerlidir.

H.323 protokolündeki güvenlik problemleri geçmişte saptanmıştır. Ulusal Altyapı Güvenlik Düzenleme Merkezi (NISCC, National Infrastructure Security Co-ordination Centre) tarafından 2004 Ocak ayında farklı H.323 uygulamalarına ait birçok güvenlik açığı keşfedildi. Bu güvenlik açıkları arasında en önemlisi tampon taşması (buffer overflow) saldırısıdır. Bu saldırıda saldırgan H.323 konuşan bir VoIP cihazına özel ASN.1 paketleri göndererek bir DoS saldırısı gerçekleştirir ve bu sayede H.323 VoIP cihazı üzerinde yüklü bir data yoğunluğuna sebep olarak sistemin çökmesine sebep olur. Bu saldırıdan etkilenebilen H.323 protokolünü

5. İNTERNET PROTOKOLÜ ÜZERİNDEN SES İLETİMİNDE GÜVENLİK

Bir önceki bölümde bahsedilen VoIP güvenlik saldırıları hem VoIP hizmeti veren operatörleri hem de bu hizmeti alan firmaları ve son kullanıcıları büyük ölçüde tehdit etmektedir. Bu saldırıların genel amaçları arasında ücretsiz konuşmak, kimlik ve bilgi çalmak ya da kullanıcıları rahatsız etmek sayılabilmektedir. VoIP teknolojisindeki güvenlik tehditleri IP dünyasındaki VoIP'e özel olmayan diğer tehditleri de içermektedir. Bu nedenle, IP ağının güvenliği için alınması gereken önlemler, VoIP güvenliği için de gereklidir.

VoIP güvenliğini sağlamak amaçlı alınabilecek önlemler arasında en önemlileri şu şekildedir:

1. Standart bir VoIP ağında, ses ve veri paketleri aynı ağda bulunmakta ve bu nedenle de birbirlerinden etkilenmektedirler. Örneğin, veri iletiminin yapıldığı IP ağına yapılan bir saldırı, tüm ağdaki ses görüşmelerine de zarar verecektir. Bu nedenle alınması gereken en önemli önlemlerden biri, ses ve veri trafiğini birbirinden ayırmaktır. Bunun için de ses ve veri trafiği için ayrı Sanal Yerel Alan Ağları (VLAN-Vitual LAN) kullanılarak ses trafiği izole edilmelidir. Ayrıca Erişim Listeleri (ACL-Access List) kullanılarak ses ve veri VLAN'leri arasında erişimler kısıtlanmalıdır.
2. Kullanılan VoIP protokolüne özgün ses ve sinyalleşme paketleri şifrelenmelidir.
3. VoIP ağında bulunan sunuculara istenmeyen kişilerin erişmesini engellemek amacıyla cihazlara Telnet erişimi kısıtlanmalıdır.
4. VoIP ağının güvenliği için güvenlik duvarları (firewall) kullanılmalı ve Ağ Adres Çevrimi (NAT-Network Address Translation) yapılmalıdır.
5. DoS saldırılarına karşı dayanıklılık sağlaması açısından VoIP ağındaki sunucular için yedeklilik sağlanmalıdır.

Bu bölümde, VoIP teknolojisinde güvenliğin sağlanmasında en önemli rolleri oynayan şifreleme algoritmaları ve güvenlik duvarı/NAT uygulamaları konularına ayrıntılı olarak değinilecektir.

5.1 Veri Şifreleme (Kriptoloji) Metotları

İki katılımcı arasında güvenli oturumların kurulmasını sağlamak amacıyla katılımcılar arasındaki datalar DES (Data Encryption Standard), 3DES (Triple-DES), vb. gibi **şifreleme metotlarıyla** şifrelenirler. Bu şifreleme metotları veri şifreleme işlemi şifreleme anahtarları

ile gerçekleştirmektedir. Tüm katılımcıların (VoIP cihazlarının) veri şifrelemede kullanılan bu anahtarlardan haberdar olmaları gerekmektedir. Yani katılımcılar kullanılan anahtar konusunda mutabakata varmalıdırlar. Bu nedenle de veri şifrelemede kullanılan bu anahtarların katılımcılar arasında takası gerekmektedir.

Her katılımcı diğer katılımcının kullandığı anahtar bilgisine sahip olmalıdır ki diğer katılımcının gönderdiği şifreli datayı çözebilsin. Tam bu noktada yani, kullanılan ortak anahtarların takası noktasında anahtarların takasının güvenilirliği söz konusudur yani, katılımcılar arasındaki anahtar takasının güvenli bir şekilde yapılması gerekmektedir. Aksi taktirde, veri şifrelemede kullanılan bu anahtarların kötü niyetli kişiler tarafından ele geçirilmesi ve bunun sonucunda da katılımcılar arasındaki şifreli verinin açığa çıkması söz konusu olur. Bu nedenle, katılımcılar arasındaki anahtar takasını güvenli bir şekilde yapılmasını sağlayan Ön-Paylaşımlı Anahtar Anlaşma Metodu (PSK-Pre-Shared Key Agreement), Açık Anahtar Altyapısı (PKI-Public Key Infrastructure) gibi **anahtar anlaşma/takas metotları** kullanılmaktadır. Anahtar takası, ilgili anahtarların diğer katılımcıya şifrlenip gönderilmesiyle gerçekleştirilmektedir. Bu sayede katılımcılar arasındaki verinin şifrlenmesini ve bu şifrlenmiş verilerin tekrar çözülmesini sağlayan anahtarlar katılımcılar arasında güvenli bir şekilde iletilebilmektedir..

Katılımcıların veri şifrelemede kullanılan şifreleme metotlarının, şifrelemede ve şifre çözmede kullanılan anahtarların takası için kullanılan metotların ve bu metotların kendilerine özgü kullandıkları güvenlik parametrelerinin neler olduğu konusunda mutabakata varmaları yani anlaşmaları gerekmektedir. Bu nedenle de tüm bu anahtarlama işlemlerini yönetmek ve katılımcıların kullanılan metotlar ve parametreler konusunda anlaşmasını sağlamak amacıyla Internet Anahtar Takası (IKE- Internet Key Exchange), Çoklu Ortam Internet Anahtarlama (MIKEY-Multimedia Internet KEYing), vb. gibi **anahtar yönetim protokolleri** kullanılmaktadır. Bu protokoller veri şifrelemede kullanılan ilgili anahtarların üretilmesini sağladıkları gibi şifrelemeyle ilgili parametrelerin katılımcılar arasında belirlenmesini sağlayan mekanizmaları yönetmekte de kullanılmaktadırlar.

Katılımcılar arasındaki şifreleme metotlarının, anahtar takas metotlarının ve anahtar yönetim protokollerinin kullanılmasını sağlayan Güvenli Gerçek Zamanlı Taşıma Protokolü (SRTP-Secure Real-Time Transport Protocol), Internet Protokolü Güvenliği (IPSec-IP Security), vb. gibi **güvenlik protokolleri** kullanılmaktadır. Bu güvenlik protokolleri sayesinde katılımcılar hangi anahtar yönetim protokolünün ve hangi anahtar takas metodunun kullandığını bilmektedirler.

Özetle, katılımcılar arasında güvenli oturumların kullanılmasını sağlayan belirli bir güvenlik protokolü bulunmaktadır. Her bir güvenlik protokolü de belli bir anahtar yönetim protokolünü kullanmaktadır. Örneğin SRTP protokolü anahtar yönetim protokolü olarak MIKEY protokolünü kullanırken; IPsec protokolü anahtar yönetim protokolü olarak IKE protokolünü kullanmaktadır. Her bir anahtar yönetim protokolü sayesinde de katılımcılar arasında kullanılan veri şifreleme metotları ve anahtar takas metotları konusunda mutabakata varılmaktadır.

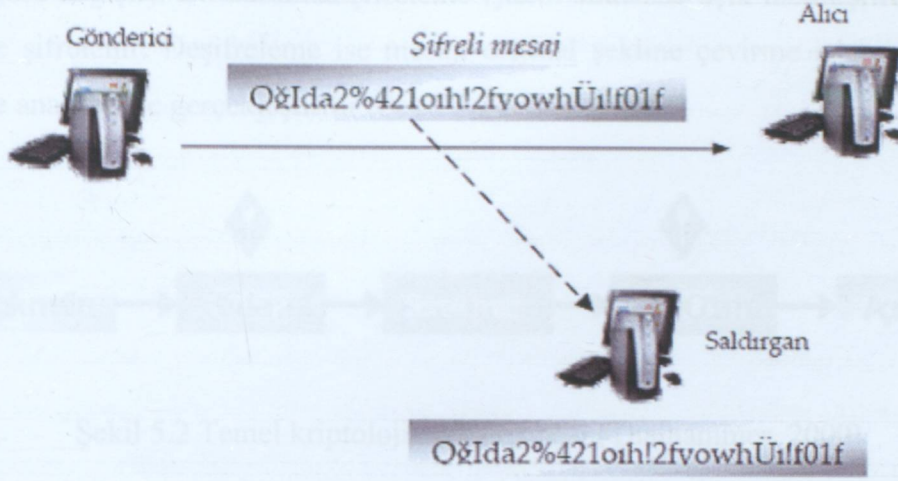
5.1.1 Veri Şifrelemeye Giriş

Kriptoloji Romalılar zamanından beri var olup 2. dünya savaşı gibi modern savaşlarda önemli rol oynamıştır (Thalhammer, 2000). Son zamanlarda kriptoloji alanındaki gelişmeler bilgisayar endüstrisinin güvenli bilgi alış verişi, depolama ve işleme ihtiyaçlarını karşılamıştır. VoIP'in ve elektronik ticaretin yaygınlaşmaya başlamasıyla da kriptoloji alanına büyük çapta ticari bir ilgi oluşmuştur.

Sistemler arası bağlantılarda ya da herhangi iki nokta arasındaki haberleşmede verinin güvenli bir şekilde gittiğinden emin olmak gerekir. Bunun sağlanması ise gönderilen verinin şifrenmesi ile olur. Böylece açık haberleşme kanalları kullanılarak verinin güvenli bir şekilde ulaştırılması sağlanır. İletişimde açık bir haberleşme kanalı kullanılıyorsa gizli tutulmak istenen bilginin yetkisiz bir kişi tarafından dinlenebileceği veya haberleşme kanalına girip (araya girme) veriyi bozabileceği ya da değiştirebileceği düşüncesi her zaman için önemli bir problem oluşturur.

Verilerin güvenilir bir biçimde aktarımı ve elde edilmesi için kriptoloji bilimi aracılığıyla çeşitli şifreleme, anahtarlama ve çözümleme algoritmaları sunulmaktadır. Kriptoloji; bir mesajın okunamayacak şekle sokularak iki veya daha fazla nokta arasında, mesajın aktarıldığı ortamdan güvenli paylaşımını sağlamaktadır. Kısaca kriptoloji veriyi yalnızca okuması istenen şahısların okuyabileceği bir şekilde saklamak ve göndermek amacıyla kullanılan bir teknolojidir.

Örneğin, Şekil 5.1'de bir saldırganın hattı dinleyerek mesajı ele geçirmesi gösterilmiştir. Ancak saldırgan mesaja sahip olsa bile, mesaj şifreli olduğundan içeriği konusunda bilgi sahibi olamaz.



Şekil 5.1 Hattı dinleyen bir saldırganı karşı şifrelemenin kullanılması (Thalhammer, 2000)

Kriptolojide veri, matematiksel yöntemler kullanılarak kodlanır ve başkalarının okuyamayacağı hale getirilir. Bu matematiksel kodlamaya “*kripto algoritması*” adı verilir. İlk bilinen kripto algoritmaları 4000 yıl kadar önce ortaya çıkmıştır. Zaman geçtikçe, kullanılan teknikler ve cihazlar gelişmiş ve her geçen gün yeni teknikler kullanılır ve yeni algoritmalar üretilir olmuştur. Bu teknoloji şu anda bilişim güvenliğinin vazgeçilmez bir parçasıdır.

Kriptolojinin başlıca uygulama alanları şu şekildedir:

- Kablolu ve kablosuz ağlarda ses ve/veya veri aktarımının istenmeyen kişilerce izlenmesinin önlenmesi,
- Bilgisayar sistemlerinde bulunan verilere yetkisiz erişimlerin engellenmesi,
- İnternet üzerinden ses uygulamaları (VoIP),
- Güvenli bir şekilde e-ticaret işlemlerinin yapılabilmesi.

Kriptoloji esas olarak şifreleme ve şifre çözme (deşifreleme) 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 metne geçme işlemi “şifreleme”; şifreli metinden açık metne geçme işlemi ise “şifre çözme” olarak adlandırılır.

Şifreleme işleminin güvenli bir şekilde gerçekleştirilmesi şifreleme sırasında kullanılan tüm yöntem ve bilgilerin gizliliğine dayanır. Ancak herhangi bir nedenle kripto işlemlerinin açığa çıkabileceği düşünülerek iletişim güvenliği, “*şifreleme anahtarı*” adı verilen ek bilgi ile artırılmaktadır (Bir anahtar rasgele bit’lerden oluşan bir yazıdır. Bit sayısı kullanılan kripto

sistemine göre deđiřir). Bu durumda řifreleme iřlemi sırasında açık metin řifreleme anahtarı aracılığı ile řifrelenir. Deřifreleme ise mesajı orijinal řekline çevirme iřlemidir. Bu da bir deřifreleme anahtarı ile gerçekteřtirilir (řekil 5.2).



řekil 5.2 Temel kriptoloji mekanizması (Thalhammer, 2000)

Kriptolojiyi deđerlendirirken en önemli deđerkenlerden biri anahtar uzunluđu, veya anahtarın alabileceđi farklı deđerlerin sayısıdır. Anahtar uzunluđu arttıkça, olası anahtar sayısı arttıđından, saldırganın bu řifreyi çözmesi güçleřir, ama aynı zamanda da řifreleme ve řifre çözme hızı yavaşlar. Anahtarımız n farklı deđer alabiliyorsa, 0 ile $n-1$ arasında bir sayıyla eşdeđer olduđunu düşünmek iřimizi kolaylařtıracaktır. Örneđin anahtar olarak Türk alfabesini kullanırsak $n=28$ olacaktır. Anahtar uzunluđu ifade edilirken n sayısı doğrudan kullanılmaz, onun yerine o tamsayıyı bilgisayar belleğinde saklayabilmek için gerekli olan bit sayısı kullanılır. Bu o sayının 2 tabanındaki logaritmasına eşittir. Eklenen her bit, n sayısını iki ile çarpar. Örneđin, 16 bit'lik bir anahtar, $2^{16}=65536$ deđer alabilir.

Anahtarın deneme-yanılma yöntemiyle bulunmasını engellemek için, bugünkü süper bilgisayarlardan milyonlarca kat daha hızlı çalışan bir bilgisayarla bile milyarlarca yıl sürmesi için, yaklaşık 100 bit'lik bir anahtar uzunluđunun uygun olduđu düşünölmektedir. Çizelge 5.1'de farklı anahtar boyları için saniyede bir milyon, bir milyar ve bir trilyon řifre deneyebilen bilgisayarlar için kırma zamanları verilmiřtir (Singhai ve Sahoo, 2002).

Çizelge 5.1 Farklı hızdaki bilgisayarların farklı anahtar uzunluđundaki řifreleri çözme süreleri

Anahtar Uzunluđu (n)	2^n	10^6 řifre/s hızında bilgisayarın ortalama çözme süresi	10^9 řifre/s hızında bilgisayarın ortalama çözme süresi	10^{12} řifre/s hızında bilgisayarın ortalama çözme süresi
32 bit	$\sim 4 \times 10^9$	36 dk	2.16 sn	2.16 ms
40 bit	$\sim 10^{12}$	6 gün	9 dk	1 sn
56 bit	$\sim 7.2 \times 10^{16}$	1142 yıl	1 yıl 2 ay	10 saat
64 bit	1.8×10^{19}	292 000 yıl	292 yıl	3.5 ay
128 bit	1.7×10^{38}	5.4×10^{24} yıl	5.4×10^{21} yıl	5.4×10^{18} yıl

Kriptoloji başlıca 4 ana fonksiyonu sağlamaktadır. Bunlar:

- Gizlilik.
- Kimlik doğrulama.
- Veri bütünlüğü.
- İnkâr edememe.

Gizlilik (Confidentiality): Gizlilik, bilginin yetkisiz kişilerin eline geçmesinin engellenmesidir. Gizlilik, hem disk gibi kalıcı ortamlarda saklı bulunan veriler için hem de ağ üzerinde bir göndericiden bir alıcıya gönderilen veriler için söz konusudur. Saldırganlar, yetkileri olmayan verilere birçok yolla erişebilirler: Parola dosyalarının çalınması, sosyal mühendislik, bilgisayar başında çalışan bir kullanıcının ona fark ettirmeden özel bir bilgisini ele geçirme, vb. Bunun yanında trafik analizinin yani, hangi gönderici ile hangi alıcı arası haberleşmenin olduğunun belirlenmesine karşı alınan önlemler de gizlilik hizmeti çerçevesinde değerlendirilir.

Kimlik doğrulama (Authentication): Kimlik Doğrulama, bilginin doğru kaynaktan alındığını doğrulamak için kullanılır. Ağ güvenliği açısından kimlik sınaması; alıcının, göndericinin iddia ettiği kişi olduğundan emin olması anlamına gelmektedir. Bunun yanında, bir bilgisayar programını kullanırken bir parola girmek de kimlik sınaması çerçevesinde değerlendirilebilir. Günümüzde kimlik sınaması, sadece bilgisayar ağları ve sistemleri için değil, fiziksel sistemler için de çok önemli bir hizmet haline gelmiştir. Akıllı karta ya da biyometrik teknolojilere dayalı kimlik sınama sistemleri yaygın olarak kullanmaya başlanmıştır.

Veri bütünlüğü (Data integrity): Bilgi veya mesaj bütünlüğü bilginin ağdaki yolculuğu sırasında değişikliğe uğramadığından emin olmak için gereklidir. Bir diğer deyişle, bu hizmetin amacı, veriyi göndericiden çıktığı haliyle alıcısına ulaştırmaktır. Bu durumda veri, haberleşme sırasında izlediği yollarda değiştirilmemiş, araya yeni veriler eklenmemiş, belli bir kısmı ya da tamamı tekrar edilmemiş ve sırası değiştirilmemiş şekilde alıcısına ulaşır.

İnkâr edememe (Non-repudiation): İnkâr edememe, bir mesajı gönderen kişinin o mesajı size gönderdiğini inkâr edememesini sağlayan alındı onayını sağlar. Bu hizmet sayesinde, ne gönderici alıcıya bir mesajı gönderdiğini ne de alıcı göndericiden bir mesajı aldığını inkâr edebilir. Bu hizmet, özellikle gerçek zamanlı işlem gerektiren finansal sistemlerde kullanım alanı bulmaktadır ve gönderici ile alıcı arasında ortaya çıkabilecek anlaşmazlıkların en aza

indirilmesini sağlamaya yardımcı olmaktadır.

Kriptoloji bilimi üç farklı algoritma sistemi ortaya koymuştur:

- Simetrik şifreleme algoritmaları.
- Asimetrik şifreleme algoritmaları.
- Özetleme/Karıştırma (Digest/Hash) algoritmaları.

5.1.2 Simetrik Şifreleme Algoritmaları

Simetrik şifreleme algoritmaları şifreleme ve deşifreleme işlemleri için tek bir gizli anahtar (secret key) kullanmaktadır. Bu sebeple kullanılan anahtarın üçüncü kişilerden gizlenmesi gerekmektedir. Simetrik şifreleme aynı zamanda **Özel Anahtar Kriptoloji** olarak da bilinir. Simetrik şifrelemede şifreli metin alıcıya gönderilirken şifreli metinle birlikte gizli anahtarın da alıcıya güvenli bir şekilde gönderilmesi gerekmektedir. Şifrelenmiş mesaj sadece bu gizli anahtar kullanılarak açılabilir. Simetrik şifreleme algoritmaları çok hızlı şifreleme ve deşifreleme işlemleri gerçekleştirebildiğinden dolayı günümüzde çok yaygın olarak kullanılmaktadır. Bununla beraber, asimetrik algoritmalar nazaran saldırıya karşı daha az dirençlidirler.

Günümüzde yaygın olarak kullanılan başlıca simetrik şifreleme algoritmaları şu şekildedir:

- AES (Advanced Encryption System).
- DES (Data Encryption Standart).
- 3DES (Triple DES).
- IDEA (International Data Encryption Algorithm).
- RC4 (Rone's Code 4).
- RC5 ((Rone's Code 5).
- Blowfish.

Simetrik şifrelemenin blok ve akış şifreleme olarak bilinen iki çeşidi bulunmaktadır.

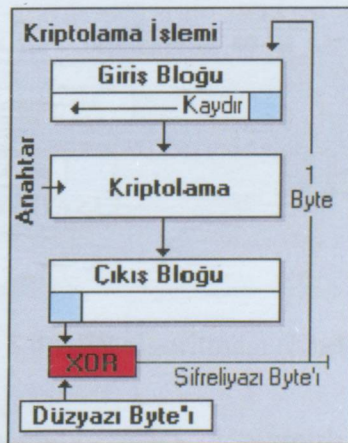
Akış Şifreleme: Bir akış şifreleme bilgiyi bit'lere veya bazı durumlarda byte'lara göre işler. Akış şifreleme farklı uzunluklardaki girişlerle çalışabilir. Yani, algoritma işlenmeden önce

belirli boyuttaki bir bilginin girilmesini beklemez. Akış şifreleme algoritmalarına; RC2 ve RC4 algoritmaları örnek olarak verilebilir.

Blok Şifreleme: Bir blok şifreleme bilgiyi bloklar halinde işler. Blok şifreleme şifrelenecek bir blok bilgiyi alır (genelde 64 bit) ve tek anahtarı ile seçilmiş fonksiyonu kullanarak onu aynı boyuttaki başka bir bloğa dönüştürür (Şekil 5.3). Blok şifreleme algoritmalarına; DES, AES, IDEA ve RC5 algoritmaları örnek olarak verilebilir. Bu algoritmalar aşağıdaki özellikleri gerçekleştirmeye çalışırlar.

- **Karıştırma:** Anahtar ve şifrelenmiş mesaj arasındaki ilişki olabildiğince karışık olmalıdır.
- **Dağıtma:** Tek bir açık mesaj karakterinin etkisi olabildiğince fazla şifrelenmiş karaktere yansıtılmalıdır.
- **Sıra değiştirme:** Şifrelemeye başlamadan önce açık mesajın içeriği değişik bir sıraya konur.
- **Yer değiştirme:** Tekrar eden kalıplar başka kalıplarla değiştirilir.

Blok şifreleme algoritmalarının gücü söz konusu olduğunda algoritmada kullanılan döngü sayısı, anahtarların XOR işlemine sokulması, blok uzunluğu, anahtarın uzunluğu ve özelliği büyük önem taşımaktadır. Ayrıca kullanılacak anahtarın rastlantısal olması da gerekir yani, bilgiyi şifrelemek için kullanılan şifreleme anahtarı rasgele üretilir.



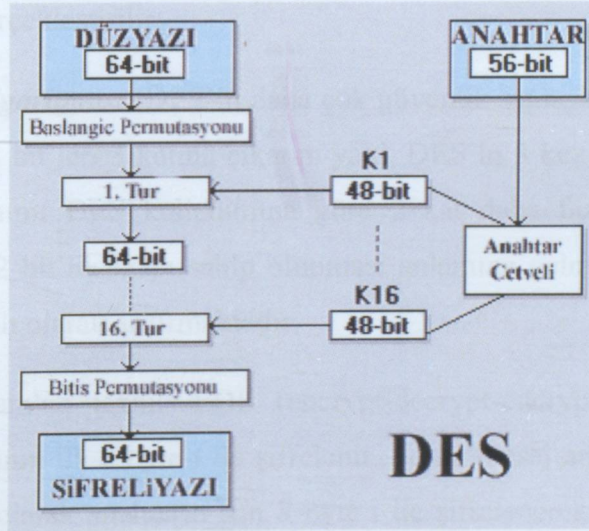
Şekil 5.3 Blok şifreleme (Kurt, 2001)

Blok şifreleme algoritmalarında anahtarın uzunluğu ya da bit sayısı en temel saldırı olan geniş anahtar arama saldırısına karşı güçlü olmalıdır. Örneğin DES algoritması 56-bit anahtar kullanırken; AES algoritması DES'in bu zaafını örter niteliktedir ve 128, 192, 256 bit anahtar seçenekleri mevcuttur. Ayrıca anahtarın rastlantısal olması gerekmektedir.

Blok şifreleme algoritmalarında döngü sayısı da iyi seçilmek zorundadır. Çünkü lineer transformasyon ve yer değiştirmelerin, bu seçilen değerle algoritmaya yeterli gücü vermesi gerekmektedir. Ayrıca yapılan saldırıların başarısız olması için en önemli şartlardan biridir.

Bilgi Şifreleme Standardı (DES-Data Encryption Standard): DES algoritması en yaygın olarak kullanılan blok 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.

Düzyazı, bazı permütasyon ve yedekleme işlemlerine tabi tutulur. Sonrasında, güvenli bir şifreli yazı bloğu yaratmak için çıktılar XOR işlemi kullanılarak orijinal düzyazı ile birleştirilir. Bu şifreleme serisi 16 kere tekrarlanır. Her seferinde farklı anahtar bit grupları kullanılır (Şekil 5.4).



Şekil 5.4 DES algoritması (Kurt, 2001)

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 kalmakta ve hatta 3 ila 7 saat arası gibi kısa bir zaman süresinde kırılabilir. DES'in zayıflıkları nedeniyle daha güçlü ve etkili

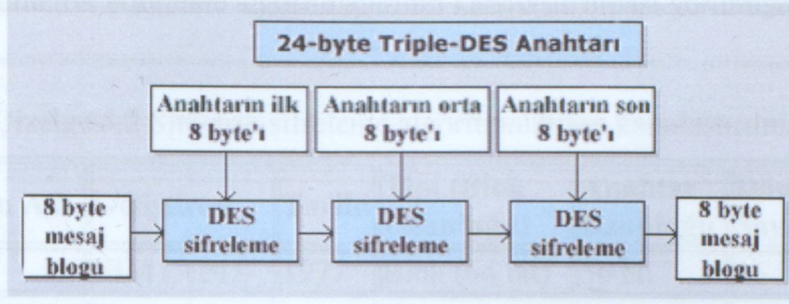
şifreleme metotları geliştirilmiştir.

Gelişmiş Şifreleme Sistemi (AES-Advanced Encryption System): AES, simetrik algoritmalar içerisinde en güçlü algoritmalarından biridir. DES algoritması 1990'lı yıllara kadar kendini başarı ile savundu. Ancak onun en büyük zaafı 56 bit anahtara sahip olması ve anahtarın bir şekilde daha büyük uzunlukta kullanılabilecek bir yönteminin olmamasıydı. Daha sonraları paralel işlemcili bilgisayarların kullanılması ve geniş anahtar arama saldırıları nedeniyle kısa bir zaman dilimi içinde kırılması mümkün hale gelmişti. Ayrıca güçlü şifre çözme saldırılarına karşı da yetersiz kalmaya başlamıştı.

Heys, 1994 yılındaki çalışmasında bir SPN algoritması kullanarak diferansiyel ve lineer kriptanalize karşı güçlü DES algoritmasına eşit güçte bir algoritmayı 8 döngüde sağladı. AES algoritması 128 bit veri bloklarını 128, 192, 256 bit anahtar seçenekleri ile şifreleyen bir algoritmadır. SPN algoritmasının geniş bir çeşididir. 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. AES algoritmasında her döngü dört katmandan oluşur. İlk olarak 128 bit'lik veri 4×4 byte matrisine dönüştürülür. Daha sonra her döngüde sırasıyla byte'ların yer değiştirmesi, satırları öteleme, sütunları karıştırma ve XOR'lama işlemleri gerçekleştirilir.

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. 3DES kullanımı DES kullanımına göre 2 kat daha fazla güvenlik sağladığına inanılmaktadır. Bu, 112 bit'lik koda sahip olunması anlamına gelmektedir. Ayrıca kodlama süresini de doğru orantılı olarak arttırmaktadır.

3DES tarafından kullanılan teknik EDE (encrypt-decrypt-encrypt) olarak bilinmektedir. Düzyazı 3DES anahtarının ilk 8 byte'ı ile şifrelenir. Sonra mesaj anahtarın ortadaki 8 byte'ı ile deşifrelenir ve son olarak anahtarın son 8 byte'ı ile şifrelenerek 8 byte'lık bir blok elde edilir (Şekil 5.5). Eğer kullanılan her anahtar aynı ise yapılan işlem DES'in kullanımıyla eşdeğerdir. Eğer her anahtar birbirinden farklı ise anahtarın ortasındaki 8 byte ile deşifreleme işlemi mesajı iyice karmaşık hale getirir.



Şekil 5.5 3DES algoritması (Kurt, 2001)

Uluslararası Bilgi Kriptolama Algoritması (IDEA –International Data Encryption Algorithm): 64-bit bloklar üzerinde 128-bit anahtar kullanan bir simetrik şifreleme metodudur. IDEA patentli bir algoritmadır.

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. Giriş ve çıkış blokları 8 byte uzunluğundadır. RC2'nin düzgün çalışması için, giriş düzyazısı 8 byte'ın bir kaç katı olmalıdır. RC2 için giriş anahtarı 1 ile 1024 bit arası bir uzunlukta olabilir. Giriş anahtarı algoritma tarafından şifreleme işlemlerinde kullanılacak bir anahtar yaratmak için kullanılır. Şifreleme anahtarı bir bit'den 1024 bit'e kadar değerler alabilir. RC2'nin Amerika dışına ihracatı 40 ile 48 bit arası anahtar sınırlaması ile mümkündür.

RC4 (Rone's Code 4) Algoritması: RC4, 1987'de RSA Laboratories tarafından geliştirilen bir simetrik akış şifreleme metodudur. Pseudo-random numara sırasına dayalıdır. RC4'den elde edilen çıkış, bilgi akışı ile XOR'lanır. Bu sebeple hiçbir RC4 anahtarı iki farklı bilgi akışını şifrelemek için kullanılmamalıdır. RC4 1 ile 2048 bit arası uzunluklarda anahtarları destekler. Fakat Amerika dışına satılan yazılımlarda 40 bit sınırlaması uygulanır. 40 bit altındaki anahtarların RC4 ile kullanılması tavsiye edilmez. DES ile karşılaştırıldığında RC4 beş kat daha hızlıdır. Fakat geçmişte RC4 kırma girişimleri başarı ile sonuçlandı. RC4'ü çalıştırmada kullanılan kod DES algoritmasının onda biri kadardır.

Blowfish Algoritması: AES'e benzer şekilde hızlı çalışmak üzere tasarlanmış bir algoritmadır. 32 bit mikro işlemciler ile 1 byte data 18 işlemci döngüsünde şifrelenir. 5 KB'tan daha az bir hafızaya ihtiyaç duyar. Uygulaması son derece kolaydır ve farklı uzunlukta kripto anahtarları seçilerek farklı güvenlik seviyeleri elde edilebilir.

Çizelge 5.2’de simetrik şifreleme algoritmalarının karşılaştırılması verilmiştir.

Çizelge 5.2 Simetrik şifreleme algoritmalarının karşılaştırılması

Algoritmanın Adı	Geliştiren	Tarihi	Tipi (Blok Uzunluğu)	Anahtar Uzunluğu	Döngü Sayısı	Kullanım Koşulları
DES	IBM (ABD)	1977	Blok (64 bit)	56 bit	16	Serbest
IDEA	Lai-Massey, ETH Zurich (İsviçre)	1992	Blok (64 bit)	128 bit	8	Serbest
RC2	Rivest, RSA Data Security (ABD)	1992	Akış Şifreleme	1024 bit’e kadar	-	Algoritma RSA tarafından saklı tutuluyor
RC5	Rivest, RSA Data Security (ABD)	1995	Blok (32, 64 veya 128 bit)	2048 bit’e kadar	255'e kadar	Serbest
AES	Heys	1994	Blok (128 bit)	128, 192 ya da 256 bit	8, 12, 14	Serbest

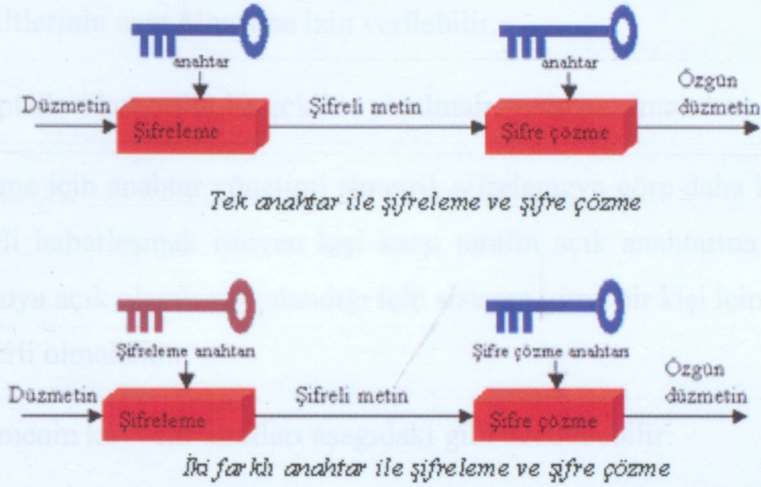
5.1.3 Asimetrik Şifreleme Algoritmaları

Simetrik şifreleme tekniğindeki anahtar dağıtım problemini çözmek için şifreleme ve şifre çözme işlemlerinin her birisi için ayrı ayrı anahtar kullanma prensibine dayanan bir şifreleme sistemi geliştirilmiştir. Bu sisteme Asimetrik Şifreleme ya da **Açık Anahtar Kriptoloji Sistemi (PKE-Public-Key Encryption)** adı verilmektedir. Şifreleme ve şifre çözme işlemleri birbirinin simetriği olmayan algoritmalarla gerçekleştirildiğinden dolayı bu sistem asimetrik şifreleme sistemi olarak bilinir.

Simetrik şifreleme algoritmaları şifreleme ve şifre çözme işlemlerini tek bir gizli anahtarla gerçekleştirmektedir. Alıcıya şifreli metinle birlikte bu gizli anahtarın da güvenli bir kanaldan iletilmesi gerekmektedir. Bu durum simetrik şifreleme algoritmalarının en büyük dezavantajıdır. Simetrik şifreleme algoritmalarının bu problemini ortadan kaldırılması için asimetrik şifreleme algoritmaları ortaya atılmıştır.

Asimetrik şifreleme sisteminde şifreleme ve şifre çözme işlemleri için bir çift anahtar kullanılır. Bir anahtar (**açık anahtar-public key**) mesajı şifrelemek için kullanılır ve diğer anahtar (**özel anahtar-private key**) şifre çözmek için kullanılır (Şekil 5.6). Her iki terminalde

de (gönderici ve alıcı) bu anahtar çifti bulunmaktadır ve her bir terminal diğerinin sadece ve sadece açık anahtarından haberdardır. Bir terminal diğerinin özel anahtarı hakkında hiçbir fikre sahip değildir. Kullanılacak bu iki anahtar birlikte üretilirler. Bu anahtarlardan herhangi birine sahip olan bir saldırganın diğer anahtarı üretmesi matematiksel olarak imkansız denebilecek derecede zordur.



Şekil 5.6 Simetrik ve asimetrik şifreleme algoritmalarında anahtar yapısı

Anahtar çiftlerini üreten algoritmaların matematiksel özelliklerinden dolayı açık-özel anahtar çiftleri her kişi için farklıdır, diğer bir deyişle her kullanıcının açık-özel anahtar çifti yalnızca o kullanıcıya özeldir. Ayrıca şifre çözüm anahtarı şifre anahtarından hesaplanamaz. Bu algoritmalara açık anahtarlı algoritmalar denmesinin sebebi şifre anahtarı halka (kamuya/genel kullanıma) açılabiliridir. Yani, bir yabancı bir iletiyi şifrelemek için şifreleme anahtarını kullanabilir, ancak sadece ilgili şifre çözüm anahtarına sahip bir kişi iletinin şifresini çözebilir. Bu sistemde, şifre anahtarına genellikle açık anahtar denir, şifre çözüm anahtarı da genellikle özel anahtar olarak adlandırılır.

Bir şahsın açık anahtarı bu şahsa mesaj göndermek isteyen herhangi biri tarafından kullanılabilir. Gönderici mesajı, alıcının açık anahtarı ile şifreler. Alıcı, gelen mesajı kendi özel anahtarı ile açar. Bir kullanıcının açık anahtarıyla kilitlenen bir mesajı ancak ona ait özel anahtar çözebilir. Açık anahtar kamuya açıktır, elektronik kimlik belgelerinin içinde diğer kişisel bilgilerle birlikte tutulur ve herkes birbirinin açık anahtarını e-kimliklerine ulaşmak suretiyle istediği zaman elde edebilir.

Asimetrik şifreleme için anahtar yönetimi çok önemlidir. Anahtar yönetimi için dikkat

edilmesi gereken noktalar şöyle sıralanabilir:

- Açık anahtarlar kontrollü olarak bir otorite tarafından yayınlanmalıdır.
- Anahtar çiftleri merkezi bir otorite tarafından üretilebilir veya her kullanıcı kendi anahtar çiftini üretebilir.
- Şifreleme için ayrı ayrı anahtar çiftleri olmalıdır. Çok özel durumlar için şifreleme anahtar çiftlerinin aynı olmasına izin verilebilir.
- Anahtar iptalleri kontrollü bir şekilde yapılmalı ve duyurulmalıdır.

Asimetrik şifreleme için anahtar yönetimi simetrik şifrelemeye göre daha kolaydır çünkü, bir kullanıcıyla şifreli haberleşmek isteyen kişi karşı tarafın açık anahtarına ihtiyaç duyar. Bu açık anahtar kamuya açık olarak yayınlandığı için sisteme giren bir kişi için sadece bir anahtar çifti üretmek yeterli olmaktadır.

Asimetrik şifrelemenin kuvvetli tarafları aşağıdaki gibi özetlenebilir:

- Anahtar yönetimi ölçeklenebilir.
- Kripto-analize karşı dirençlidir (Kırılması zordur).
- Bütünlük, kimlik doğrulama ve inkâr edememe güvenlik hizmetleri sağlanabilir.

Asimetrik şifrelemenin zayıf yönleri ise aşağıdaki gibidir:

- Algoritmalar genel olarak yavaş çalışırlar. Simetrik şifreleme algoritmalarına göre yaklaşık 1500 kat daha yavaşırlar.
- Anahtar uzunluğu bazı durumlar için kullanışlı değildir. Mobil cihazlar için klasik algoritma anahtar uzunlukları sorunlu olabilir.

Sonuç olarak açık anahtar şifreleme yönteminde şifreleme mantığı kısaca şu şekilde olmaktadır:

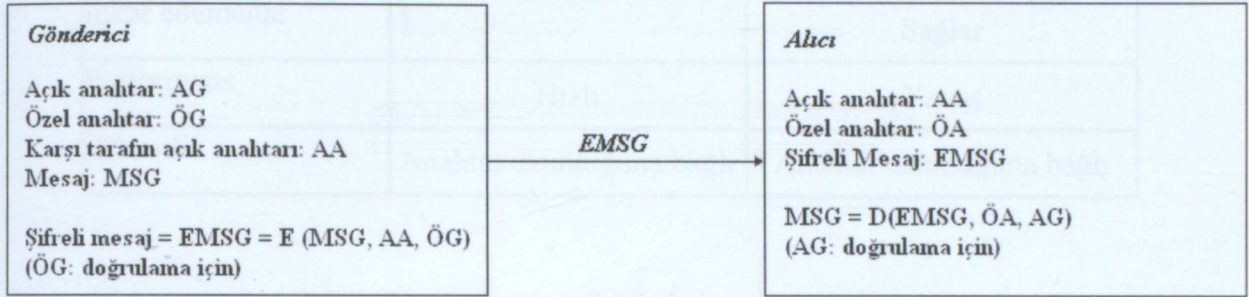
Gönderici taraf:

1. Gönderilecek olan mesajı alıcının açık anahtarı ile şifreler. Bu şifre ancak ve ancak alıcının özel anahtarı ile çözülebilmektedir.
2. Doğrulama için mesajın son halini kendi özel anahtarı ile ilişkilendirir ve alıcıya gönderir. Alıcı taraf mesajın doğruluğunu anlamak için göndericinin açık anahtarını

kullanır (Şekil 5.7).

Alıcı tarafta:

1. Gelen mesaj ilk önce göndericinin açık anahtarı ile doğrulanır.
2. Sonrasında alıcı kendi özel anahtarı ile şifreli mesajı çözer.



Şekil 5.7 Açık anahtar mekanizması (Kultti, 2005)

Şekil 5.7’de E fonksiyonu şifrelemeyi ifade ederken D fonksiyonu şifre çözmeyi ifade etmektedir.

Asimetrik algoritmalar, simetrik algoritmalarla göre daha güvenli ve kırılması zor algoritmalarlardır. Her ne kadar bu yöntemin, anahtarların alıcı tarafa iletilmesi işlemini basitleştirdiği düşünülse de asimetrik algoritmaların işlem süresinin yüksek oluşu, veri şifrelemede yaygın olarak kullanılmalarını engellemektedir. Bununla birlikte performansları simetrik algoritmalarla göre oldukça düşüktür.

Mesaj gönderebileceğimiz kullanıcıların sayısı arttıkça, elde etmemiz gereken açık anahtar sayısı da artacaktır. Sistemde 100 kullanıcı varsa, her bir kullanıcının ayrı bir açık anahtarı olacağından, tüm bu açık anahtarlar, erişilebilir olmalıdır. Bu problem de sayısal sertifikalar teknolojisi yardımı ile çözülebilmektedir (İleriki bölümlerde ayrıntılı olarak değinilecektir).

Asimetrik ve simetrik şifreleme sistemlerinin özellikleri Çizelge 5.3’de karşılaştırılmaktadır.

Çizelge 5.3 Simetrik ve asimetrik şifreleme algoritmalarının karşılaştırılması

Konu	Simetrik Şifreleme	Asimetrik Şifreleme
Gizlilik	Sağlar	Sağlar
Bütünlük	--	Sağlar
Kimlik doğrulama	--	Sağlar
İnkar edememe	--	Sağlar
Performans	Hızlı	Yavaş
Güvenlik	Anahtar uzunluğuna bağlı	Anahtar uzunluğuna bağlı

Günümüzde yaygın olarak kullanılan başlıca iki tip asimetrik şifreleme algoritması vardır:

- Diffie-Hellman.
- RSA (Rivest Shamir Adleman).

5.1.3.1 Diffie-Hellman Anahtar Anlaşma/Takas Metodu

İlk asimetrik şifreleme sistemi 1976 yılında Stanford üniversitesindeki iki araştırmacı tarafından bulundu. Whitfield Diffie ve Martin Hellman herkese açık bir haberleşme kanalında paylaşılan özel anahtarı geliştirme ve takas etmek için bir sistem buldular. Bu sisteme Diffie-Hellman anahtar takas sistemi adı verilmektedir.

Diffie-Hellman anahtar takas sistemi şifreleme ve şifre çözme için kullanılan bir metot değildir. Taraflar arasında şifreleme anahtarlarının takas edilebilmesini sağlayan bir sistemdir. Diffie-Hellman takas sistemiyle her iki taraf bazı genel nümerik değerler konusunda anlaşarak bir anahtar oluşturur. Sonrasında da anahtarların matematiksel dönüşümlerini takas ederek *oturum anahtarı* adı verilen üçüncü bir anahtarı hesaplarlar. Bu oturum anahtarı her iki takas edilmiş değeri de bilen bir saldırgan tarafından dahi kolayca bulunamaz. Çünkü bir oturum anahtarı sadece belirli bir bağlantı oturumu için kullanılır ve sonrasında atılır.

Diffie-Hellman anahtar takası mükemmel iletme gizliliği sağlayan tek metottur. Yani bir açığa çıkmış anahtar bu metotta ileriki anahtar takaslarını kesinlikle tehlikeye atmamaktadır. Çünkü Diffie-Hellman metodu gizliliği sağlarken var olan bir anahtara dayanmamaktadır. Aksine bu metot ayırık logaritma adı verilen bir matematiksel yapıya dayanmaktadır. Bu

logaritma sayesinde her bir oturum için ayrı bir anahtar oluşturulur. Bu nedenle de diğer metotlarda olduğu gibi önceden belirlenmiş bir anahtara ihtiyaç yoktur. Sadece bire bir bağlantılarda (peer-to-peer) kullanılabilir olması bu metodun tek dezavantajıdır. Şimdi bu metodun çalışma mantığına değinelim.

İlk önce katılımcılar Diffie-Hellman parametreleri konusunda mutabakata varmalıdır. 2'den büyük bir asal sayı olan p ve p 'den küçük bir tam sayı olan g Diffie-Hellman parametrelerini oluşturmaktadır. g genellikle üretici (generator) olarak adlandırılır.

Her iki katılımcı da rasgele gizli bir özel numara (x -secret private number) üretir. Bu numara $p-1$ değerinden küçük olmak zorundadır. Gönderici kendi ürettiği numarasını (x_i) kullanarak bir açık anahtar (y_i -public key) oluşturur ve alıcıya iletir.

$$y_i = g^{x_i} \bmod p \quad (5.1)$$

Alıcı da aynı şekilde kendi özel numarası (x_r) ile bir açık anahtar (y_r) oluşturur ve bu anahtar ile cevap verir.

$$y_r = g^{x_r} \bmod p \quad (5.2)$$

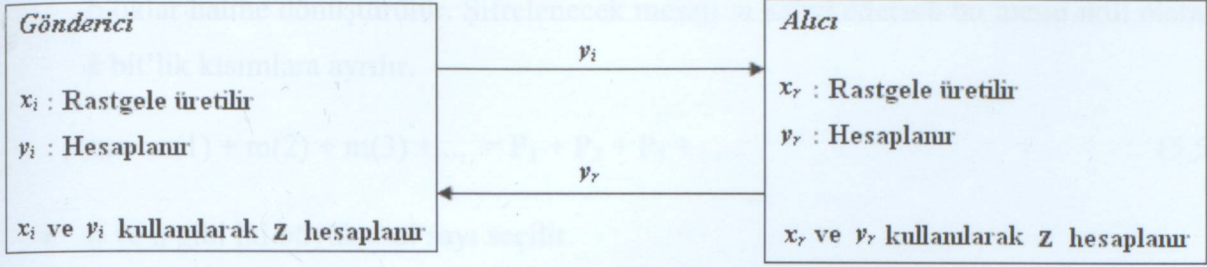
Her iki katılımcının özel anahtarları kullanılarak z adı verilen ortak bir gizli oturum anahtarı (common secret key) elde edilir. Bu gizli oturum anahtarı katılımcılar dışındaki kişilerin çözmesi imkansızdır.

$$z = g^{(x_i \cdot x_r)} \bmod p \quad (5.3)$$

Bir saldırgan en fazla açık anahtarlara erişebilirken z gizli oturum anahtarına kesinlikle erişemez. Bunun sebeplerinden biri bu oturum anahtarı sadece tek bir oturum için geçerlidir. Yani her bir oturum için ayrı bir oturum anahtarı üretilmektedir. Diğer sebep ise y açık anahtarlarına ulaşan bir saldırganın bu anahtarları kullanarak x özel numaralarını ya da z oturum anahtarını türetmesi imkansızdır.

Her bir katılımcı diğer katılımcının gönderdiği açık anahtar (y) ile birlikte kendi özel numarasını (x) kullanarak gizli oturum anahtarını (z) hesaplar (Şekil 5.8).

$$z = g^{(x_i \cdot x_r)} \bmod p = y_i^{x_r} \bmod p = y_r^{x_i} \bmod p \quad (5.4)$$



Şekil 5.8 Diffie-Hellman anahtar anlaşma/takas metodu (Kultti, 2005)

Diffie-Hellman anahtar takas yöntemi ortadaki adam saldırılarına karşı savunmasız kalabilmektedir. Bu saldırıda saldırgan gönderici ile alıcının arasına girerek göndericinin mesajlarını ele geçirir ve sanki alıcıymış gibi davranarak gönderici ile mesajlaşır. Sonrasında saldırgan sanki kendisi gerçek göndericiymiş gibi gerçek alıcı ile başka bir Diffie-Hellman anahtar takasını başlatır. Sonuç olarak saldırgan gönderici ve alıcı ile iki farklı anahtar oturumu kurar ve gerçek katılımcılar arasındaki sonraki tüm mesajların şifrelerini çözebilir, değiştirebilir ya da yeniden şifreleyebilir duruma gelir. Her ne kadar bu senaryonun gerçekleşmesi pratikte zor görünse de bu durumun ciddi bir güvenlik açığı oluşturduğu göz ardı edilemez.

5.1.3.2 RSA (Rivest Shamir Adleman) Şifreleme Algoritması

RSA algoritması 1977 yılında R.Rivest, A.Shamir ve L.Adleman tarafından bulunmuş ve daha sonra açık anahtar şifreleme mantığına uygun biçimde geliştirilmiştir (Porter vd., 2006). Bu algoritma, açık anahtar şifreleme ve dijital imza sistem işlemlerinde güvenli bir şekilde kullanılmaktadır.

Görünüşte son derece basit matematiksel ilişkilerle çalışan bu yöntemde iki ayrı anahtar bulunmaktadır. 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. Ancak mesajı sadece gizli anahtar kimde ise o çözebilir. Gizli anahtar da sadece sahibinde bulunur.

Bir genel anahtarlı şifreleme tekniği olan RSA, çok büyük tamsayıları oluşturma ve bu sayıları işleminin zorluğu üzerine düşünülmüştür. Anahtar oluşturma işlemi için asal sayılar kullanılarak daha güvenli bir yapı oluşturulmuştur. Anahtar oluşturma algoritması şu şekildedir (Şekil 5.9):

- RSA şifreleme algoritmasında şifrelenecek olan açık metin öncelikle pozitif tamsayı

bloklar haline dönüştürülür. Şifrelenecek mesajı m kabul edersek bu mesaj ikili olarak k bit'lik kısımlara ayrılır.

$$m = m(1) + m(2) + m(3) + \dots = P_1 + P_2 + P_3 + \dots \quad (5.5)$$

- p ve q gibi iki büyük asal sayı seçilir.
- Bu iki asal sayının çarpımı n ve bir eksiklerinin çarpımı Z hesaplanır.

$$n = p \times q \quad (5.6)$$

$$Z = (p-1) \times (q-1) \quad (5.7)$$

- 1'den büyük Z 'den küçük ve Z ile aralarında asal bir E tamsayısı seçilir.
- Seçilen E tamsayısının $(\text{mod } Z)$ 'de tersi alınır, sonuç D gibi bir tamsayıdır.

$$D = E^{-1}(\text{mod } Z) \quad (5.8)$$

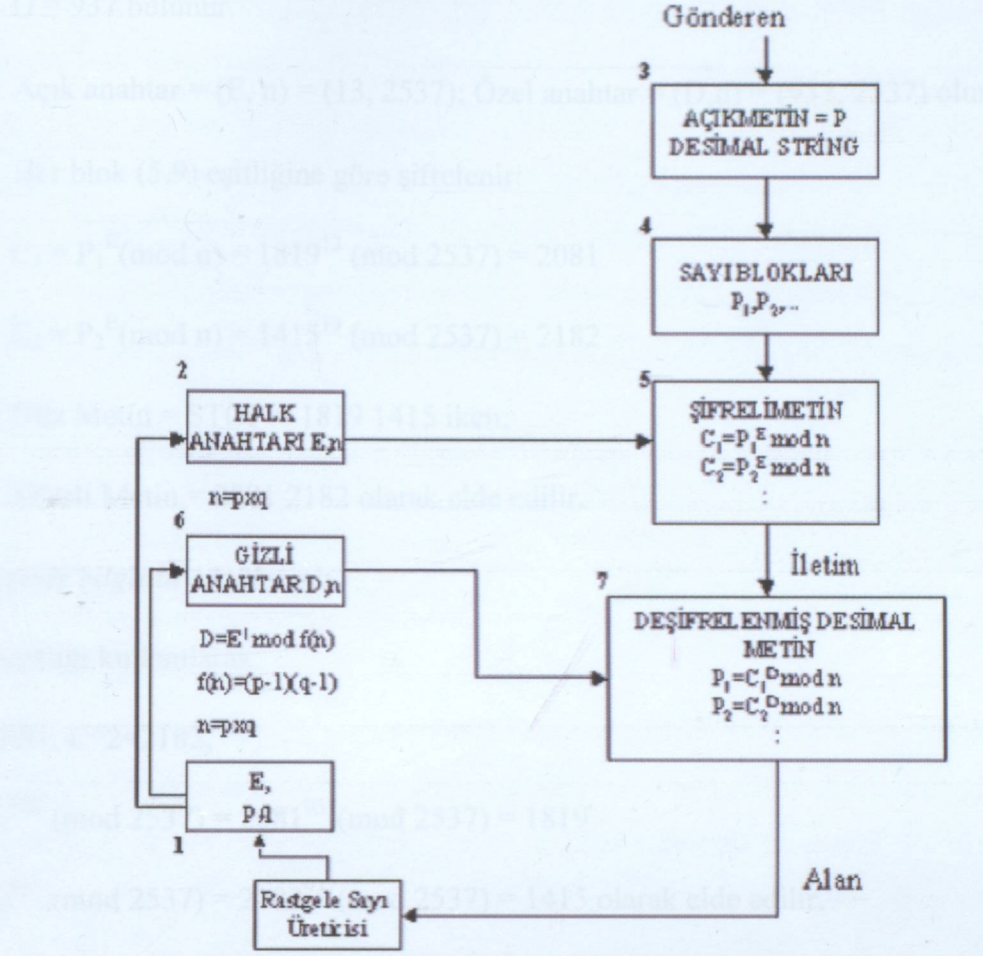
- E ve n tamsayıları açık anahtarı, D ve n tamsayıları ise özel anahtarı oluşturur. Yani açık anahtar (E, n) çifti iken özel anahtar (D, n) çiftidir.
- Daha sonra şifreleme için her bir kısma (5.9) eşitliği uygulanır. Böylece şifreleme işlemi tamamlanır. Girişte kullandığımız m açık metnini şifrelenmiş olarak C şeklinde elde ederiz.

$$C_i = m_i^E (\text{mod } n) \quad (5.9)$$

Özel anahtar olan D sayısının (E, n) sayılarından elde edilmesi zor bir işlemdir. Eğer bir kişi n sayısını çarpanlarına ayırarak p ve q sayılarını elde edebilirse özel anahtarı da kolaylıkla bulabilir. Bu sebeple RSA sisteminin güvenliği çarpanlarına ayırma probleminin zorluğu temeline dayanır. Çarpanlarına ayırma işleminin kolay bir yönteminin bulunması, RSA algoritmasının kırılması anlamına gelir.

Deşifreleme: Belirlediğimiz D gizli anahtarı ile elimizde bulunan şifrelenmiş C metnini çözmemiz gerekiyor. Özel anahtar (D, n) kullanılarak şifre çözümü (5.10) eşitliğinde verilmektedir.

$$m_i = C_i^D (\text{mod } N) \quad (5.10)$$



Şekil 5.9 RSA asimetrik şifreleme algoritması (Porter vd., 2006)

RSA Algoritmasına Sayısal Bir Örnek:

$p = 43$, $q = 59$ ve $E = 13$ için RSA şifreleme sistemi kullanılarak **STOP** sözcüğünün şifrlenmesi:

Harfleri rakama çevirmek için her bir rakamın bir harfi temsil ettiğini düşünelim ($A = 01$, $B = 03$, $C = 04$, $D = 05$ $O = 14$, $P = 15$, ... $S = 18$, $T = 19$). Bu durumda STOP sözcüğünü ikili bloklar halinde organize edersek: ST OP= 1819 1415 elde edilir. Buradan: $P_1 = 1819$; $P_2 = 1415$ olur.

- (5.6) eşitliğinden: $n = pxq = 43 \times 59 = 2537$ bulunur.
- (5.7) eşitliğinden: $Z = (p-1) \times (q-1) = 42 \times 58 = 2436$ bulunur.
- $E = 13$ olarak verilmiş.
- (5.8) eşitliğinden: $D = E^{-1} \pmod{Z} \Rightarrow D \times E = 1 \pmod{Z} \Rightarrow D \times 13 = 1 \pmod{2436} \Rightarrow$

$D = 937$ bulunur.

- Açık anahtar = $(E, n) = (13, 2537)$; Özel anahtar = $(D, n) = (937, 2537)$ olur.
- Her blok (5.9) eşitliğine göre şifrelenir:

$$C_1 = P_1^E \pmod{n} = 1819^{13} \pmod{2537} = 2081$$

$$C_2 = P_2^E \pmod{n} = 1415^{13} \pmod{2537} = 2182$$

Düz Metin = STOP = 1819 1415 iken;

Şifreli Metin = 2081 2182 olarak elde edilir.

Şifrelenmiş bilginin çözülmesi:

(5.10) eşitliği kullanılarak:

$$C^1=2081, C^2=2182,$$

$$P_1 = C_1^{937} \pmod{2537} = 2081^{937} \pmod{2537} = 1819$$

$$P_2 = C_2^{937} \pmod{2537} = 2182^{937} \pmod{2537} = 1415 \text{ olarak elde edilir.}$$

RSA Sisteminin Güvenirliği: RSA sisteminin kırılması birkaç değişik şekilde yorumlanabilir. Sisteme en çok zarar verecek saldırı, bir saldırganın belli bir açık anahtara karşı gelen gizli anahtarı bulmasıdır. Bunu başarabilen bir saldırgan şifrelenen bütün mesajları okuyabilir. Bunu yapmanın en akla gelen yolu n 'nin asal çarpanlara ayrılması yani, p ve q 'nın hesaplanmasıdır. p , q ve E kullanılarak D kolaylıkla hesaplanabilir. Ancak buradaki zorluk n modülünün çarpanlarına ayrılmasıdır. RSA sisteminin güvenliği çok büyük sayıların asal çarpanlarına ayrılmasının zorluğu varsayımına dayanır. Büyük sayıların çarpanlarına ayrılmasının zorluğu ispatlanmış değildir. Son üç yüz yıl içerisinde Fermat ve Legendre gibi ünlü matematikçiler bu konuda çalışmalar yapmışlardır.

5.1.4 Özetleme/Karma Algoritmaları (Digest/Hash Algorithms)

Özetleme algoritmaları, girdi olarak kullanılan herhangi bir uzunluktaki veriyi işleyerek sabit uzunlukta bir özet değeri üreten tek yönlü algoritmalar (Luthra ve Ashraf, 2005). Bu fonksiyonlar tek yönlü oldukları için veri bütünlüğü ve kimlik doğrulaması ile ilgili uygulamalarda temel yapıtaşı haline gelmiştir.

Bir özetleme fonksiyonu, herhangi bir uzunluktaki metni giriş değeri olarak alır ve sonuç

olarak sabit uzunluklu bir deęer üretir. Bu deęere mesaj özetı (message digest) adı verilir. Burada üretilen özet, fonksiyona giren metnin karakterini taşımaktadır denilebilir. Giriş metninde yapılacak tek bir karakter deęiřiklięi bile üretilcek özetle büyük deęiřikliklere yol açar. Ayrıca, özetleme fonksiyonu tek yönlü olduęundan, özetten asıl metne geri dönüş yoktur. Özetleme fonksiyonları, uzun metinlerin asimetrik bir algoritma ile řifrelenmeleri sırasında asimetrik algoritmanın bařarım dezavantajını ortadan kaldırmak amacıyla kullanılırlar. Tüm mesaj metni yerine yalnızca mesajın özetı alınarak asimetrik algoritmayla řifreleme yapılır.

Özetleme algoritmalarının en önemli özellikleri, birbirinden çok az farklı girdiler için dahi tamamen ayrı çıktıları üreterek çakışmaları önleyebilmeleridir. Özet deęerinden girdi verilerine ulaşmak neredeyse imkansızdır. Özet deęerleri, veri bütünlüęünün bozulup bozulmadıęının kontrolü için kullanılmaktadır.

Bilindięi üzere asimetrik řifrelemede, her kullanıcının bir açık anahtarı bir de gizli anahtarı bulunmaktadır. Açık anahtardan gizli anahtara ulaşmanın hesapsal karmaşıklığı pratik bir atak düzenlenemeyecek derecede yüksektir. Dięer taraftan asimetrik sistemler simetrik sistemlere göre son derece yavařtır. Bu nedenle asimetrik sistemler ile bir veriyi řifrelemeden önce, simetrik bir yapı ile řifrelenecek verinin boyutu küçültülerek özetı elde edilir. Şifreleme de verinin bu özetine yapılır.

Günümüzde kullanılmakta olan asimetrik řifreleme metodlarının temel olarak iki kısımdan oluřtuęunu düşünebiliriz. Bu kısımlardan ilki řifrelenecek verinin boyunu küçülterek özetini çıkaran “özet fonksiyonu”, ikincisi ise oluřturulan özetı řifreleyen “asimetrik řifreleme algoritması”dır.

Özet fonksiyonları genellikle simetrik algoritma tabanlı ve hızlı algoritmalarlardır. Ayrıca özetin uzunluęu verinin uzunluęundan bağımsız ve sabittir. Özet uzunluęu mesajın uzunluęu ne olursa olsun oldukça kısadır (160 bit, 256 bit veya 512 bit gibi). Dolayısıyla özet kullanımı řifrelemenin pratik olarak gerçeklenebilmesini saęlamaktadır.

En bilinen özetleme algoritmaları olarak Güvenli Özet Algoritması-1 (SHA-1-Secure Hash Algorithm-1), RACE Bütünlük Asli Deęerlendirme Mesaj Özetı-160 (RIPEMD_160 -RACE Integrity Primitives Evaluation_160) ve Mesaj Özetı 5 (MD5 -Message Digest 5) sayılabilir. Ayrıca, MD2, MD4 ve HMAC algoritmaları da örnek olarak verilebilmektedir.

Özetleme Algoritmalarının Özellikleri: Bir özet fonksiyonu (H), verinin sayısal karşılığını (M) kullanarak sabit uzunluğa sahip mesajın özetini ($h=H(M)$) oluşturur. İlk olarak uzun mesajı, $m_1, m_2, \dots, m_s$ olmak üzere eşit uzunlukta bloklara ayrılır. Gerekli durumlarda son blok belirli bir fonksiyon kullanarak blok uzunluğuna tamamlanır. H_0 başlangıç vektörü ve f sıkıştırma fonksiyonu olmak üzere, $H_i=f(H_{i-1}, M_i)$ değerleri hesaplanır. Sıkıştırma fonksiyonunun son kez kullanıldığında elde edilen çıktı, mesajın özeti olarak kullanılır. H fonksiyonunun iç yapısı açıktır ve gizli anahtar içermez, dolayısıyla şifreleme yapmak için kullanılmazlar.

Özetleme fonksiyonun güvenliliğini sağlayan bazı özellikler vardır. Bunlardan birincisi özetleme fonksiyonunun tek yönlülük özelliğidir yani, özetini kullanarak özetini alan mesaja ulaşmak kolay değildir. İkinci özellik, verilen herhangi bir mesaj (M) için, M 'den farklı ve aynı özete sahip başka bir mesaj bulunması zordur. Özetleyecek olursak, özetleme fonksiyonlarının sağlaması gereken temel özellikler aşağıda belirtilmiştir:

- Özetlenecek mesaj (girdi) herhangi bir boyutta olabilir.
- Mesaj özeti (çıkıtı) sabit bir uzunluktadır.
- Verilen herhangi bir mesaj için özeti hesaplanması kolaydır.
- $H(x)$ tek yönlüdür.
- $H(x)$ çakışmalara karşı dayanıklıdır.

Güvenli Özetleme Algoritmaları (SHA- Secure Hash Algorithms): Güvenli Özetleme Algoritması, Amerika'nın ulusal güvenlik kurumu olan NSA (National Security Agency) tarafından tasarlanmış ve ilk olarak 1993 yılında FIPS PUB 180 standardında yayınlanmıştır. Sıkıştırma fonksiyonundaki küçük bir değişiklik 2 yıl sonra tekrar NSA tarafından SHA-1 adında FIPS 180-1 standardında yayınlanmıştır.

SHA-1, uzunluğu en fazla 2^{64} bit olan mesajları girdi olarak kullanır ve 160 bit'lik mesaj özeti üretir. Bu işlem sırasında, ilk önce mesajı 512 bit'lik bloklara ayılır ve gerekirse son bloğun uzunluğunu 512 bit'e tamamlar. SHA-1 çalışma prensibi olarak R. Rivest tarafından tasarlanan MD5 özet fonksiyonuna benzer tekrarlayan bir yapısı vardır. Her tekrarlama bir sıkıştırma fonksiyonu kullanır. Bu fonksiyon, mesajın 512 bit'lik bloğunu alır ve 16 bit'lik kelimelere ($m_0, m_1, \dots, m_{15}$) çevirir. Daha sonra bu kelimeler (5.11) eşitliği kullanılarak 2560 bit'e genişletilir ve her biri 20 matematiksel fonksiyon içeren 4 tur çalıştırılır ve 160 bit'lik

mesajın özeti elde edilir.

$$m_i = (m_{i-3} + m_{i-8} + m_{i-14} + m_{i-16}) \ll 1 \quad (5.11)$$

SHA özet fonksiyon ailesinde çıktı uzunluğu daha uzun olan ve küçük farklar içeren ve SHA-2 ailesi olarak adlandırılan dört farklı algoritma (SHA-224, SHA-256, SHA-384 ve SHA-512) bulunur. SHA-2 algoritmaları SHA-1 algoritmalarına göre daha güvenli yani, kırılması çok daha zor algoritmalarlardır. Ancak bunun yanında işlem hızı açısından da çok daha yavaş algoritmalarlardır. Çizelge 5.4’de tüm SHA algoritmalarının karşılaştırılması yapılmıştır.

Çizelge 5.4 SHA algoritmalarının karşılaştırılması

	Mesaj Uzunluğu	Blok Uzunluğu	Mesaj Özeti
SHA1	$< 2^{64}$	512	160
SHA256	$< 2^{64}$	512	256
SHA384	$< 2^{128}$	1024	384
SHA512	$< 2^{128}$	1024	512

Mesaj Özeti 5 (MD5-Message Digest 5): MD5, veri bütünlüğünü test etmek için kullanılan, Ron Rivest tarafından 1991 yılında geliştirilmiş bir tek yönlü şifreleme algoritmasıdır. Girdi olarak kabul edilen verinin boyutundan bağımsız olarak 128 bit’lik (16 Byte) özetler (çıktılar) üretir. Örneğin 17645312 verisinin MD5 algoritması ile özetlenmiş hali 98b011d88c9ae33766814dcc76ad7b5c olmaktadır.

5.1.5 Anahtar Anlaşma/Takas Metotları (Key Agreements/Exchange Methods)

Anahtar anlaşma/takas metotları içerisinde yaygın olarak kullanılan birkaç tane mekanizma bulunmaktadır. Bu mekanizmaların kullanılma sebebine gelince şifreleme için gerekli olan anahtar bilgisinin açık bir şekilde gönderilmemesi gerekmektedir. Tam olarak bu mekanizmaların nasıl uygulanacağı bu mekanizmaları kullanan MIKEY, IKE, vb. gibi anahtar yönetim protokollerine bağlıdır. Bu protokollere ileriki bölümlerde ayrıntılı olarak değinilecektir. Başlıca anahtar anlaşma/takas metotları şu şekildedir :

- Ön-Paylaşımlı Anahtar Anlaşma Metodu (PSK-Pre-Shared Key Agreement).
- Diffie-Hellman Anahtar Anlaşma/Takas Metodu.
- Açık Anahtar Altyapısı (PKI – Public Key Infrastructure).

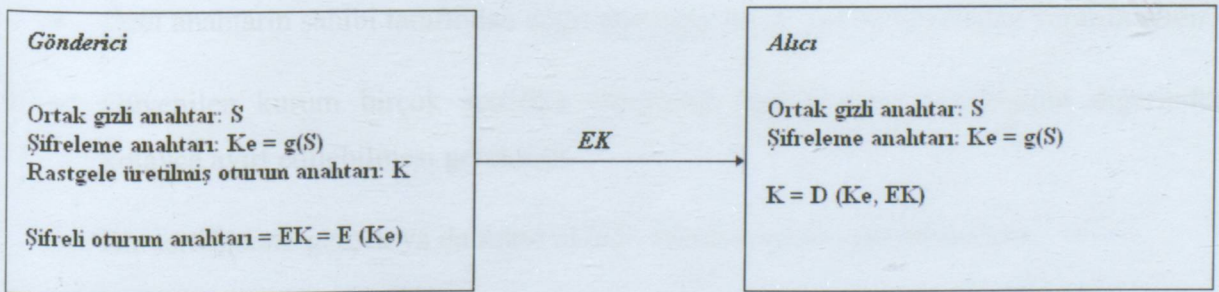
Bunlardan ilki simetrik şifreleme algoritmalarında kullanılırken; diğerleri ise önceki bölümlerde de anlatıldığı üzere asimetrik şifreleme yani, açık anahtar şifreleme algoritmalarında kullanılmaktadır. Diffie-Hellman metodunu önceki bölümlerde gördük, şimdi diğer iki yönteme ayrıntılı olarak değinelim.

5.1.5.1 Ön-Paylaşımlı Anahtar Anlaşma Metodu (PSK-Pre-Shared Key Agreement)

Ön paylaşımlı anahtar anlaşma metodu simetrik şifreleme metotlarında kullanılan bir anahtar anlaşma mekanizmasıdır. En temel anahtar anlaşma protokolü olan ön paylaşımlı anahtar her iki terminalin (katılımcının) de ortak bir gizli anahtarını (secret key) paylaşmalarını gerektirmektedir. Yani, her iki terminalde de önceden tanımlı olan bir sır anahtarı bulunmaktadır. Her iki terminal de bu anahtarı bir şifreleme anahtarı (encryption key) türetmek için kullanmaktadır. Sonrasında, gönderici üretilmiş şifreleme anahtarı ile şifrelenen rasgele üretilen bir oturum anahtarı (session key) oluşturur ve gönderir. Alıcı terminal mesajı alır ve ortak sır anahtarı ile şifre çözme işlemini uygular ve böylece mesajı içeren oturum anahtarına erişir (Şekil 5.10).

Bu mekanizma her ne kadar hızlı ve basit olsa da, katılımcılar arasında ortak bir gizli anahtarının tutulması gerekliliği biraz sıkıntılıdır. Bu nedenle de bu metot çok ölçeklenebilir değildir. Bir ön paylaşımlı anahtar planı sadece birkaç kullanıcının bulunduğu senaryolar için daha uygun bir metottur. Bu senaryoda anahtar yönetimi daha kolay olmaktadır.

Ön paylaşımlı bir anahtarın uzun bir zaman diliminde kullanılabilmesi ve bu anahtarın yenilenmesinin çok kolay olmamasından dolayı anahtar takası genelde aynı anahtar kullanılarak gerçekleştirilmektedir.



Şekil 5.10 Ön-Paylaşımlı anahtar anlaşma metodu (Kultti, 2005)

Şekil 5.10'da E fonksiyonu şifrelemeyi ifade ederken D fonksiyonu şifre çözmeyi ifade etmektedir.

5.1.5.2 Açık Anahtar Altyapısı (PKI – Public Key Infrastructure)

Asimetrik şifreleme sistemleri anahtar yönetimi konusunda simetrik şifreleme sistemlerine göre çok daha başarılıdırlar. Asimetrik şifreleme sistemleri bu nedenle anahtar yönetimi için en çok tercih edilen sistemlerin başında gelir. Açık anahtar altyapısına (AAA) aşağıdaki iki sebepten dolayı ihtiyaç duyulur:

- Asimetrik şifreleme sistemlerini gerçeklemek için.
- Açık ve özel anahtarları yönetmek için.

Ayrıca açık anahtar altyapısı sistemleri bize kimlik doğrulama, inkar edememe, mesaj bütünlüğü ve gizlilik gibi hizmetleri simetrik şifrelemenin kullanıldığı bir yöntemle sunarlar.

Asimetrik şifrelemede bir kişi için üretilen anahtar çifti, özel ve açık anahtardan oluşur. Bu anahtarlardan açık olanı anahtarın sahibiyle haberleşmek isteyen herkes tarafından görülebilir ve kullanılabilir. Bu açık anahtarın isteyen kişilerce kullanımını kolaylaştırmak için değişik şekillerde yayınlanması ve isteyenlerin erişimine açılması mümkündür. Bu yayınlama şekline sertifika adını verilmektedir. Bu tanıma göre ideal bir sertifika aşağıda belirtilen özellikleri taşımalıdır (Tübitak UEKAE, 2006):

- Elektronik ortamda yayınlanabilmesi ve otomatik olarak işlenebilmesi için tamamen sayısal olmalıdır.
- Özel anahtarın sahibinin adını, çalıştığı şirketin/kurumun adını ve irtibat bilgilerini içermelidir.
- Sertifikanın ne zaman yayınlandığını anlamak kolay olmalıdır.
- Özel anahtarın sahibi tarafından değil güvenilir bir 3. kurum tarafından yaratılmalıdır.
- Güvenilen kurum birçok sertifika yaratacağı için her bir sertifikanın diğerinden kolayca ayırt edilebilmesi gereklidir.
- Bir sertifikanın gerçek ya da sahte olduğu kolayca tespit edilebilmelidir.
- Değiştirmeye karşı korunmuş olmalıdır.
- İçindeki bilgilerin güncel olup olmadığı istendiği anda tespit edilebilmelidir.
- Hangi uygulamalar için kullanılabileceği sertifikanın içinde yazmalıdır.

İdeal sertifika tanımına uygun bir elektronik sertifika oluşturabilmek için uluslararası ITU kurumu X.509 standardını tanımlamıştır. Bu standarda uygun olarak hazırlanan bir sertifika aşağıdaki özellikleri taşımaktadır (Tübitak UEKAE, 2006):

- Sayısaldır, bilgisayarda veya elektronik bir cihazda hazırlanır.
- Sahibinin adını ve açık anahtarını içerir.
- Sahibinin çalıştığı şirketin/kurumun adını içerir.
- Genelde sahibinin e-posta adresini içerir.
- Kullanıma giriş tarihini ve son kullanım tarihini içerir.
- Yayınlayan güvenilir kurumun adını içerir.
- Yayınlayan kuruluş tarafından verilmiş tekil bir seri numarasına sahiptir.
- İçeriğin bütünlüğü yayınlayan kuruluşun sayısal imzasıyla koruma altına alınmıştır.

Bu özellikleri taşıyan örnek bir sertifika Şekil 5.11’de verilmektedir.

Seri No	2368
Sertifika Sahibi	Ahmet Uzun
Şirket/Kurum	Zirve Finans A.Ş.
Yayınlayan	UEKAE
E-posta Adresi	auzun@zirve.com.tr
Yayın Tarihi	05.02.2004
Son Kullanım	05.02.2005
Açık Anahtar	2489349e894859f45489450dab45454 ca0908d8809
Yayınlayan Kurumun Sayısal İmzası	ae89349c989893e8989548d0 823048b08023f9e903

Şekil 5.11 X.509 standardına uygun bir sertifika örneği (Tübitak UEKAE, 2006)

5.1.6 Anahtar Yönetim Protokolleri (Key Management Protocols)

Şifreli iletişimin tüm metotlarında tüm katılımcı noktaların şifreleme ve şifre çözme işlemlerini nasıl gerçekleştirecekleri konusunda anlaşma sağlamaları gerekmektedir. Özellikle tüm katılımcıların hangi şifreleme metodunun, hangi anahtarın ve hangi parametrelerin

kullanıldığını bilmeleri gerekmektedir. SRTP, IPSec ve TLS gibi güvenlik protokolleri tüm bu servisler için anahtar yönetim protokolleri kullanılmaktadırlar.

Anahtar yönetim protokolleri şifrelemeyle ilgili parametrelerin katılımcılar arasında belirlenmesini sağlayan anahtar anlaşma/takas mekanizmalarını yönetmekte kullanılmaktadırlar. Anahtar yönetim protokolünün formatı sayesinde katılımcılara güvenli bir haberleşme imkanı sağlayan gerekli parametrelerde mutabakata varılmaktadır. Şimdi bu protokollerin neler olduğunu ve ne gibi özelliklere sahip olduklarına değinelim.

5.1.6.1 İnternet Güvenlik İlişkisi ve Anahtar Yönetim Protokolü (ISAKMP- The İnternet Security Association and Key Management Protocol)

ISAKMP, iki katılımcı arasındaki güvenlik ilişkilerinin (SA-Security Association) kurulumu, müzakeresi, değiştirilmesi ve silinmesi için gerekli prosedürleri ve paket formatlarını tanımlamaktadır. Güvenlik ilişkileri, IP, ulaşım ve uygulama katmanları güvenlik servisleri gibi çeşitli ağ güvenlik servislerinin yürütülmesi için gerekli tüm bilgileri içermektedir. ISAKMP, anahtar takası ve veri doğrulamada kullanılan data alanlarını (Payload field) tanımlamaktadır. Bu formatlar anahtar takası ve veri doğrulama için tutarlı bir yapı sağlamaktadır (Singhai ve Sahoo, 2002).

ISAKMP, anahtar takasının yanı sıra özellikle güvenlik ilişkilerinin yönetimini sağladığı için diğer anahtar yönetim protokollerinden farklıdır. Farklı güvenlik özelliklerine sahip farklı anahtar yönetim protokolleri bulunmaktadır. Ancak güvenlik ilişkisinin formatı konusunda tüm bu farklı anahtar yönetim protokollerinin anlaşmaya varmaları gerekmektedir, işte ISAKMP protokolü bu ortak yapıyı tüm anahtar yönetim protokollerine sunmaktadır.

Güvenlik ilişkisi bir etki alanı içerisinde bulunan noktaların kimlik doğrulaması için oluşturulmuş bir yapıdır. Oturumu açmak için kimlik bilgileri doğrulanan tarafa bu ilişkiler çerçevesinde gerekli izinler verilir. Haberleşme sırasında iki yönlü ilişki kullanılmaktadır. Yani her bir nokta için farklı güven ilişkileri kullanılır. Bir bağlantı esnasında sunucu istemciden güven belgesi ister ve kendi içerisinde bulunan sertifikayı gönderir.

5.1.6.2 İnternet Anahtar Takası (IKE- İnternet Key Exchange)

İnternet Anahtar Takas Protokolü, ISAKMP protokolüne benzer yapıda ancak ISAKMP, İnternet için Güvenli Anahtar Takas Mekanizması (SKEME-Secure Key Exchange Mechanism for İnternet) ve Oakley Anahtar Belirleme (Oakley Key Determination)

protokollerine dayanan karma bir protokoldür (Harkins ve Carrel, 1998). IKE özellikle **IPsec** protokolü için gerekli anahtar anlařma mekanizmasının yönetimi için geliştirilmiřtir.

IKE protokolü iki nokta arasındaki güvenlik iliřkisinin (SA-Security Association) elde edilmesinden sorumludur. SA, IPsec tarafından IP bařlığının řifrelenmesinde kullanılan řifre anahtarlarını ve řifre profilini içermektedir.

Veriyi řifrelemek ve dođrulamak, řifreleme ve dođrulama algoritmaları ve bunlar için gerekli olan bir oturum anahtarıyla yapılır. IKE protokolü bu oturum anahtarlarının dađıtımını yapmak ve uç noktalarının hangi güvenlik politikalarında anlařacaklarını kararlařtırmak için kullanılan bir metottur. Yani IKE, SA'ların yaratılmasını üstlenir ve bilgiyi güvenli hale getirmede kullanılacak anahtarları yaratır. Bu teknik veriyi řifreleyip deřifrelemede kullanılacak simetrik anahtarların yaratılmasını sađlar.

IKE'nin üç ana görevi bulunmaktadır:

- Uç noktalara karřılıklı dođrulama için yöntem sađlar.
- Yeni IPsec bađlantıları oluřturur (yeni SA'lar yaratır).
- Mevcut bađlantıları yönetir.

İleriki bölümlerde IPsec protokolü anlatılırken IKE protokolüne daha ayrıntılı olarak deđinilecektir.

5.1.6.3 Çoklu Ortam Internet Anahtarlama (MIKEY-Multimedia Internet Keying)

MIKEY, güvenli çoklu ortam oturumlarının kurulmasını sađlayan gereksinimleri karřılamak için tasarlanmıř bir protokoldür. Bu protokolün bařlıca özellikleri řu řekildedir (Arkko vd., 2004):

- Güvenlik amaçlı kullanılan parametreler çift yönlü (gidiř-dönüř) olarak deđiřtirilebilmektedir.
- Basit yapıdadır.
- SDP gibi oturum kurma protokollerinde uygulanabilmektedir.
- Noktadan noktaya güvenliđi sađlayabilmektedir (end-to-end security).
- Düşük bant geniřliđi tüketimi ve düşük iř gücü gereksinimi sađlamaktadır.

MIKEY protokolü, gerçek-zamanlı multimedya 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 protokollerine entegre olabilmesidir. 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.

MIKEY protokolünde kullanılan başlıca terimler şunlardır (Orrblad, 2004):

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.

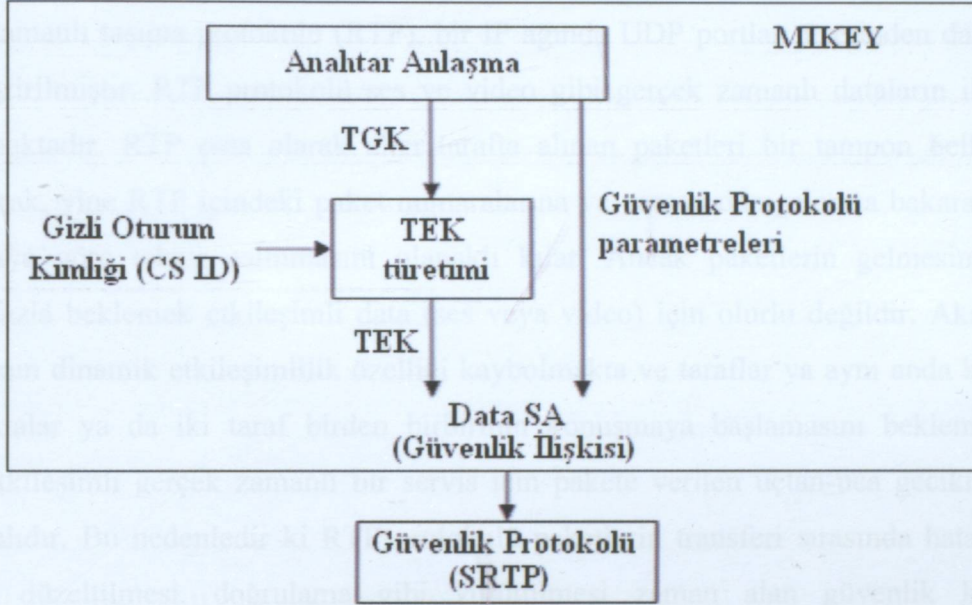
TEK Üretim Anahtarı (TGK-TEK Generation Key): İki ya da daha fazla katılımcının kendi aralarında anlaşmaya vardıkları bir anahtardır. TEK anahtarlarının üretilmesinde kullanılır.

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

MIKEY Protokolü Çalışma Prensipleri: Başlangıçta MIKEY protokolü rasgele bir TGK anahtarı üretir. Bu anahtar vasıtasıyla güvenlik protokolünün kullanacağı anahtar olan TEK anahtarı belli bir CS ile ilişkilendirilerek oluşturulur. Her bir veri akışı (oturum) için farklı bir

CS ve farklı bir TEK anahtarı oluşturulmaktadır. Bu farklı oturumlar birbirinden CS ID ile ayrılmaktadır (Şekil 5.12).

Bir CSB birden fazla gizli oturum (CS) içermektedir. Her bir CS 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 5.12 MIKEY anahtar yönetim protokolü (Orrblad, 2004)

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 önceki bölümde anlatılan anahtar takas metotları kullanılmaktadır.

5.1.7 Güvenlik Protokolleri

Katılımcılar arasındaki şifreleme metotlarının, anahtar takas metotlarının ve anahtar yönetim protokollerinin belirlenmesini sağlamak amaçlı güvenlik protokolleri kullanılmaktadır. Bu güvenlik protokolleri sayesinde katılımcılar hangi anahtar yönetim protokolünün ve hangi anahtar takas metodunun kullanılması konusunda karşılıklı olarak mutabakata varırlar.

5.1.7.1 Güvenli Gerçek Zamanlı Taşıma Protokolü (SRTP-Secure Real-Time Transport Protocol)

Ses ve etkileşimli (iki-yönlü) video uygulamaları gerçek-zamanda çalışmalıdır. Gerçek zamandan anlaşılan, sesi gönderen taraftaki ses işaretleri arasındaki zamansal ilişkinin en az gecikme ile ve bozulmadan alıcı tarafından alınabilmesidir. Böylece alıcı alınan işarete karşı düşen ses veya videodan istenen anlamı çıkarabilmeli ve dinamik etkileşimi bozmadan yanıt verebilmelidir.

Gerçek-zamanlı taşıma protokolü (RTP), bir IP ağında UDP portları üzerinden data taşımak için geliştirilmiştir. RTP protokolü ses ve video gibi gerçek zamanlı dataların iletimi için kullanılmaktadır. RTP esas olarak alıcı tarafta alınan paketleri bir tampon bellekte önce depolayarak, yine RTP içindeki paket numaralarına ve zaman damgalarına bakarak belli bir algoritmaya göre tekrar çalınmasını olanaklı kılar. Ancak paketlerin gelmesini 150-200 ms'den fazla beklemek etkileşimli data (ses veya video) için olurlu değildir. Aksi takdirde konuşmanın dinamik etkileşimlilik özelliği kaybolmakta ve taraflar ya aynı anda konuşmaya başlamaktalar ya da iki taraf birden birbirinin konuşmaya başlamasını beklemektedirler. Kısaca etkileşimli gerçek zamanlı bir servis için pakete verilen uçtan-uca gecikme bütçesi aşılmamalıdır. Bu nedenledir ki RTP protokolü paketlerin 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, vb. gibi güvenlik işlemlerini sağlamaktadır. SRTP'nin bir anahtar türetim mekanizması ve şifreleme algoritması içeren bir formatı bulunmaktadır. Anahtar türetim mekanizması MIKEY gibi bir anahtar yapısına ihtiyaç duymaktadır. SRTP protokolü IETF tarafından 2004 yılının Mart ayında yayınlanmıştır (Baugher ve McGrew, 2004).

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 (Orrblad, 2004):

1. SRTP aşağıda belirtilen işlevleri sayesinde gelişmiş bir güvenlik sağlamaktadır

- 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 datalara gerçekleştirilebilecek saldırılara karşı büyük bir savunma sağlamaktadır.
- Yeni şifreleme algoritmalarını benimseyebilecek güncellenebilir bir yapıya sahiptir.
- Her iki terminalde de rasgele oturum anahtar türetim fonksiyonunu gerçekleştiren güvenli bir yapısı bulunmaktadır. Bu rasgele oluşturulan anahtarlar ön-hesaplama ataklarına karşı bir koruma sağlamaktadır.

2. SRTP aşağıda belirtilen işlevleri sayesinde yüksek bir performans 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 data belleği çok az bir yer kaplamaktadır.

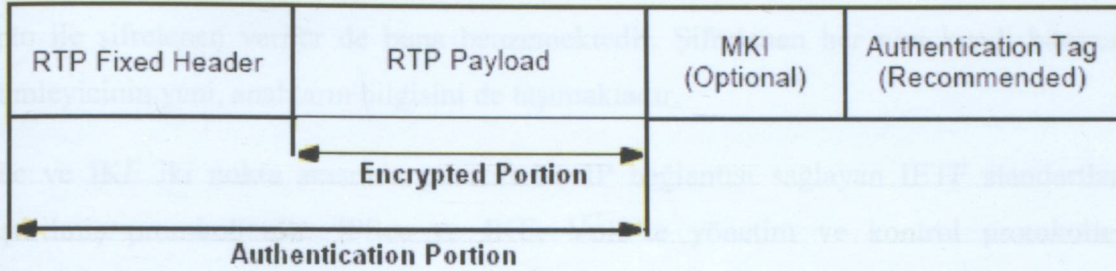
3. SRTP'nin aynı zamanda aşağıda belirtilen avantajları bulunmaktadır:

- SRTP protokolü RTP protokolünün bir profili olarak tanımlanmıştır. Bu nedenle varolan RTP yığınları içerisine kolaylıkla entegre edilebilmektedir.
- SRTP, OSI referans modelinin 5. katmanında (oturum katmanı) şifreleme sağlamaktadır. Yani, SRTP protokolü RTP tarafından kullanılan önde gelen katmanlardan olan ulaşım, ağ ve fiziksel katmanlardan bağımsızdır. Paket kayıplarında, kayıp durumlarında paketlerin alıcıya tekrar gönderilmesinde ve bit hatalarına karşı özellikle çok hassastır.
- SRTP, anahtar yönetiminin sebep olduğu yükü hafifletmektedir. Çünkü gizlilik, bütünlüğü sağlama gibi anahtarlama işlevlerini tek bir anahtar hem SRTP akışları hem de buna ilişkin SRTCP akışları için gerçekleştirmektedir. Özel durumlarda tek bir anahtar, birden fazla SRTP akışını koruyabilmektedir.

Bir RTP profili olarak tanımlanmasından dolayı SRTP, mevcut çoklu ortam (multimedya) standartları ile kullanılabilir. H.323 protokolü için SRTP desteği H.235 Annex G ile tanımlanmıştır. SIP protokolü için ise SRTP için gerekli anahtar yönetim mekanizmalarının

desteklenmesi için Oturum Tanımlama Protokolü (SDP-Session Description Protocol) geliřtirmeleri tanımlanmıřtır. Böylece, SRTP ve MIKEY kombinasyonu H.323 ve SIP gibi farklı multimedya standartları arasında uçtan uca řifreleme saęlamaktadır.

SRTP Paket Yapısı:



řekil 5.13 SRTP protokolü paket yapısı (Baugher ve McGrew, 2004)

SRTP güvenli olmayan RTP paketlerini güvenli hale getiren bir RTP profili ve uzantısıdır. SRTP paket yapısı sabit RTP paketini (RTP Payload) belli bir řifreleme metodu kullanarak řifreler ve RTP paketi alıcıya řifrenmiř olarak gönderilir. SRTP, RTP paketinin řifrenmesinde Geliřmiř řifreleme Sistemini (AES-Advanced Encryption System) kullanmaktadır.

Bununla birlikte SRTP protokolü, Ana Anahtar Kimlięi (MKI-Master Key Identifier) ve Mesaj Doğrulama Etiketini (Authentication Tag) adı verilen iki alanı daha içermektedir (řekil 5.13). Opsiyonel olan ana anahtar kimlięi alıcı tarafa hangi anahtarın kullanılacağını belirtirken; kullanılması tavsiye edilen doğrulama etiketi ise mesaj doğrulama verisini taşımak için kullanılmaktadır.

Doęrulama etiketi sabit RTP Bařlık (RTP Header) bilgisiyle řifrenmiř RTP Paketinin (RTP Payload) toplam boyutunu içermektedir. Alıcı taraf paketi aldıktan sonra doğrulama etiketinde yazan deęer ile kendisine ulaşan RTP Bařlık bilgisiyle řifrenmiř RTP Paketinin toplam boyutunu karşılaştırır ve paketin doğru bir paket olup olmadığı bilgisine ulaşır.

SRTP protokolü anahtar takası için Çoklu Ortam İnternet Anahtarlama (MIKEY- Multimedia İnternet KEYing) protokolünü kullanmaktadır. MIKEY anahtarların ve güvenlik parametrelerinin takası için kullanılmaktadır. SRTP’de MIKEY protokolü gizlilik ve veri bütünlüęü gibi güvenlik işlevlerini gerçekleřtirmek için tek bir “Ana Anahtar (Master Key)” kullanmaktadır. Bu ana anahtarla ilgili bilgi Ana Anahtar Kimlięi (MKI-Master Key Identifier) alanı tarafından tanımlanmaktadır.

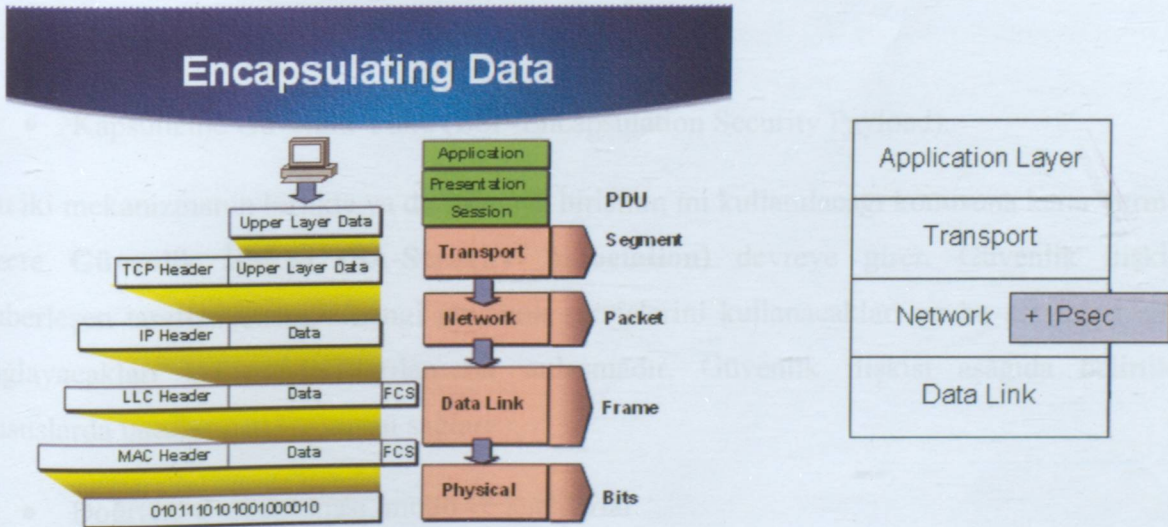
5.1.7.2 İnternet Protokolü Güvenliği (IPSec-IP Security)

Veri şifreleme, basit veya karmaşık kripto sistemleriyle oluşturulmaktadır. Sistemler arasında gönderilmek istenen veri ilk haliyle şifrelenir. Şifrelenen veri karşı sisteme ulaştığında ise şifre çözme işlemi uygulanır. Her şifrelenen veri herhangi bir sistem ile çözümlenemez. Bunu farklı kapıların kilit yapılarının ve anahtarlarının farklı olduğu mantığına benzetebiliriz. Kripto ile şifrelenen veriler de buna benzemektedir. Şifrelenen her veri kendi bünyesinde çözümleyicinin yani, anahtarın bilgisini de taşımaktadır.

IPSec ve IKE iki nokta arasında güvenli bir IP bağlantısı sağlayan IETF standartlarında geliştirilmiş protokollerdir. IPSec ve IKE, VoIP'te yönetim ve kontrol protokollerinin güvenliğini sağlamak için kullanılmaktadır. IPSec, IP trafiğinin güvenliğinden sorumluyken IKE protokolü ise IPSec şifre anahtarlarının ve Güvenlik İlişkisinin (SA – Security Association) oluşturulmasından sorumludur (Orrblad, 2004).

IPSec, güvensiz bir ortamda iki kişinin güvenli bir şekilde konuşmasını sağlamak ve bu konuşma sırasında her iki kişinin gerçekten doğru kişiler olmasının sağlanması ve ilgili konuşmanın 3. bir kişi tarafından dinlenmemesini/değiştirilmemesini sağlamak için kullanılan bir protokoldür.

IPSec tanım olarak OSI referans modelinin IP katmanında tüm IP iletişimini şifrelemek ve doğrulamak için kullanılan bir standarttır (Şekil 5.14).



Şekil 5.14 OSI referans modelinde IPSec protokolünün yeri (Orrblad, 2004)

IPSec protokolünün katılımcılara sağladığı işlevler başlıca şu şekildedir:

- Doğrulama (Authentication): Her iki kişinin gerçekten doğru kişiler olması.
- Veri bütünlüğü (Data integrity): Konuşmanın içeriğinin değişmeden karşıya ulaşması.
- Gizlilik (Confidentiality/Encryption): Konuşmanın 3. bir kişi tarafından duyulsa bile anlaşılmaması.
- İnkâr edememe (Non-repudiation) : Bir mesajı gönderen kişinin o mesajı size gönderdiğini inkâr edememesini sağlayan alındı onayı.

IPSec protokolünün yapısına değinmeden önce basit anlamda IPSec protokolünün ağ güvenliğini nasıl sağladığını ifade edecek olursak:

1. Karşılıklı olarak katılımcılar arasında kimlik doğrulaması yapılır.
2. Katılımcılar arasında güvenlik anlaşması yapılır.
3. Veriler şifrelenmiş olarak katılımcılar arasında iletilir.

IPSec bağlantılarının oluşturulması esnasında karşı taraf ile bir **tünel** anlaşması yapılır. Tünel işleminde paketler bir çerçeve içerisine alınarak saklanır. Paketler istenilen hedefe ulaştığı an saklama üst verisi iptal olur ve paketin hedefe yönlendirilmesi için asıl paket verisi kullanılır.

IPSec protokolü iki tip tünel modunu desteklemektedir. Bunlar:

- Doğrulama Başlığı (AH-Authentication Header).
- Kapsülleme Güvenlik Yüğü (ESP-Encapsulation Security Payload).

Bu iki mekanizmanın birlikte ya da yalnızca birisinin mi kullanılacağı konusuna karar vermek üzere **Güvenlik İlişkisi (SA-Security Association)** devreye girer. Güvenlik ilişkisi, haberleşen taraflar arasında hangi güvenlik servislerini kullanacakları ve bu servisleri nasıl sağlayacakları konusunda varılan bir anlaşmadır. Güvenlik ilişkisi aşağıda belirtilen hususlarda tarafların anlaşmasını sağlar:

- Doğrulama algoritması, modu ve anahtarlar.
- Şifreleme algoritması, modu ve anahtarlar.
- Şifreleme algoritması senkronizasyonu için Başlangıç Vektörü (IV-Initiation Vector) uzunluğu.

- Anahtarlar ve Güvenlik ilişkisinin ömrü.
- Güvenlik ilişkisinin kaynak adresi (ağ ya da alt ağ adresi de olabilir).

Güvenlik ilişkisi, Bir etki alanı içerisinde bulunan noktaların kimlik doğrulaması için oluşturulmuş bir yapıdır. Oturumu açmak için kimlik bilgileri doğrulanan tarafa bu ilişkiler çerçevesinde gerekli izinler verilir. Haberleşme sırasında iki yönlü ilişki kullanılmaktadır. Yani her bir nokta için farklı güven ilişkileri kullanılır. İki makine IPSec ile haberleşmeden önce birbirlerinin kimlik tanımlamasını yapmalı ve bir şifreleme metodu üzerinde anlaşmalıdırlar. Makineler bunu bir veya daha fazla güvenlik ilişkisi kurarak gerçekleştirirler. Güvenlik ilişkisi iki makine arasında kullanılacak olan belirli güvenlik ayarlarına bağlı bir anlaşma gibi düşünülebilir. Güvenlik ilişkileri tek yönlüdür ve belirli bir ömre sahiptirler. Tipik olarak, iki taraf arasındaki iki-yönlü haberleşmelerde iki SA'ya ihtiyaç vardır.

Güvenlik ilişkileri, IPSec konuşan cihazlarda (örneğin VoIP ağ geçidi) özel bir veritabanında saklanırlar ve veritabanı içerisinde her AH veya ESP başlığında bulunan **Güvenlik Parametre İndeksi (SPI - Secure Parameter Index)** sayesinde tanınırlar. Bir IP paketi alındığında alıcı taraf paketin güvenlik parametre indeksi üzerinden ilgili güvenlik ilişkisinin içeriğine ulaşır ve paketi nasıl çözmesi gerektiği konusunda bilgi edinir. Eğer alıcı taraf, IP paketini herhangi bir güvenlik ilişkisi içeriği ile ilişkilendiremezse veya yanlış bir anlaşma üzerinden paketi açmaya çalışırsa paketi yanlış çözümler.

Güvenlik ilişkisi, anlaşma sağlanmış bir anahtar, güvenlik iletişim kuralı ve güvenlik parametre indeksi birleşiminden oluşur. Bunlar birlikte kullanıldığında, gönderenden alana doğru iletişimi korumak için kullanılan güvenliği tanımlar. SPI, SA'da yer alan ve alıcı tarafta bulunan birden çok güvenlik ilişkisini ayırt etmekte kullanılan benzersiz, tanımlayıcı bir değerdir. Örneğin, bir VoIP cihazı birden çok VoIP cihazıyla aynı anda güvenli iletişim kurabilir. Bu durumda, hedef VoIP cihazı gelen paketleri işlemek için hangi SA'nın kullanılacağını belirlemek amacıyla SPI'ları kullanır. Yani kısaca bir VoIP cihazı farklı VoIP cihazlarını SPI'lar vasıtasıyla ayırt eder.

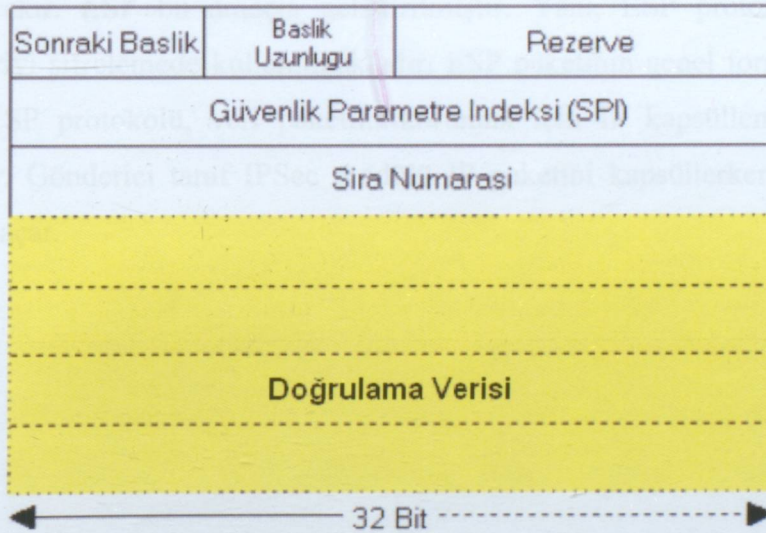
Güvenlik ilişkilerini yönetimini Internet Anahtar Takası (IKE- Internet Key Exchange) protokolü sağlamaktadır. IKE, Güvenlik ilişkisi yönetimini merkezileştirir, böylece bağlanma süresini azaltmış olur. Bilgileri güvenlik altına almak için kullanılan, paylaşılan gizli anahtarlar oluşturur ve yönetir.

Şimdi IPSec protokolünün desteklediği tünel modlarını ayrıntılı olarak inceleyelim.

Doğrulama Başlığı (AH-Authentication Header): AH, adından da anlaşılacağı gibi sadece doğrulama işlemini sağlamaktadır yani, veriyi doğrulamak için kullanılan bir protokoldür. AH, IP paketindeki data için şifreli karmaşık bir fonksiyon kullanarak **Mesaj Doğrulama Kodu (MAC-Message Authentication Code)** bilgisi elde eder. Bu MAC verisi orijinal paket ile beraber karşı tarafa yollanır ve alıcı kişinin orijinal verinin bütünlüğünün değiştirilmediğini anlamasını sağlar.

IPSec protokolünde AH, IP paketleri için veri kaynağının doğrulanması ve bağlantısız veri bütünlüğünün sağlanması amacıyla kullanılır. Kullanılan şifreleme algoritmasının türüne bağlı olarak kaynağın inkar edilememesini de sağlar. IP paketlerine doğrulama verisi (MAC) eklenir (Şekil 5.15). Doğrulama bir doğrulama algoritması ve ilgili anahtarın kullanımıyla sağlanır. IP paketinde bulunan veriden MAC oluşturmak için MD5 ya da SHA-1 gibi özetleme algoritmaları kullanır. Elde edilen MAC, karşı tarafa, mesajın bütünlüğünün korunduğunun anlaşılması için, orijinal paketle birlikte iletilir.

Gönderici IP paketini göndermeden önce doğrulama başlığını hesaplar, alıcı ise SPI ile ilgili güvenlik ilişkisi içeriğine bakarak hangi doğrulama algoritmasının ve anahtarlama yönteminin kullandığını bulur ve göndericiyi doğrular.



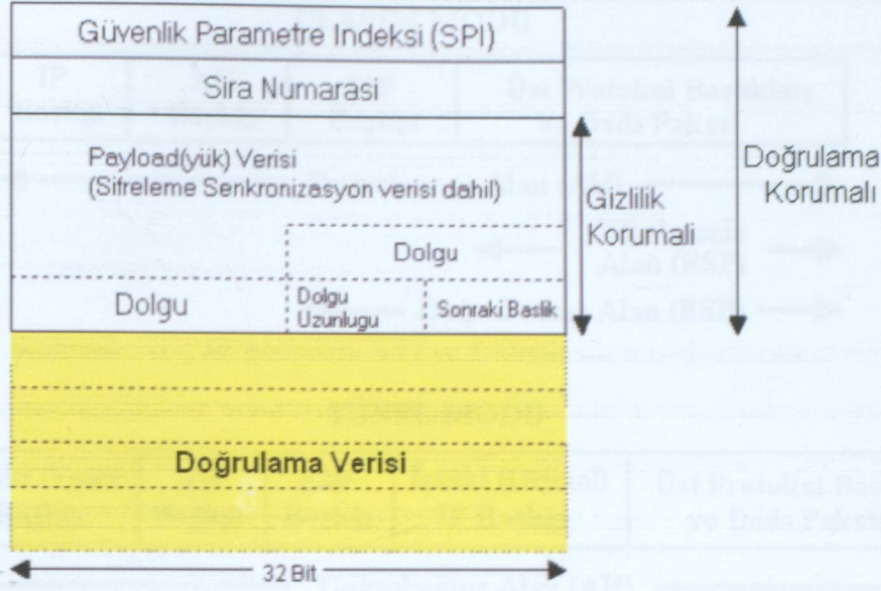
Şekil 5.15 IPSec AH başlık formatı (Orrblad, 2004)

- **Sonraki Başlık (Next Header):** Orijinal IP başlığının protokol numarasını ifade etmektedir. Yükü tanımlamak için kullanılır, TCP veya UDP gibi.
- **Başlık Uzunluğu (Payload Length):** Kimlik doğrulama başlığının uzunluğunu belirtir.

- **Güvenlik Parametre İndeksi (SPI-Security Parameter Index):** Kimlik doğrulama başlığı bağlantılarını diğerlerinden ayırmayı mümkün kılan güvenlik ilişkilerini belirlemeyi sağlayan 32-bit'lik bir seri numaradır.
- **Sıra Numarası (Sequence Number):** AH datagramının seri numarasını ifade eder. Birden başlayarak arttırılarak haberleşmede güvenlik ilişkisi üzerinde gönderilen paket sayısını belirler. Sıra numarasının tekrarlanmasına izin verilmez. Alıcı bu numaraya ait güvenlik ilişkisinin sıra numarasını kontrol ederek daha önce alınıp alınmadığını belirler. Eğer daha önce alınmış ise paket kabul edilmez.
- **Doğrulama Verisi (MAC-Massage Authentication Code):** Alıcının orijinal verinin bütünlüğünün değiştirilmediğini anlamasını sağlayan bir sağlama toplamı (checksum).

Kapsülleme Güvenlik Yüğü (ESP-Encapsulation Security Payload): ESP, yük doğrulama (payload authentication), veri bütünlüğü (data integrity) ve güvenilirlik/şifreleme (confidentiality/encryption) işlemlerinin tümünü gerçekleştirmektedir. ESP protokolü hem doğrulama hem de güvenilirlik için kullanılabilir. Bunun yanında sadece doğrulama veya sadece güvenilirlik için de kullanılabilir.

IP paketinin yük (payload) verisi doğrulama sırasında açıktır ve verinin gizliliği için şifrenmesi gerekir. ESP bu amaçla geliştirilmiştir. Yani, ESP protokolü IP paketinin içindeki tüm veriyi şifrelemede kullanılmaktadır. ESP paketinin genel formatı Şekil 5.16'da verilmektedir. ESP protokolü, veri paketini korumak için IP kapsülleme (encapsulation) işlemini kullanır. Gönderici taraf IPsec modülü IP paketini kapsüllerken, alıcı taraf IPsec modülü kapsülü açar.



Şekil 5.16 IPsec ESP başlık formatı (Orrblad, 2004)

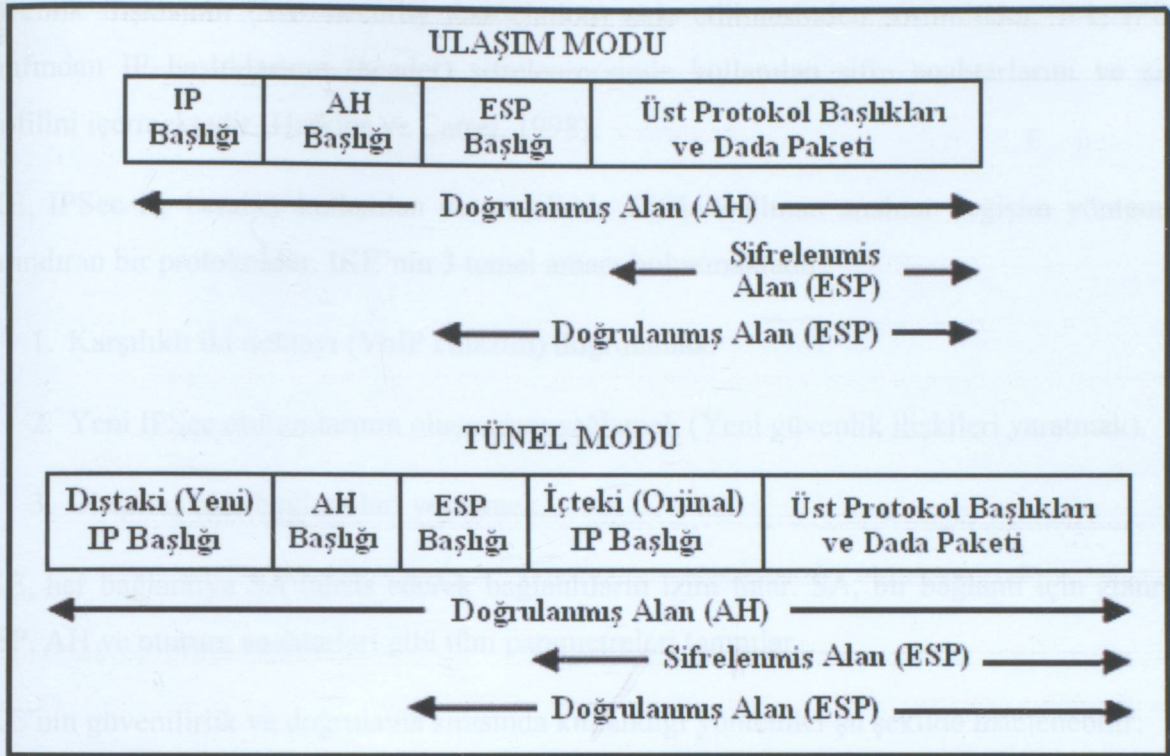
- *Dolgu (Padding):* Kullanılan blok şifrelemenin blok ölçüsüne uyacak şekilde verinin uzunluğunu değiştirmek için kullanılan bir bölümdür. 0 ile 255 byte arasında değişmektedir.
- *Dolgu Uzunluğu:* Dolgu alanının byte olarak uzunluğunu ifade etmektedir.

IPsec iki ayrı iletim modunu desteklemektedir. Bunlar:

- Ulaşım Modu (Transport Mode).
- Tünel Modu (Tunnel Mode).

Ulaşım Modu: Bu modda, IP paketinin sadece üst katmanlarındaki başlık (header) kısmı ve veri kısmı şifrelenmektedir. IP başlığı ve alt katman başlıkları şifrelenmemektedir. Yani, IP paketinin yükü (payload) olarak üst katman protokol verisi taşınır. Gönderilecek IP paketinde üst katman protokol verisi seçilir ve IP paketine yük olarak şifrelenir.

Tünel Modu: Bu modda IP paketi komple (tüm katmanların başlıkları ve orijinal veri) şifrelenerek yeni bir IP paketi oluşturulmaktadır (Şekil 5.17). IP paketinde sadece üst katman protokol verisi değil tüm paket şifrelenir ve kapsüllenerek yeni bir IP paketi yaratılır. İki sistem arasında tünel kurulduğunda arka plandaki gönderici ve alıcının bilgilerine erişilemez. Alıcı, kullanıcı kimliği ve varış IP adresinden güvenlik ilişkisi bilgisini elde eder. SPI ve IP başlığı açık olarak gönderilir.



Şekil 5.17 IPsec tünel ve ulaşım modları (Kuhn ve Thomas, 2005)

Saklama ve yönlendirme işlemlerinin tümüne tünel oluşturma denilir. Özgün paket yeni bir paket içinde gizlenir. Bu yeni pakette, ağlar arasında dolaşmasını sağlayan yeni adresleme ve yönlendirme bilgileri vardır. Tünel oluşturulduğunda ağdaki trafiği dinleyen kötü amaçlı bir üçüncü kişi, özgün kaynak ve hedef bilgileri gibi özgün paket verilerine hiçbir şekilde ulaşamaz. Saklı alınan (şifrelenen) paketler hedeflerine ulaştığında, saklama üstbilgisi kaldırılır (şifre çözülür) ve orijinal veri elde edilir.

Tünel, içinden saklı paketlerin geçtiği mantıksal bir veri yolu olarak düşünülebilir. Tünel genellikle özgün kaynak ve hedef çiftine saydamdır ve ağ yolunda noktadan noktaya bağlantı olarak görünür. Çiftler, tünelin başlangıç ve bitiş noktaları arasındaki yönlendiricilerden, anahtarlardan, proxy sunucularından veya diğer güvenlik ağ geçitlerinden haberdar değildir.

AH tünel modu, tünelin içeriği için şifreleme gizliliği sağlamaz, yalnızca güçlü bütünlük ve kimlik doğrulama sağlar. ESP Tünel modunda ise bütünlük ve kimlik doğrulamanın yanında DES, 3DES gibi şifreleme metotları ile paketlerin gizliliği sağlanır.

Internet Anahtar Takası (IKE- Internet Key Exchange): IKE protokolü iki nokta arasındaki

güvenlik ilişkisinin (SA- Security Association) elde edilmesinden sorumludur. SA, IPSec tarafından IP başlıklarının (header) şifrelenmesinde kullanılan şifre anahtarlarını ve şifre profilini içermektedir (Harkins ve Carrel, 1998).

IKE, IPSec ile beraber kullanılan ve temelinde Diffie-Hellman anahtar değişim yöntemini barındıran bir protokoldür. IKE'nin 3 temel amacı bulunmaktadır:

1. Karşılıklı iki noktayı (VoIP cihazını) doğrulamak.
2. Yeni IPSec oturumlarının oluşmasını sağlamak (Yeni güvenlik ilişkileri yaratmak).
3. Oluşmuş olan bağlantıları yönetmek.

IKE, her bağlantıya SA tahsis ederek bağlantıların izini tutar. SA, bir bağlantı için atanmış ESP, AH ve oturum anahtarları gibi tüm parametreleri tanımlar.

IKE'nin güvenilirlik ve doğrulama sırasında kullandığı yöntemler şu şekilde listelenebilir:

IKE Güvenilirlik (Encryption) Mekanizmaları: IKE protokolü şifrelemede hem simetrik hem de asimetrik metotları kullanabilmektedir. Ancak günümüzde IPSec için en çok simetrik şifreleme metotları kullanılmaktadır.

- Kullanılabilen simetrik şifreleme metotları: AES, 3DES, DES.
- Kullanılabilen asimetrik şifreleme metotları: RSA, Diffie-Hellman.

IKE Doğrulama (Authentication) Mekanizmaları: IKE protokolü doğrulamada SHA-1 ve MD5 gibi özetleme fonksiyonlarını kullanmaktadır.

IKE protokolü Faz-1 (Phase-1) ve Faz-2 (Phase-2) olmak üzere iki fazdan oluşmaktadır. Faz-1'e Ana Mod (Main Mode); faz-2'ye ise Hızlı Mod (Quick Mode) da denilmektedir.

IKE Faz-1: Bu fazda şifre anahtarı elde etmek için Diffie-Hellman (DH) protokolü çalıştırılmaktadır ve bununla birlikte karşılıklı noktaları doğrulamak için özel bir anahtar üretilmektedir. Bu anahtar her iki noktada da tanımlı olduğu takdirde bu noktalar birbiri ile VoIP görüşmesi yapabilirler.

Kısaca bu modda şu işlemler gerçekleşmektedir:

1. **SA Müzakeresi (SA Negotiation):** Karşılıklı noktalar birbirleriyle bazı hususlarda anlaşmaya varırlar. Bu hususlar; şifreleme metodunu (DES, 3DES gibi), doğrulama protokolünü (MD5, SHA1 gibi), Diffie-Hellman (DH) protokolüyle oluşturulan

anahtarın uzunluğunu ve bu anahtarın yaşam süresini (lifetime), vb. içermektedir.

2. **Anahtar Değiş tokuşu (Key Exchange):** Diffie-Hellman protokolü kullanılarak IPSec için diğer aşamalarda kullanılacak faz-1 anahtarı oluşturulup karşılıklı olarak güvenli bir şekilde iletilmektedir.
3. **Doğrulama (Authentication):** Oluşturulan özel bir anahtarla karşılıklı iki noktanın birbirini doğrulaması sağlanmaktadır. Her bir katılımcıda da aynı anahtarın (şifrenin) önceden tanımlı olması gerekmektedir. Bu anahtara önceden-paylaşılmış anahtar (pre-shared key) adı verilmektedir. Daha sonra bu önceden üzerinde anlaşılmış anahtar özetleme fonksiyonları kullanılarak (MD5 ya da SH1) güvenli bir şekilde taraflar arasında iletilir her iki katılımcı anahtarları karşılaştırarak birbirlerini doğrularlar.

IKE Faz-2: Bu aşamada her iki taraf güvenlik ilişkileri konusunda anlaşmaya varırlar (SA Negotiation). Ayrıca bu modda IPSec'in nasıl korunacağı ve veri akışında kullanılacak şifreleme ve doğrulama oturum anahtarlarını sağlamak için faz-1'den yeni anahtar malzemesi türetilir.

IKE ve IPSec bağlantılarının limitli ömürleri vardır. Bu ömürler zaman (saniye) veya veri miktarı (kilobyte) olarak tanımlanır. Bu ömürler güvenlik amaçlı bağlantıların çok uzun süreler boyunca kullanılmamasını sağlamak için tanımlanırlar. IPSec bağlantı ömrü genellikle IKE bağlantı ömründen kısadır ve IPSec bağlantısı faz-2 görüşmesi uygulanarak kolaylıkla yenilenebilir.

IPSec ve IKE Parametreleri: IPSec protokolünü konuşturabilmek için, IPSec ve IKE ile ilgili kullanılabilecek birçok parametre mevcuttur. IPSec bağlantısını oluştururken bu parametrelerin iyice anlaşılması ve bu parametrelere dikkat edilmesi gerekmektedir. Bu parametreleri özetleyecek olursak:

- IPSec iletim modu (Tünel/Ulaşım).
- IPSec tünel modu (ESP/AH/ya da her ikisinde).
- IPSec bağlantı ömrü.
- IKE modu (Ana mod/Hızlı mod).
- IKE şifreleme metodu (DES, 3DES, AES, vb.).
- IKE Diffie-Hellman protokol grubu.

- IKE doğrulama metodu (MD5 ya da SH1).
- IKE SA ömrü.

Sonuç itibariyle VoIP üzerinden haberleşen iki nokta arasında IPSec güvenlik protokolünün kullanıldığı durumda sırasıyla gerçekleşen işlemler şu şekilde olmaktadır:

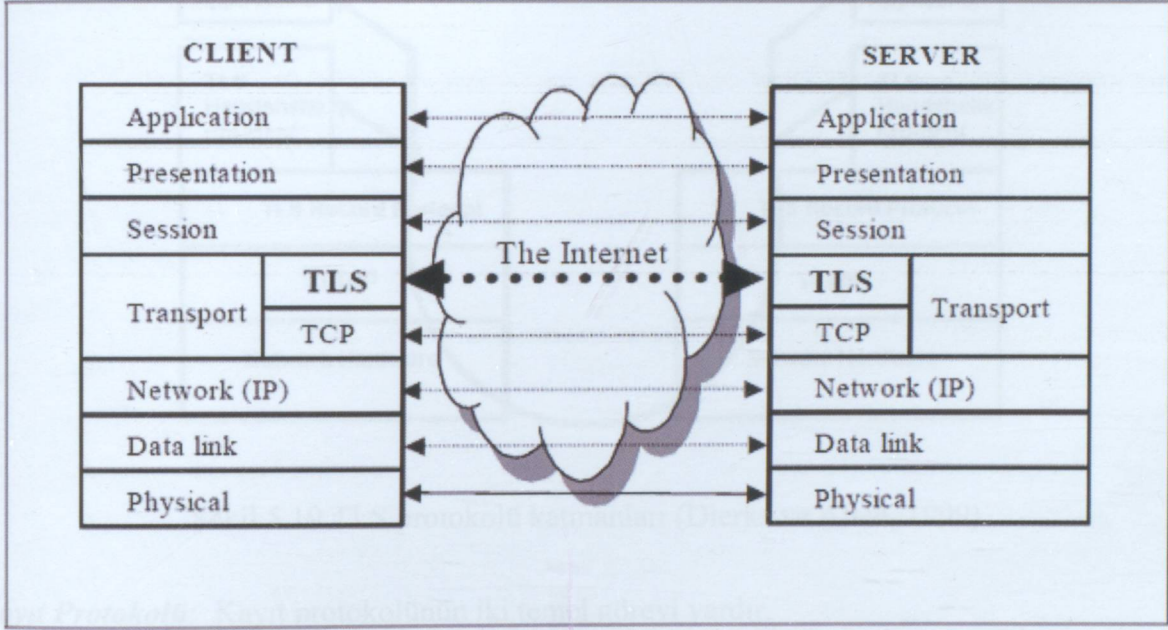
1. IKE ana modda, karşılıklı her iki noktada da tanımlı olmak zorunda olan özel bir anahtar (pre-shared key) tanımlanır ve her iki nokta birbirini bu anahtar vasıtasıyla doğrular.
2. IKE protokolüyle her iki nokta arasında bir güvenlik ilişkisi oluşturulur. Bu güvenlik ilişkisi sayesinde yukarıda belirtilen hususlar konusunda karşılıklı olarak anlaşmaya varılır ve sonraki aşamalarda bu yöntemler kullanılır.
3. Diffie-Hellman metoduyla sonraki aşamalarda IPSec protokolünde kullanılacak olan anahtarlar oluşturulur ve güvenli bir şekilde katılımcılar arasında iletilir.
4. Bu aşamadan sonra IPSec protokolü IP başlıklarının şifrlenmesinden sorumludur. VoIP uygulanan her bir noktada IPSec Güvenlik Yönetim Veritabanı (SPD-Security Policy Database) tanımlanmaktadır. Bu veritabanında IPSec güvenlik uygulamasının gerçekleştirileceği VoIP cihazlarının IP adresleri ve istenirse kaynak ve hedef port numaraları ve protokol tipleri (UDP ya da TCP olarak) belirtilmektedir. VoIP cihazlarına gelen her bir paket analiz edilerek SPD veritabanında olup olmadığı kontrol edilir. Eğer gelen paket bu veritabanında eşlenirse, cihaz bu paket için tanımlanmış güvenlik ilişkisini uygulamaya sokar ve başlangıçta cihazların birbirlerini doğrulaması sağlanır. Sonrasında ise karşılıklı iki nokta arasında, üretilen anahtarlar ve şifreler vasıtasıyla bir tünel oluşturulur. Yani, gelen ve giden paketler şifrlenerek iletilir ve alınır.

5.1.7.3 Ulaşım Katmanı Güvenliği (TLS-Transport Layer Security)

TLS 1.0 (TLS versiyon 1.0) protokolü OSI referans modelinin 4. katmanında (ulaşım katmanı) şifreleme sağlayan RFC 2246 tarafından tanımlanan bir güvenlik protokolüdür (Şekil 5.18). TLS, web uygulamalarında güvenliği sağlamak için kullanılan Netscape'in SSL 3.0 (Secure Socket Layer version 3.0) protokolüne dayanılarak modellenmiştir (Dierks ve Allen, 1999). Bu nedenle TLS'e SSL 3.0 protokolünün geliştirilmiş bir hali denilebilir. Bu protokol bağlantı yönelimli (connection oriented) ve güvenilir (reliable) transmisyon

protokolü gerektirdiğinden dolayı UDP transmisyonu kullanan protokoller ile çalışmaz.

Bir VoIP ağında TLS protokolü istemci-sunucu uygulamalarında mesaj gizliliğini, katılımcıların doğrulanmasını ve mesaj bütünlüğünü sağlamaktadır. Her ne kadar genelde http güvenliği için kullanılsa da, TLS bağımsız bir protokoldür. Yani TLS, TCP gibi bağlantı yönelimli ve güvenilir transmisyon protokolü kullanan farklı uygulamalar için kullanılabilir.



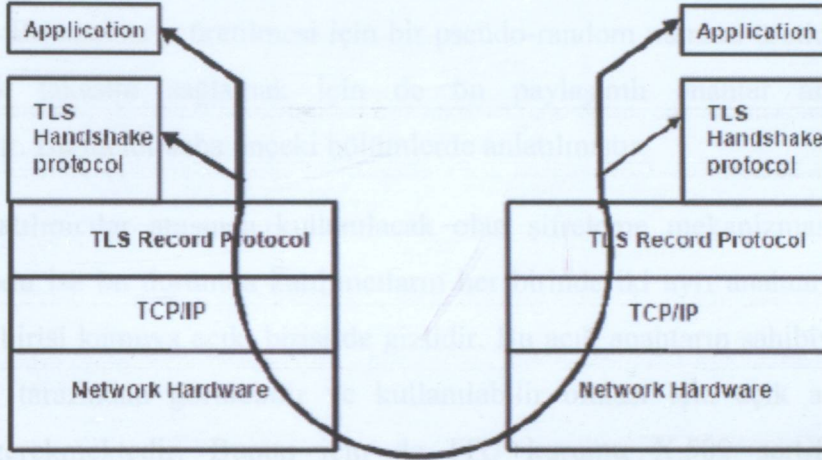
Şekil 5.18 TLS protokolü istemci/sunucu modeli (Dierks ve Allen, 1999)

TLS, güvenliği sağlama işini Kayıt Protokolü (Record Protocol) ve El-Sıkışma Protokolü (Handshake Protocol) olmak üzere iki katmanı sayesinde gerçekleştirmektedir (Şekil 5.19). El sıkışma protokolü katılımcıların doğruluğunu saptamak amacıyla güvenlik anlaşması (negotiation) sağlarken; kayıt protokolü gizlilik ve data bütünlüğünü sağlamaktadır. Şimdi bu protokollerin genel özelliklerine değinelim.

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. Data gönderiminden önce kullanılacak olan şifreleme algoritmaları ve şifrelemeyle ilgili anahtarlar konusunda katılımcıların anlaşmasını sağlamaktadır.

TLS protokolü el sıkışma protokolü sayesinde şifreleme öncesinde (ki bu kayıt protokolü ile olur) 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.



Şekil 5.19 TLS protokolü katmanları (Dierks ve Allen, 1999)

Kayıt Protokolü: Kayıt protokolünün iki temel görevi vardır.

1. Katılımcılar arasındaki datanın simetrik ya da asimetrik şifreleme metotları ile şifrlenerek 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, vb. gibi saldırılar engellenmektedir.

Şifreleme metotları sayesinde veriler şifrlenerek herhangi bir saldırganın araya girerek mesajları ele geçirmesi engellenir. Daha doğrusu 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. Gönderici datayı göndermeden önce özetleme fonksiyonu ile MAC bilgisini oluşturur (datanın bir özetini çıkarır) 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 pseudo-random numara üreticisi ve anahtarın güvenli olarak takasını sağlamak için de ön paylaşımli anahtar anlaşma metodu kullanılmaktadır. Bu metot daha önceki bölümlerde anlatılmıştır.

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. Bunun için de ITU kurumu X.509 sertifika standardını tanımlamıştır.

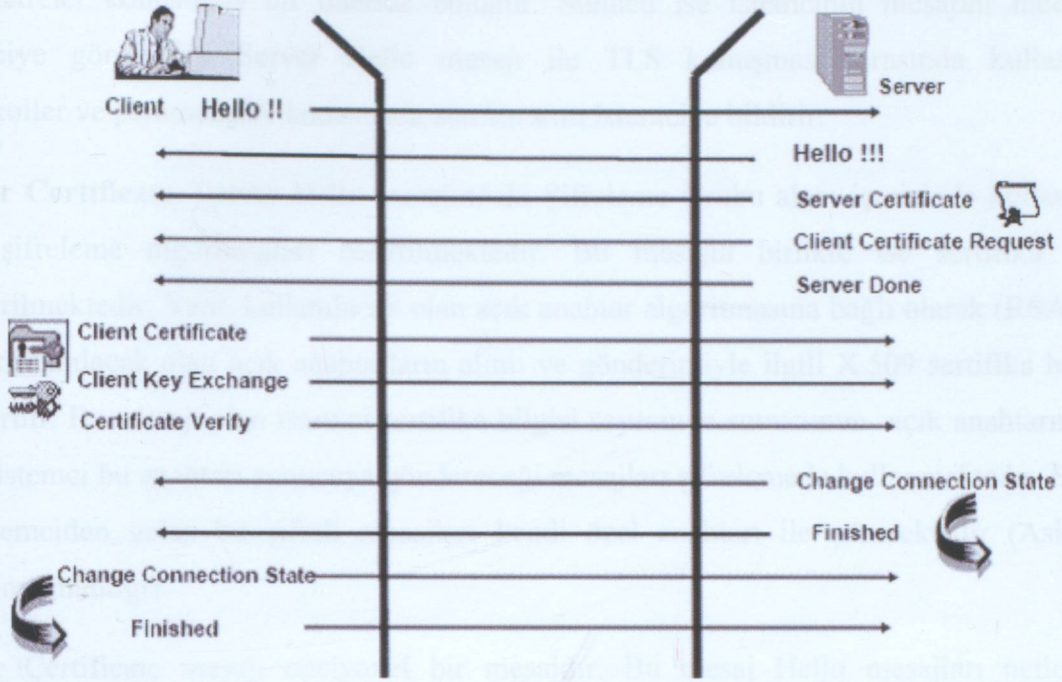
TLS protokolünde genel olarak kullanılan başlıca şifreleme metotları aşağıdaki gibidir.

Gizliliği (Confidentiality) sağlamak için kullanılabilen simetrik şifreleme metotları: IDEA, DES, 3DES, AES.

Gizliliği (Confidentiality) sağlamak için kullanılabilen asimetrik şifreleme metotları: RSA, Diffie Helman (DH).

Mesaj bütünlüğünü (Message integrity) sağlamak için kullanılabilen tek yönlü özetleme (karma) fonksiyonları: MD5, SHA-1.

TLS Mesajlaşma Yapısı: Katılımcılar güvenli bir TLS bağlantısı kurmak için karşılıklı olarak birbirlerine belirli mesajlar gönderip alırlar (Şekil 5.20). Bu mesajların gönderimi ve alımı bittikten sonra katılımcılar arasında güvenli bir oturum kurulur.



Şekil 5.20 TLS protokolü mesaj akış şeması (Dierks ve Allen, 1999)

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 servislerini 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. Sunucu da istemciden gelen bu şifreli mesajları kendi özel anahtarı ile çözmektedir (Asimetrik şifreleme mantığı).

Server Certificate mesajı opsiyonel bir mesajdır. Bu mesaj Hello mesajları neticesinde kullanılacak olan şifreleme metodu eğer asimetrik bir şifreleme metodu ise kullanılmaktadır. Aksi takdirde bu mesaj istemci ve sunucu arasında gidip gelmemektedir.

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 data 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.

5.2 Güvenlik Duvarı (Firewall) ve Ağ Adres Çevrimi (NAT-Network Address Translation) Uygulamaları

Herhangi bir ağda güvenliği sağlamak, idealde ağdaki her bir makinede (bilgisayarlar, sunucular ya da VoIP cihazları) gerekli tüm güvenlik önlemlerinin alınmasıyla sağlanır. Pratikte ise bu yapılamamaktadır. Ayrıca, kullanılan kimi protokollerin güvenlikten yoksun olduğu bilinse dahi kullanılmasına devam edilmektedir. Böyle durumlarda güvenlik duvarları, içeride az korumalı makinelerin olduğu bir ağla, dış dünya arasına yerleştirilerek aradaki fiziksel bağlantının güvenli bir şekilde oluşturulması sağlanır. Dolayısıyla içerideki ağa girmek isteyen her kötü niyetli dış saldırı, önce özel olarak korumalı tasarlanmış güvenlik duvarı makinesini bertaraf etmek zorundadır.

Günümüzde iç ağların hemen hepsi tahsisli olmayan IP numaraları (10.0.0.0, 192.168.0.0, vb. gibi) kullanılmaktadır. Bu IP numaraları internet üzerindeki yönlendiriciler (router) tarafından bilinmez. Dolayısıyla bu ağlardan internetteki herhangi bir makineye bir erişim olduğu zaman internetteki makine bu ağa nasıl geri döneceğini bilmez ve pratikte iletişim yapılamaz. Güvenlik duvarı ise, dinamik veya statik olarak internette bilinen ve kendisine yönlendirme yapılabilen bir IP numarasına sahiptir. İç ağdaki makinelere erişim sağlayabilmek için güvenlik duvarı, kendisine iç ağdan gelen her paketin kaynak adresini kendi adresi olarak değiştirir. Kendisine internetten gelen paketlerin de hedef adresini iç ağdaki ilgili makinenin adresi olarak değiştirir ve bu yolla iç ağdaki makinelerin internet üzerindeki makinelerle haberleşmesini sağlar. Bu işleme *Ağ Adres Çevrimi (NAT - Network Address Translation)* adı verilir.

NAT yapıldığı zaman, oluşan trafiğin internetten görüldüğü hali, internette bulunan tek bir makinenin (ki o da güvenlik duvarıdır) bazı internet alışverişleri yaptığıdır. İnternete, bu makinenin arkasındaki ağın büyüklüğü, bu ağdaki makinelerin cinsi, sayısı, ağın yapısı, vb.

hakkında herhangi bir bilgi gitmez. Dolayısıyla NAT, yalnızca tahsissiz ağlardan internete erişimi sağlamakla kalmaz, ağındaki makineler hakkında bilgi edinilmesini ve dolayısıyla size karşı yapılabilecek saldırıları zorlaştırır.

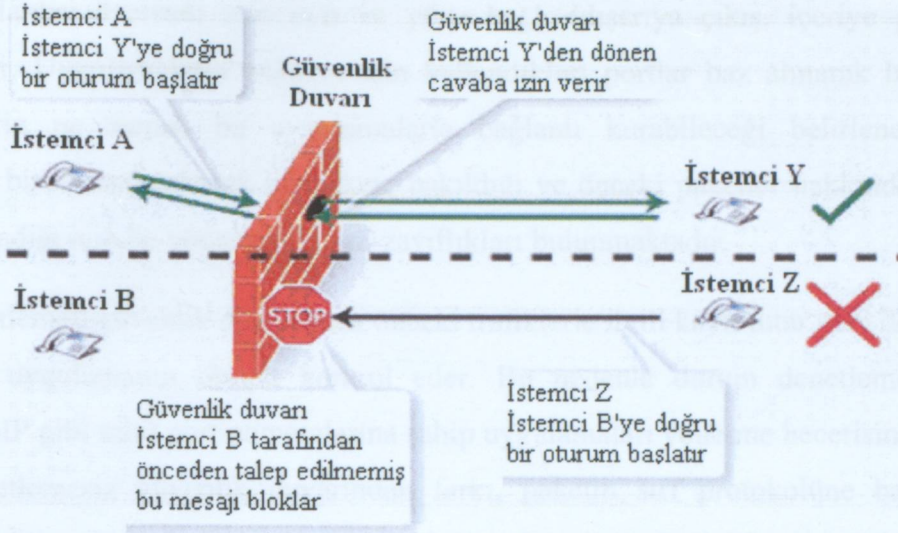
Standart bir ağ içerisindeki güvenlik duvarı ve NAT uygulamaları VoIP’te güvenliği sağlayan en önemli uygulamalardır. Bununla birlikte, bu uygulamalar bazı problemlere de yol açabilmektedir. Tüm VoIP protokolleri (SIP, H.323, vb.) güvenlik duvarları ve NAT ile ilgili benzer problemlere sahiptir. Her ne kadar IPv6’nın kullanılmaya başlanmasıyla birlikte bu problemlerin çözüleceğine inanılsa da VoIP sistemleri güvenlik duvarı ve NAT uygulamalarının sebep olduğu problemlerle her zaman uğraşmak zorunda kalacaktır.

Bu bölümde, VoIP güvenliği konusunda güvenlik duvarı/NAT uygulamalarının önemine ve bu uygulamaların avantajlarının yanında getirdikleri zorlukların neler olduğuna ve bu zorlukların nasıl aşılabileceğine değinilecektir.

5.2.1 Güvenlik Duvarı (Firewall)

Güvenlik duvarı, bir ağ sistemin özel bölümlerini halka açık bölümlerden ayıran, kullanıcıların ancak kendilerine tanınan haklar düzeyinde sistemden yararlanmasını sağlayan çözümlerdir. Güvenlik duvarı belirli bir makineyi denetlemek için o makine üzerine kurulabileceği gibi, bir bilgisayar ağını denetlemek için de kurulabilir. Ağ güvenlik duvarı, içeride bilgisayarlar ve sunucular gibi makinelerin olduğu bir kurum ağı ile dış ağ (internet) arasına yerleştirilir ve aradaki fiziksel bağlantı yalnızca güvenlik duvarı tarafından sağlanır (Şekil 5.21). Güvenlik duvarları salt dış saldırılara karşı sistemi korumakla kalmaz, performans artırıcı ve izin politikası uygulayıcı amaçlar için de kullanılırlar. Ağ güvenlik duvarı, yazılım veya donanımla yazılımın entegre olduğu çözümler şeklinde olabilir.

Güvenlik duvarları bugünün IP tabanlı ağlarında güvenliğin temelini oluşturmaktadır. Bir güvenlik duvarı, IP ağına yapılan saldırılara karşı bir savunma sistemidir. Güvenlik duvarları, kötü niyetli saldırıları içeren data trafiğini engellemektedir. Eğer gelen bir data trafiği güvenlik duvarının tanımlarına uymuyorsa engellenir. Güvenlik duvarı üzerindeki bu tanımlar ağ yöneticisi tarafından yapılmaktadır. “Dışarıdan gelen tüm FTP trafiğini engelle” ya da “Tüm http (port 80) trafiğine izin ver” gibi tanımlar bunlara örnek verilebilir. Tabi ki farklı güvenlik duvarları üzerinde farklı komplekslikte tanımlar yapılabilmektedir.



Şekil 5.21 Basit bir güvenlik duvarı uygulaması (Porter vd., 2006)

Bir güvenlik duvarının en faydalı özelliklerinden biri güvenlik kurallarının oluşturulmasıdır. Güvenlik duvarları için bir ağdaki son kademedeki geçit tüneli denilebilir. Çünkü, hiçbir data trafiği güvenlik duvarını geçmeden lokal ağa (LAN) giremez ve lokal ağdan çıkamaz. Bu güvenlik kuralları sayesinde güvenlik duvarları VoIP uygulamalarının güvenlik yönetimini kolaylaştırmaktadır. Ancak güvenlik duvarları VoIP uygulamalarında port yönetimi, çağrı kurulum prosedürleri gibi konularda problemlere yol açabilmektedir. İleriki bölümlerde bu problemlerin neler olduğuna değinilecektir. Ayrıca modern ve gelişmiş ağ yapılarında güvenlik duvarlarının vazgeçilmez olması nedeniyle bu problemlere karşı çözüm önerilerinin neler olduğuna da değinilecektir.

Güvenlik Duvarı Modelleri: Genel olarak VoIP trafiği UDP portları üzerinden iletilmektedir. Güvenlik duvarları bu tip paketleri paket filtreleme adı verilen bir teknikle işlemektedir. Paket filtreleme yöntemi sayesinde güvenlik duvarından geçmeye çalışan her bir paketin başlık bilgisine, IP adreslerine, port numaralarına ve protokol tiplerine (TCP, UDP) bakılarak paketin yasal bir paket olup olmadığı belirlenir. İki tip paket filtrelemeli güvenlik duvarı bulunmaktadır. Bunlardan biri Durum Denetlemesiz Güvenlik Duvarı (Stateless Firewall) iken diğeri Durum Denetlemeli Güvenlik Duvarıdır (Stateful Firewall).

Durum denetlemesiz güvenlik duvarı, en basit güvenlik duvarıdır. Herhangi bir oturum içerisinde önceden oluşan data trafiğiyle ilgili herhangi bir kayıt tutmamaktadır. Bu yöntemle güvenlik duvarından geçen her üçüncü seviye (IP, IPX, vb.) paketine bakılır ve ancak belli şartlara uyarsa bu paketin geçişine izin verilir. Paket filtreleme, güvenlik duvarının her

fiziksel bağlantısı üzerinde ayrı ayrı ve yöne bağlı (dışarıya çıkış, içeriye giriş) olarak uygulanabilir. Uygulamaların bağlantı için kullandıkları portlar baz alınarak hangi ağların veya kişilerin ne zaman bu uygulamalarla bağlantı kurabileceği belirlenebilir. Paket filtrelemede birim zamanda tek bir pakete bakıldığı ve önceki paketler hakkında bir bilgiye sahip olunmadığı için bu yöntemin çeşitli zayıflıkları bulunmaktadır.

Durum denetlemeli güvenlik duvarı hem önceki trafiklerle ilgili kayıt tutar hem de data paketi içerisindeki uygulamanın türünü kontrol eder. Bu nedenle durum denetlemeli güvenlik duvarları VoIP gibi sabit port numaralarına sahip uygulamaları yönetme becerisine sahiptirler. Durum denetlemesiz güvenlik duvarından farkı, paketin sırf protokolüne bakarak karar verilmesi yerine, güvenlik duvarının bir bağlantıyı hangi tarafın başlattığını takip etmesi ve çift yönlü paket geçişlerine buna göre karar vermesidir. Her bağlantının durum bilgisi tablolarda tutulduğu için durum denetlemesiz güvenlik duvarındaki zayıflıklar bu güvenlik duvarında bulunmamaktadır. Dezavantajı ise çok daha fazla işlemci gücüne ve belleğe ihtiyaç duymasıdır. Özellikle bağlantı sayısı arttıkça işlem ihtiyacı da artacaktır. VoIP uygulamalarında durum denetlemesiz güvenlik duvarı yerine durum denetlemeli güvenlik duvarı tercih edilmelidir.

VoIP'te Güvenlik Duvarı İhtiyacı: Standart güvenlik duvarı uygulamalarının yanında, güvenlik duvarları çoğu kez VoIP ağları içerisinde konumlandırılmaktadır ve data ve ses paketlerinin akış kontrolünden sorumlu olmaktadır. Bu durum mevcut ağ içerisinde VoIP tabanlı cihazlar içeren bir yapı için çok büyük bir öneme sahiptir. Bu tip cihazlardan çıkan ya da bu tip cihazlara gelen tüm ses trafiğini oluşturan RTP protokolünün dinamik UDP portlarını kullanmasından dolayı yüzlerce UDP portunun ağ içerisinde açık tutulması önemli derecede güvenlik açığına sebep olacaktır. Bundan dolayıdır ki bu tip VoIP tabanlı cihazlar bir durum denetlemeli güvenlik duvarının arka tarafında konumlandırılmalıdır ki güvenlik duvarı VoIP trafiğini kontrol edebilsin. Bu tip bir mekanizmanın olmadığı durumda herhangi bir UDP DoS saldırısı bu açık portların fazla olmasından yararlanarak ağı tehlikeye sokabilmektedir. Bu mekanizma ses ve data trafiği arasında bir bariyer oluşturarak ağı mantıksal (logical) bölümlere ayırmaktadır.

VoIP ve data trafiklerini ayırmak için güvenlik duvarları üzerinde fiziksel olarak da bölümler oluşturulabilmektedir. Yani, VoIP uygulaması için bir ağ ve data trafiği için başka bir ağ oluşturulmaktadır. Ancak bu konfigürasyon hem maliyet açısından hem de uygulama açısından çok kullanışlı değildir. Bu nedenle ses ve data için aynı fiziksel ağın kullanıldığı yapılar her zaman en verimli yapılardır.

5.2.2 Ağ Adres Çevrimi (NAT-Network Address Translation)

NAT, ağ içerisinde lokalde bulunan IP adreslerinin gizlenmesine ve aynı LAN içerisinde bulunan birden fazla cihazın aynı dış IP adresini paylaşmasına imkan sağlamaktadır. NAT sayesinde çıkan bir paketin IP başlığındaki lokal IP adresi yönlendiricinin global IP adresi ile değiştirilmektedir. NAT aynı zamanda bir paketin IP adreslerinin yanı sıra TCP/UDP port numaralarının da değiştirilmesine ve istenilen IP adreslerine ve portlara yönlendirilmesine imkan sağlamaktadır. NAT sayesinde lokalde bulunan birden fazla cihaz yönlendiricinin global dış IP adresini eşzamanlı olarak kullanabilmektedir. Bununla birlikte lokaldeki bu cihazlar internete çıkmadıkları durumda LAN içerisinde kendi lokal IP adreslerini kullanmaktadırlar. Sınırlı sayıda bulunan IP adreslerinin lokalde kullanılması gerekmediğinden bu durum önemli ölçüde fayda ve işlevsellik sağlamaktadır.

NAT aynı zamanda internet üzerinden lokal IP adreslerine erişimi kısıtlaması dolayısıyla bir LAN ağı için dolaylı olarak güvenliğe yardımcı olmaktadır. LAN'ın internetten soyutlanmasının yanı sıra NAT ağ yönetimini de kolaylaştırmaktadır. Örneğin bir firmanın internet servis sağlayıcısının değiştirdiğini düşünelim. Bu durumda sadece çıkış IP adresi konfigürasyonunun değiştirilmesi yeterli olacaktır. Lokal ağın adresleme yapısı ile ilgili herhangi bir değişiklik yapmak gerekmemektedir.

Farklı komplekslikte farklı NAT uygulamaları bulunmaktadır. Şimdi bu uygulamaların neler olduğuna değinelim.

Sınırsız NAT (Full cone NAT): Bu tip bir NAT uygulaması ile belirli lokal IP adresinden ve belirli porttan gelen istekler belirli dış IP adresine ve porta yönlendirilmektedir. Bununla birlikte, belirli bir dış IP ve porttan (external host) gelen istekler belirli iç IP adreslerine ve portlara yönlendirilmektedir.

IP Sınırlı NAT (Restricted Cone NAT): Bu tip bir NAT uygulamasında da belirli lokal IP adresinden ve porttan gelen istekler belirli dış IP adresine ve porta yönlendirilmektedir. Ancak, belirli bir dış IP adresinden gelen istekler belirli bir iç IP adresine ancak ve ancak öncesinde o iç IP'den o dış IP'ye doğru herhangi bir paket gönderildiyse iletilirler.

Port Sınırlı NAT (Port Restricted Cone NAT): IP sınırlı NAT uygulamasına benzemektedir. Ancak bu uygulamada kısıtlama port bazında yapılmaktadır. Belirli bir dış IP adresinden ve portundan gelen bir istek lokaldeki belirli bir IP adresine ve portuna ancak ve ancak öncesinde o iç IP'den o dış IP'ye doğru o portla bir paket gönderildiyse iletilir.

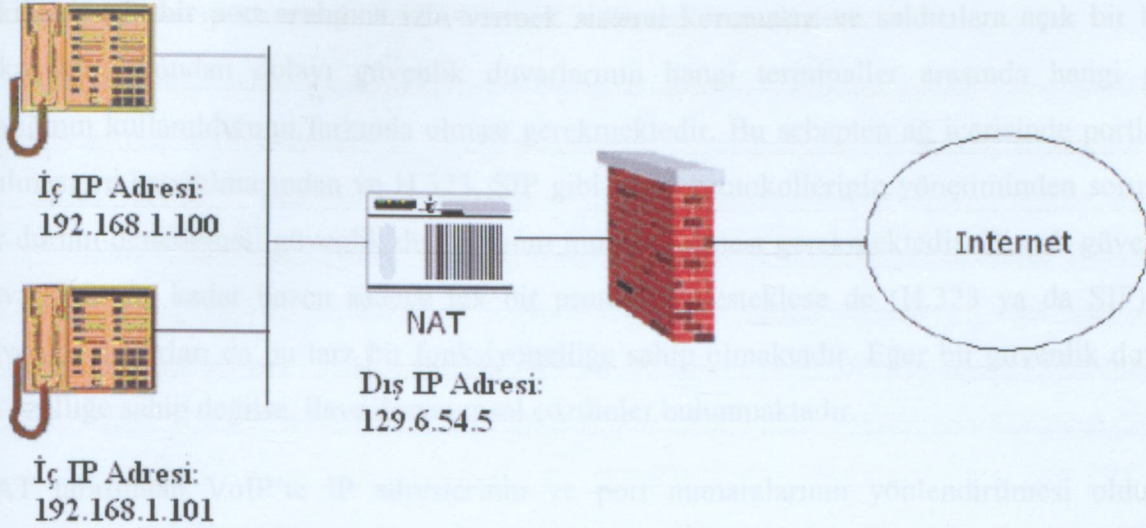
Simetrik NAT (Symmetric NAT): Belirli lokal IP adresinden ve belirli porttan gelen tüm istekler belirli dış IP adresine ve porta yönlendirilmektedir. Eğer belirli lokal IP adresinden ve belirli porttan gelen bir paket hedef olarak farklı bir dış IP adresini içeriyorsa, farklı bir yönlendirme (eşleme) metodu kullanılır. Bununla birlikte, sadece o lokal IP adresinden herhangi bir paket alan dış IP adresi o lokal IP'ye geri paket gönderebilir.

5.2.3 Güvenlik Duvarı/NAT ve VoIP Problemleri

Güvenlik duvarları ve NAT ile ilgili VoIP problemleri kullanılan VoIP protokolüne bağlı olmamaktadır. Bu tip güvenlik duvarı/NAT uygulamaları NAT arkasında bulunan bir terminalin kendisine gelen bir çağrıyı almasını zorlaştırmaktadır. Bu uygulamalar bununla birlikte hem ses kalitesini hem de RTP akışını olumsuz yönde etkilemektedir. Şimdi bu protokol-bağımsız problemlerin neler olduğuna değinelim.

Gelen Çağrılar: Kullanılan VoIP protokolüne bakmaksızın güvenlik duvarları ve NAT bir çağrı kurulumu için problemlere sebep olabilmektedir. Çağrı kurulumunda kullanılan sinyalleşme trafiğine güvenlik duvarında izin verilmesi birçok portun açılması anlamına geldiğinden dolayı bu durum saldırılara açık kapı bırakmak anlamına gelmektedir. Bu nedenle güvenlik duvarında gerekli konfigürasyonlar yapılırken tecrübeli bir yöneticinin dikkatli kural tanımları yapması gerekmektedir. Bir VoIP cihazının dış ağdan NAT'ın aktif olduğu yönlendiricinin arkasındaki (lokalindeki) bir noktaya bağlantı kurması gerektiğinde cihazın yönlendiricinin dış IP adresini ve port numarasını bilmesi gerekmektedir. Bu durum dışarıdaki arayan kişinin lokaldeki IP adresine ulaşmasını imkansız kılabilir. Hatta, NAT tarafından atanan dinamik portlar nedeniyle arayan taraftan gelen çağrı talebine ait portlar değişeceğinden bu durum tamamen imkansızlaşır. Bu nedenle NAT arkasındaki bir VoIP cihazı VoIP çağrısı alamazken sadece VoIP çağrısı yapabilecektir.

Bununla birlikte, birden fazla IP telefonun aynı hat üzerinde bulunduğu bir ağda NAT aktif edilirse bu durum bazı problemlere yol açabilmektedir (Şekil 5.22). Kavramsal olarak bu problemlerin en kolay çözümü NAT'ı tamamen iptal etmektir. Ancak NAT uygulamasının faydaları düşünüldüğünde IPv6 yapısı uygulanmaya başlandığında herkes için yeterli sayıda IP adresinin mümkün olduğu zaman bile NAT'a ihtiyaç olacaktır. Her ne kadar birçok senaryo üretilse de NAT her zaman en kolay, en ucuz ve en güvenilir çözüm olmaya devam edecektir.



Şekil 5.22 Güvenlik duvarı ve NAT arkasında bulunan IP telefonlar (Kuhn ve Thomas, 2005)

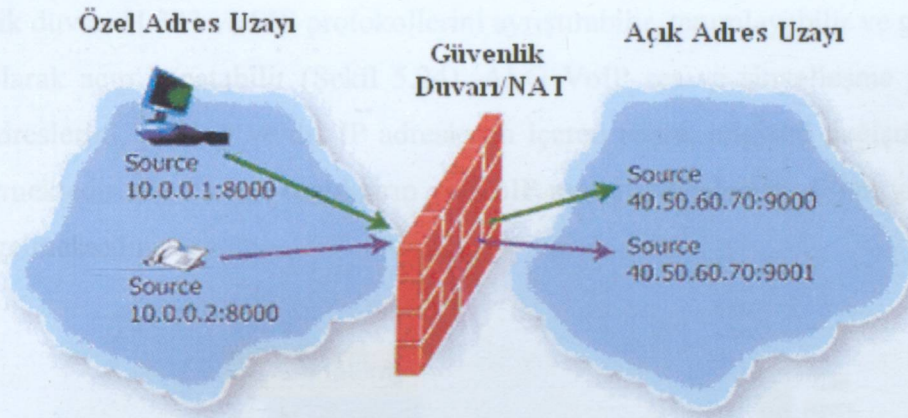
QoS Üzerine Etkiler: Güvenlik duvarları ve NAT uygulamaları gecikmeye ve jitter'a sebep olduğundan VoIP uygulamalarında ses kalitesini önemli derecede olumsuz etkileyebilmektedir. NAT aynı zamanda tüm trafiğin tek bir noktaya yönlendirilmesinden dolayı ağ üzerinde bir darboğaza sebep olmaktadır.

VoIP gecikmeye karşı çok hassas bir uygulamadır. Bu nedenle bir güvenlik duvarının gerekli yönlendirmeleri ve filtrelemeleri yaparken ses trafiğini olumsuz etkilememesi gerekmektedir. Söz konusu durum güvenlik duvarının ağ trafiğini ne ölçüde etkilediği ve işlemcisinin VoIP paketlerini hangi hızda tanıyıp yönlendirebildiğiyle ilgilidir. VoIP uygulamalarının Güvenlik duvarı işlemcisini yavaşlatmasının ya da zorlamasının sebebi güvenlik duvarları VoIP uygulamasında kullanılan protokolün (H.323, SIP, vb.) ne olduğuna bakmaksızın gelen ve giden tüm paketler için mutlaka geçerlilik filtrelemesi yapacaktır. Yani, tüm paketlerin yasal olup olmadığını kontrol edeceklerdir. Bu durum VoIP paketlerinin kuyrukta beklemesine ve dolayısıyla da ses kalitesinin bozulmasına sebep olacaktır. VoIP çağrı sayısının yüksek olduğu düşünülürse bu etkinin çok daha şiddetli olacağı aşîkardır. Bununla birlikte, güvenlik duvarındaki NAT uygulamasının gelen ve giden her paket için ayrı ayrı yönlendirme/eşleme yapması güvenlik duvarı işlemcisinin yükünü oldukça arttıracaktır. Tüm bu etkiler neticesinde de VoIP ses kalitesi hissedilir derecede olumsuz olarak etkilenecektir.

VoIP protokollerinin kullandığı portlar nedeniyle yaşanan sıkıntılar: VoIP'te sesi oluşturan RTP trafiği için 1024-65534 UDP port aralığından değişken portlar atanmaktadır. Bununla birlikte RTCP kontrol protokolü için de rasgele portlar atanmaktadır (RTCP için RTP protokolüne atanan UDP portunun bir fazlası yani ardışığı atanmaktadır). VoIP trafiği için bu

şekilde geniş bir port aralığına izin vermek sistemi korumasız ve saldırılara açık bir hale sokacaktır. Bundan dolayı güvenlik duvarlarının hangi terminaller arasında hangi port aralığının kullanıldığının farkında olması gerekmektedir. Bu sebepten ağ içerisinde portların açılması ve kapatılmasından ve H.323, SIP gibi VoIP protokollerinin yönetiminden sorumlu bir durum denetlemeli güvenlik duvarlarının mutlaka olması gerekmektedir. Birçok güvenlik duvarı her ne kadar bazen sadece tek bir protokolü desteklese de (H.323 ya da SIP) bu güvenlik duvarları da bu tarz bir fonksiyonelliğe sahip olmaktadır. Eğer bir güvenlik duvarı bu özelliğe sahip değilse, ilave donanımsal çözümler bulunmaktadır.

NAT tarafından VoIP'te IP adreslerinin ve port numaralarının yönlendirilmesi oldukça problemlidir (Şekil 5.23). Eğer yönlendirici VoIP trafiğini düzgün bir şekilde yönlendiremezse VoIP çağrıları başarılı bir şekilde kurulamayacak ya da ses trafiğinde problemler yaşanacaktır. Bu problem eğer her iki terminal de NAT arkasındaysa daha da çok şiddetlenecektir.



Şekil 5.23 Basit bir NAT uygulaması (Porter vd., 2006)

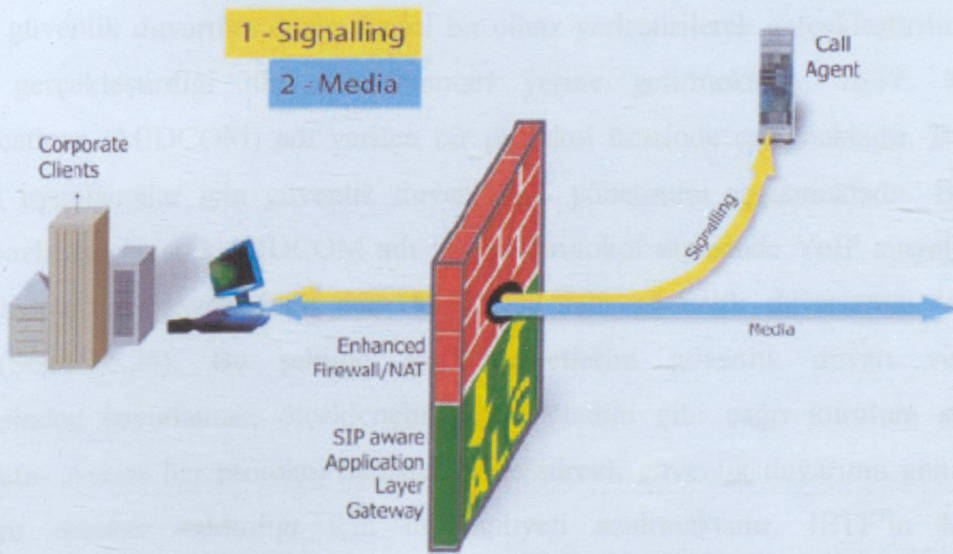
NAT'ın kullanımı VoIP sinyalleşmesinde başka bir muhtemel probleme sebep olabilmektedir. Bu problem şudur ki bir NAT uygulamasında bir dış IP adresinin lokaldeki bir IP adresine yönlendirilmesi güvenlik nedeniyle zamanın sadece belli bir periyoduyla sınırlı olmaktadır. Bu süre içerisinde bu IP adreslerini içeren herhangi bir trafik gözlenmezse ya da bağlantı bir şekilde kopmuşsa, bu yönlendirme tanımı otomatik olarak silinecektir. Bununla birlikte bir VoIP görüşmesi sırasında bu tanımlı süre boyunca bir sessizlik olursa bu durum da NAT tarafından bağlantının kopmasına sebep olabilmektedir. Bu nedenledir ki VoIP protokolleri tarafından görüşmenin devam ettiğini belirten bazı durum bilgileri kullanılmaktadır.

5.2.4 VoIP'te Güvenlik Duvarı/NAT Problemlerinin Çözüm Yöntemleri

VoIP kullanıcıları çağrı kurulum süreci içerisinde belirgin gecikmelere karşı çok toleranslı değildirler. Hele ki bu süre birkaç saniyenin üzerine çıktıysa bu durum kullanıcılar açısından can sıkıcı hale gelebilmektedir. VoIP'te çağrı kurulum süresini etkileyen birçok faktör bulunmaktadır. Bunlar arasında ağ topolojisi, terminallerin konumları, güvenlik duvarları, NAT, kimlik doğrulama ve diğer güvenlik prosedürleri bulunmaktadır. Ayrıca kullanılan VoIP protokollerine bağlı olarak da çağrı kurulum süresi değişebilmektedir. Şimdi VoIP'te güvenlik duvarı/NAT uygulamalarının sebep olduğu problemlerin çözüm yöntemlerine değinelim.

5.2.4.1 Uygulama Düzeyinde Ağ Geçitleri (ALG- Application Level Gateways)

Uygulama düzeyindeki ağ geçitleri (ALG) güvenlik duvarı/NAT problemleri için tipik ticari çözümlerdir. Bir ALG belirli uygulamalara dayanan, dinamik konfigürasyonlara izin veren ve güvenlik duvarı ya da NAT üzerinde gömülü olan bir yazılımdır. VoIP ALG yazılımı içeren bir güvenlik duvarı H.323 ve SIP protokollerini ayrıştırabilir, tanımlayabilir ve gerekli portları dinamik olarak açıp kapatabilir (Şekil 5.24). ALG VoIP ses ve sinyalleşme paketlerindeki lokal IP adreslerini, portları ve dış IP adreslerini içeren başlık bilgisini değiştirerek yeniden şekillendirmektedir. Bu durum başlıkların ve VoIP mesaj gövdelerinin (SDP gibi) değişmesi anlamına gelmektedir.



Şekil 5.24 Uygulama Düzeyinde Ağ Geçidi (ALG- Application Level Gateway)

ALG'nin lokal ağ adreslerini kendi adresleri ile değiştirmesi NAT problemini azaltmaktadır. ALG bu işlemi sadece IP adreslerini değiştirerek değil bununla birlikte RTP port trafiğini yönlendirerek de gerçekleştirmektedir. RTP ve RTCP için kullanılan ardışık port ihtiyacı burada bir probleme sebep olmaktadır. Çünkü ağ içerisindeki tüm VoIP ve data trafiği ALG'ye doğru yönlendirilmektedir, sonuç olarak da çağrı sayısı oldukça fazla olabilmektedir ve yeterli ardışık port bulabilmek bir problem oluşturabilmektedir. Bu nedenle güvenlik duvarlarının bu eksikliği çağrılarının ALG tarafından meşgul olarak reddedilmesine sebep olabilmektedir.

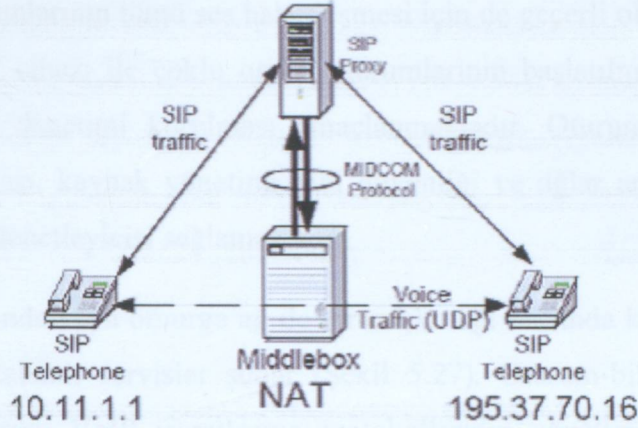
ALG'nin uygulanması beraberinde belirgin bir maliyet getirmektedir. Ayrıca VoIP paketlerinin yönetimi çağrı sayısının yüksek olduğu durumlarda sistem içerisinde gecikmelere ve jitter'a sebep olabilmektedir. Bu durum aynı zamanda ağ içerisinde data hızını yavaşlatmaktadır. ALG destekli bir güvenlik duvarının sürekli güncellenmesi ya da yenilenmesi gerekebildiğinden pahalı olabilmektedir. Tüm bu olumsuz yanlarına rağmen ALG uygulaması VoIP, güvenlik duvarı ve NAT birlikteliğini sağlamada en basit ve en güvenli yoldur.

5.2.4.2 Merkezi Cihaz (MiddleBox) Çözümleri

ALG'lerin olumsuz yanlarından biri bir güvenlik duvarına gömülü olmalarıdır ve bu nedenle de data yoğunluğunun fazla olduğu durumlarda ağ içerisinde gecikmeler, jitter ve düşük hız problemleri yaşanmaktadır. Merkezi cihaz çözümleri bu problemleri azaltmaktadır. Bu uygulama güvenlik duvarının dışına harici bir cihaz yerleştirilerek gerçekleştirilir. Bu cihaz ALG'nin gerçekleştirdiği tüm fonksiyonları yerine getirmektedir. IETF, MiddleBox Communications (MIDCOM) adı verilen bir protokol üzerinde çalışmaktadır. Bu protokol VoIP gibi uygulamalar için güvenlik duvarı/NAT yönetimini sağlamaktadır. Bu cihazlar protokol bazlı ayarlanarak MIDCOM adı verilen protokol sayesinde VoIP sinyalleşmesinin gerektirdiği portları gerektiğinde açıp kapatması için güvenlik duvarlarına talimatlarda bulunur (Şekil 5.25). Bu şekilde VoIP paketlerini güvenlik duvarı ve NAT'ın denetlemesinden soyutlamak, ölçeklenebilirliği sağladığı gibi çağrı kurulum süresini de azaltmaktadır. Ayrıca her protokol değişikliğinde sürekli güvenlik duvarının güncellenmesi gerekliliğini ortadan kaldırdığı için de maliyeti azaltmaktadır. IETF'in MiddleBox communication Grubu bu protokol üzerindeki çalışmalarına hala devam etmektedir.

Bu çözümünde bazı olumsuz yanları bulunmaktadır. Başlangıçta bu protokol-bilinçli çalışan cihaz tarafından kontrol edilebilmesi için güvenlik duvarının ayarlanması gerekmektedir. Bu

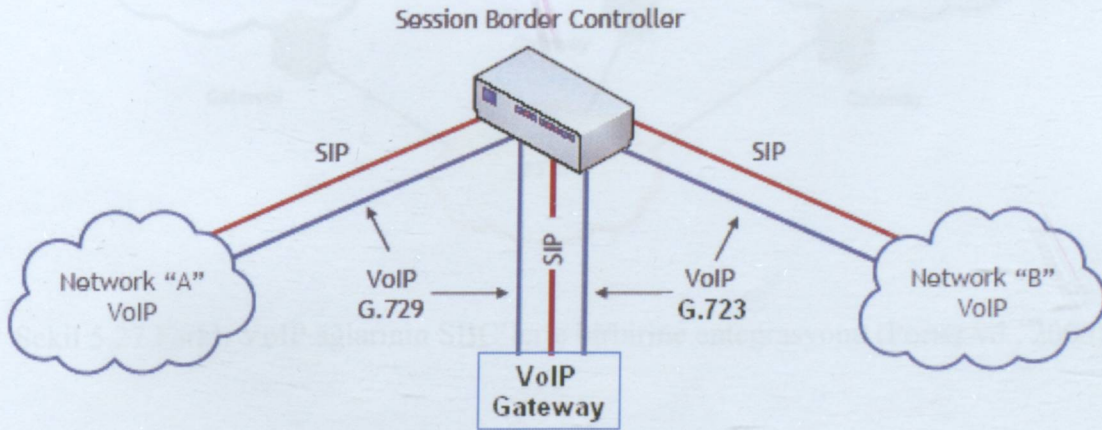
da bir başlangıç kurulum maliyeti getirmektedir. Ayrıca harici MiddleBox cihazının da saldırılara karşı korunması gerekmektedir.



Şekil 5.25 VoIP'te Merkezi cihaz senaryosu (Kuhn ve Thomas, 2005)

5.2.4.3 Oturum Sınır Denetleyicisi (SBC-Session Border Controllers)

SBC'ler tek başlarına güvenlik duvarı/NAT çözümü, çağrı kurulumu, çağrı yönetimi, doğrulama, gözlemleme ve protokol geçişleri (dönüşümleri) sağlayan geniş kapsamlı cihazlardır (Şekil 5.26).

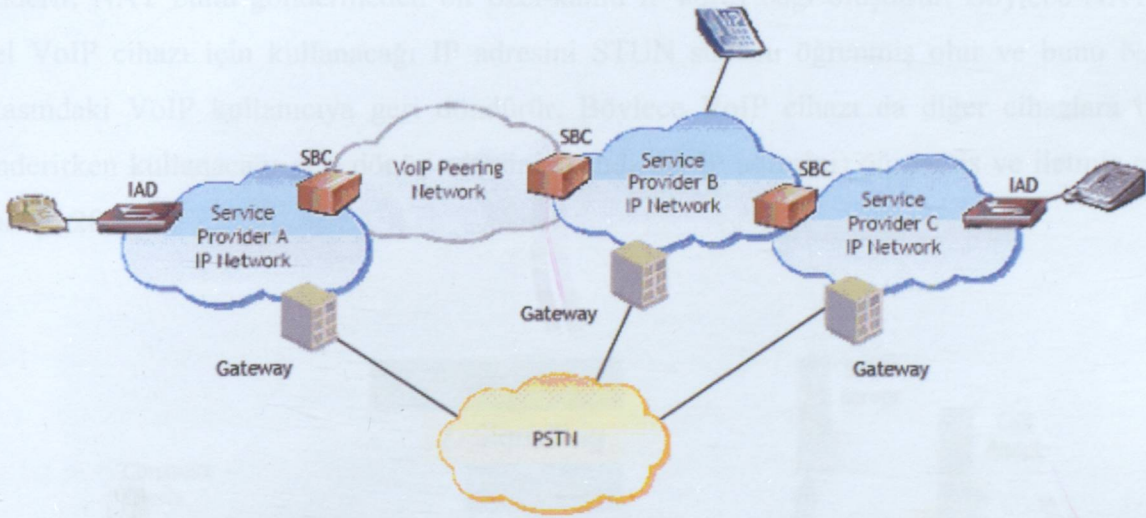


Şekil 5.26 Oturum Sınır Denetleyicisi (SBC-Session Border Controller)

SBC ihtiyacı VoIP servisinin birçok IP ağı üzerinden taşınması gerekliliğinden ortaya çıkmıştır. İnternet'in çeşitli ISS (İnternet Servis Sağlayıcısı) ve özel IP ağlarından oluşan yapısı üzerinden VoIP oturumlarını kurmak nasıl olabilir? Her şeyden önce bu ağlar birbirine güven duymamakta ve ağlarını (güvenlik duvarlarını) kullanıcıların VoIP çağrılarına

açmamaktadır. Burada internet ve PSTN arasındaki temel bir farkı görüyoruz. PSTN bir kapalı ağ olduğundan, kullanıcılar güvenli biçimde haberleşebilmektedirler. İstenmeyen bir telefon çağrısı veya yanlış numara aranması basitçe reddedilebilmektedir. VoIP ile IP ağındaki güvenlik sorunlarının tümü ses haberleşmesi için de geçerli olmaktadır. Ağ sınırında konumlandırılan SBC cihazı ile çoklu ortam oturumlarının başlatılması ve sonlandırılması üzerinde bir politika denetimi kurulması amaçlanmaktadır. Oturum politikası, güvenlik, protokol ortak çalışması, kaynak yönetimi gibi güvenliği ve ağlar arasında oturum temelli işlevleri oturum sınır denetleyicisi sağlamaktadır.

SBC, iki ISS ağı arasında veya omurga ağ ile bir erişim ağı arasında konutsal veya kurumsal kullanıcılara oturum-tabanlı servisler sunar (Şekil 5.27). Oturum-bilinçli SBC, ağın içsel kaynaklarının korunması, VoIP işaretleme protokollerinin yönetimi ve ağ kaynaklarının kullanımı gibi erişim denetim işlevlerini sağlayabilir. SBC, NAT veya güvenlik duvarı gibi diğer ara işlevleri tamamlayıcı bir rol oynamaktadır.



Şekil 5.27 Farklı VoIP ağlarının SBC'lerle birbirine entegrasyonu (Porter vd., 2006)

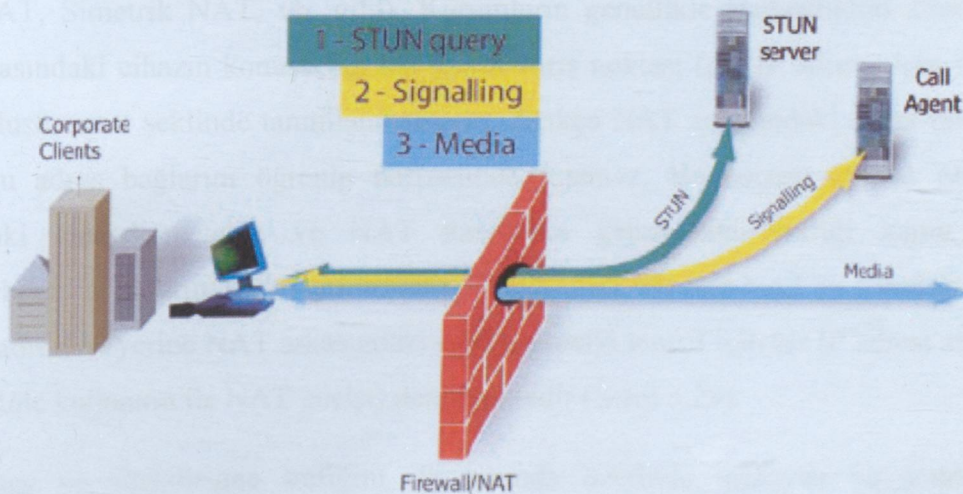
5.2.5 NAT Problemi Çözüm Yöntemleri

Lokal (özel) IP adreslerini kamu IP adreslerine çeviren NAT, özellikle H.323 ve SIP gibi gerçek zamanlı haberleşme protokolleri için büyük bir problemdir. Çünkü, VoIP mesajları cihaz IP adreslerini de içermektedir ve NAT arkasında olan özel bir VoIP cihazı şayet kamu internetteki bir VoIP cihazına bir oturum kurma isteği gönderirse, kendi IP adresini de bu iletide içermek zorundadır. Ancak burada kullanılacak IP adresini yalnız NAT bilmektedir.

VoIP cihazı NAT'da atanan bu kamu IP adresi hakkında hiçbir fikre sahip değildir. Hatta NAT'ın varlığından habersizdir. VoIP cihazı NAT arkasında olduğunu, NAT'ın kullandığı özel-kamu IP adres ilişkisini ve kendi uygulama ve protokol işlemlerinde bu kamu IP adresi kullanım ayarlarını öğrenip yapabilmelidir. Böyle durumlarda IP dünyasında 'sunucu' denen cihaz veya işlevler kurtarıcı olarak ortaya çıkar. Şimdi NAT problemi için çözüm sağlayan mekanizmalara değinelim.

5.2.5.1 UDP'nin NAT Üzerinden Basit Geçişi (STUN- Simple Traversal of UDP through NATs)

NAT sorununa bir çözüm STUN ile verilmiştir. STUN, VoIP uygulamaları için NAT tarafından atanmış kamu (dış) IP adresini elde etmek için kullanılan bir yöntemdir (Rosenberg ve Huitema, 2003). STUN aynı zaman da hangi tip NAT uygulamasının kullanıldığını belirtmek için de kullanılmaktadır. NAT arkasındaki VoIP cihazı üzerinde koştan STUN istemci (VoIP cihazı) NAT üzerinden geçecek olan bir sorguyu kamu STUN sunucusuna gönderir. NAT bunu göndermeden bir özel-kamu IP adres bağı oluşturur. Böylece NAT'ın özel VoIP cihazı için kullanacağı IP adresini STUN sunucu öğrenmiş olur ve bunu NAT arkasındaki VoIP kullanıcıya geri döndürür. Böylece VoIP cihazı da diğer cihazlara ileti gönderirken kullanacağı geri dönüş adresini (kendi dış IP adresini) öğrenmiş ve iletmış olur (Şekil 5.28).



Şekil 5.28 UDP'nin NAT Üzerinden Basit Geçişi (STUN) (Porter vd., 2006)

Bir STUN sunucusu, istemcilerin (mesela bir güvenlik duvarının arkasında kalan VoIP cihazı)

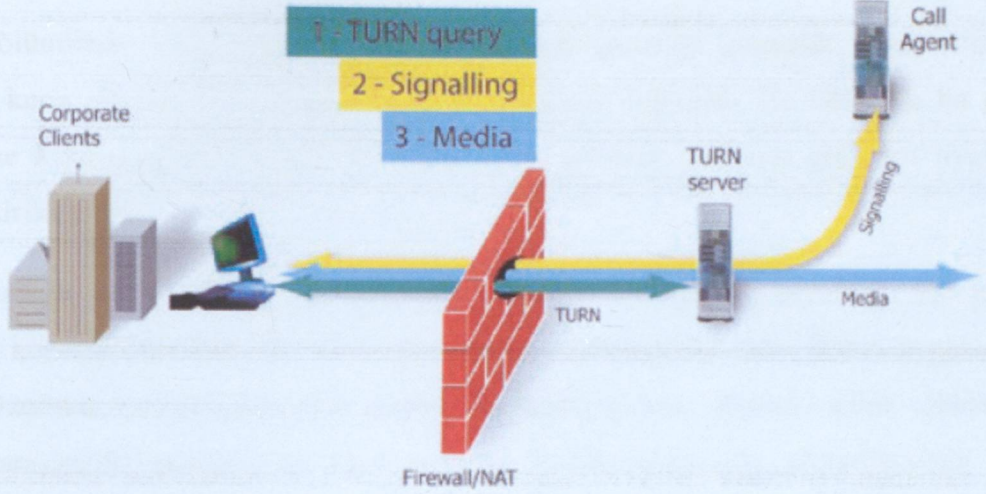
yerel ağ dışında yer alan bir VoIP hizmet sağlayıcısına VoIP araması yönlendirmesine imkan verir. STUN sunucusu, istemcilerin kendi IP adreslerini, arkasında bulundukları NAT'ın tipini ve NAT tarafından belli bir yerel port ile ilintilendirilen yan internet portunu bulmalarına imkân verir. Bu bilgi, istemci ve VoIP hizmet sağlayıcısı arasında UDP iletişimi kurulması ve böylece bir VoIP araması başlatılması için kullanılır. STUN sunucusuyla UDP 3478 portu üzerinden iletişim kurulmaktadır.

STUN protokolünün birkaç eksikliği bulunmaktadır. Bunlardan biri; STUN sadece UDP tabanlı VoIP uygulamalarda çalışırken TCP tabanlı uygulamalarında çalışmamaktadır. Bununla birlikte STUN protokolü sadece bazı NAT metotları ile çalışabilmektedir. STUN protokolü simetrik NAT uygulamasıyla düzgün çalışmamaktadır. Simetrik NAT güvenlik amaçlı port saldırılarını engellemek amaçlı aynı lokal IP adresi ve aynı porttan çıkan paketler eğer farklı dış IP adreslerine gidiyorsa her bir paket için farklı eşleme metotları kullanır. Yani, NAT çıkışında her bir paket için karşı tarafa farklı port ve farklı çıkış IP adresi iletir. Bu durumda STUN sunucusunun elde ettiği IP adresi ya da portu ile NAT'ın istemciye atadığı IP adresi ya da portu birbirinden farklı olabilmekte, bu da çağrı kurulum mesajlarının karşı taraftan geri dönüşte yanlış IP adreslerine ya da portlara gitmesine ve sonuç olarak ta çağrı kurulumlarının başarısız olmasına sebep olmaktadır.

5.2.5.2 Röle Kullanımı ile NAT Geçiş (TURN-Traversal Using Relay NAT)

Önceki bölümlerde anlatıldığı gibi farklı tiplerde NAT uygulamaları bulunmaktadır (Port sınırlı NAT, Simetrik NAT, vb. gibi). Kurumların genellikle kullandıkları simetrik NAT, NAT arkasındaki cihazın konuşacağı her kamu varış noktası (dış IP adresi) için farklı adres bağları oluşturması şeklinde tanımlanmaktadır. Açıkça NAT arkasındaki cihaz bu kadar çok özel-kamu adres bağlarını öğrenip hafızasında tutamaz. Bu soruna çözüm olarak NAT arkasındaki cihazdan gelen ve NAT üzerinden geçen tüm trafiği kamu internette adreslenebilen bir aktarım (röle) noktasına yönlendirelim. Bu röle NAT'ın yarattığı tüm çoklu kamu IP adresleri yerine NAT arkasındaki özel istemciyi temsil için bir IP adresi atasın. Buna TURN (Röle kullanımı ile NAT geçişi) denilmektedir (Şekil 5.29).

TURN, ses ve sinyalleşme trafiğini ilk adımda üzerinde toplayan ve sonrasında dış terminallere ileten bir TURN sunucusuna dayanan bir protokoldür. Bu sunucu ister müşteri tarafında isterse de herhangi bir servis sağlayıcı ağında bulunabilmektedir.



Şekil 5.29 Röle Kullanımı ile NAT Geçişi (TURN) (Porter vd., 2006)

NAT arkasında bulunan TURN destekli istemci (VoIP cihazı) bu TURN sunucusuna bir keşif mesajı gönderir. TURN sunucusu istemciye NAT tarafından kullanılan dış IP adresini ve portunu cevap olarak gönderir. İstemci sunucudan aldığı bu bilgileri VoIP çağrı kurulum mesajı içinde kullanır ve karşı taraftaki VoIP cihazı NAT arkasındaki cihaza tekrar cevap gönderirken bu mesaj içerisindeki bilgileri kullanır. Bu uygulamanın en büyük avantajı TURN sunucusu istemciye her zaman temsilen belli bir IP adresi ve portu atadığından ve TURN sunucu tarafından atanıp karşı tarafa iletilen bu IP adresi hiçbir zaman değişmeyeceği için bu uygulama simetrik NAT ile de problemsiz bir şekilde kullanılabilir.

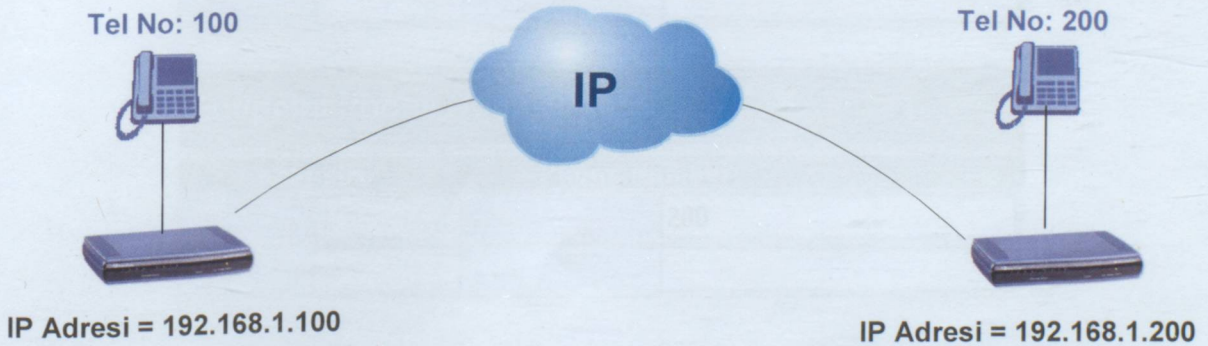
6. VoIP GÜVENLİK PROTOKOLLERİ İLE İLGİLİ UYGULAMALAR

Önceki bölümlerde VoIP teknolojisinin beraberinde getirdiği güvenlik tehditlerine ve bu tehditlere karşı alınabilecek önlemlerin neler olduğuna değinildi. Bu bölümde bu güvenlik tehditlerine karşı uygulanabilecek güvenlik protokollerinin önemini gösteren uygulamalar gerçekleştirilecektir.

İlk uygulamada bir yerel alan ağı içerisinde bulunan iki VoIP ağ geçidinin SIP protokolü üzerinden konuştukları basit bir VoIP senaryosu gerçekleştirilecektir. İkinci uygulamada ağ geçitleri üzerinde herhangi bir VoIP protokolü aktif değilken, ortadaki adam saldırısı ile ağ geçitleri arasındaki görüşmenin nasıl kolayca kaydedilebileceği gösterilecektir. Üçüncü uygulamada ağ geçitleri üzerinde Güvenli Gerçek Zamanlı Taşıma Protokolü (SRTP-Secure Real-Time Transport Protocol) aktif edilerek, ikinci uygulamada gerçekleştirilen gizli dinleme saldırısının nasıl başarısız olacağı gösterilecektir. Dördüncü ve son uygulamada ise kayıt sahteciliği, proxy taklit etme, mesaj değiştirme, izinsiz erişim, vb. gibi VoIP teknolojisinin diğer güvenlik tehditlerine karşı uygulanabilecek en önemli güvenlik protokollerinden biri olan İnternet Protokolü Güvenliği (IPSec) ile ilgili bir uygulama gerçekleştirilecektir. Bu uygulama sonunda yasal kullanıcılar arasında karşılıklı olarak IPSec protokolünün aktif edilmesi durumunda bahsedilen saldırıların gerçekleştirilmesinin mümkün olmadığı görülecektir.

6.1 Uygulama 1: Ağ Geçitleri Kullanılarak Gerçekleştirilen Basit Bir VoIP Senaryosu

Bu uygulamada SIP protokolü konuşan iki VoIP ağ geçidi ile basit bir VoIP görüşmesi gerçekleştirilecektir (Şekil 6.1).



Şekil 6.1 SIP protokolü konuşan iki ağ geçidinden oluşan basit bir VoIP senaryosu

Ağ geçitlerinin konfigürasyonu:

Ağ geçitlerinde yapılması gereken birkaç önemli konfigürasyon bulunmaktadır. Bunlar:

- Her iki ağ geçidi de aynı VoIP protokolünü konuşuyor olmalıdırlar (SIP ya da H.323). Bu uygulamada ağ geçitleri SIP protokolü üzerinden haberleşecekler.
- Ağ geçitlerinin IP konfigürasyonu yapılmalıdır. Bu uygulamada ilk ağ geçidine 192.168.1.100 IP adresi verilirken; ikincisine 192.168.1.200 IP adresi verilmiştir.
- Her iki ağ geçidinde de aynı kodlayıcı (codec) türü aktif edilmelidir. Seçilebilecek kodlayıcı türleri arasında G.711, G.729, G.723, vb. kodlayıcılar bulunmaktadır. Bu uygulamada G.711 kodlayıcısı aktif edilmiştir.
- Ağ geçitlerinin telefon numaralarının belirlenmesi gerekmektedir. Bu uygulamada ilk ağ geçidine telefon numarası olarak 100 verilirken; ikinci ağ geçide 200 numarası verilmiştir (Şekil 6.2).
- Ağ geçitlerinin çağrıları birbirlerine yönlendirebilmeleri için her bir ağ geçidinde diğerinin IP adres bilgisinin tanımlanması gerekmektedir. Yani, ilk ağ geçidinde “200 tuşlandığında çağrıyı ikinci ağ geçidinin IP adresine (192.168.1.200) gönder”; ikinci ağ geçidinde ise “100 tuşlandığında çağrıyı ilk ağ geçidinin IP adresine (192.168.1.100) gönder” şeklinde tanımlar girilmelidir (Şekil 6.3).

Endpoint Phone Number Table			
	Channel(s)	Phone Number	
1	1	100	
2			

Endpoint Phone Number Table			
	Channel(s)	Phone Number	
1	1	200	
2			

Şekil 6.2 Ağ geçitlerinin telefon numaralarının belirlenmesi

Tel to IP Routing		
Routing Index		1-10 ▾
Tel to IP Routing Mode		Route calls before manipulation ▾
Dest. Phone Prefix	Source Phone Prefix	Dest. IP Address
1 200	*	192.168.1.200
2		
3		
4		

Şekil 6.3 Ağ geçitlerinin adres tablolarının belirlenmesi

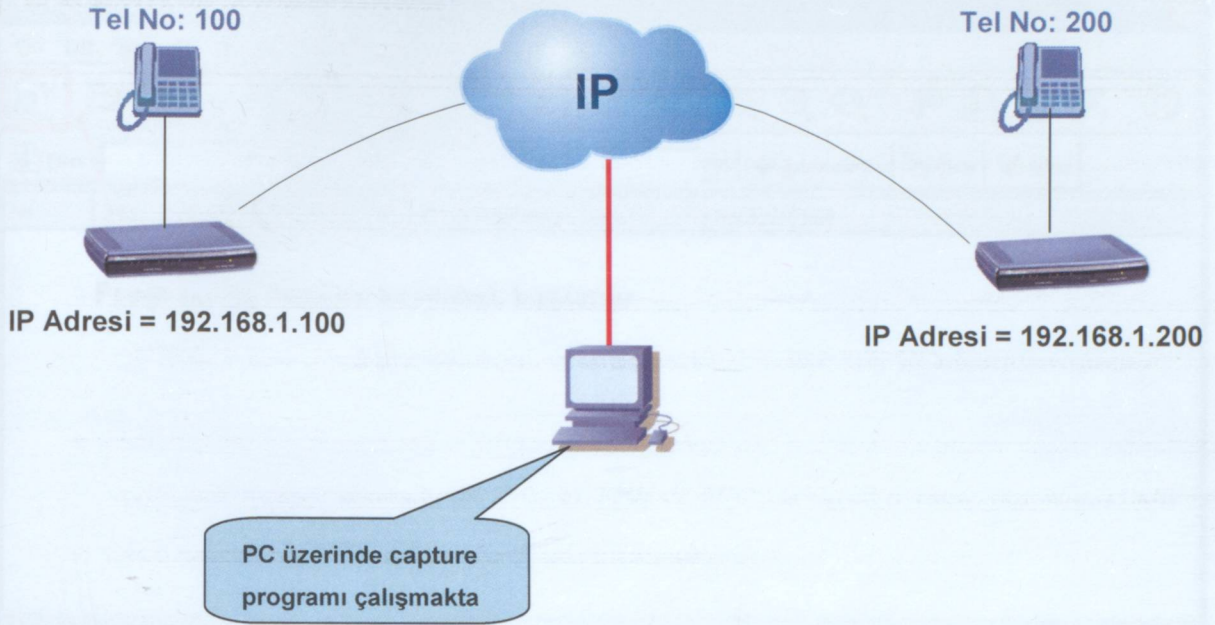
Her iki ağ geçidinde de bahsedilen konfigürasyonlar eksiksiz tamamlandığında ağ geçitleri artık birbirleri ile haberleşmeye hazırdır. İlk ağ geçidine bağlı telefonun ahizesi kaldırılıp 200 numarası tuşlandığında IP protokolü üzerinden çağrı ikinci ağ geçidine ulaşır ve ikinci ağ geçidine bağlı telefon çalar. Tüm bu çağrı kurulumu, ses paketlerinin iletimi ve çağrı sonlandırılması işlemlerinin tamamı SIP protokolü aracılığı ile gerçekleştirilmektedir.

6.2 Uygulama 2: Ortadaki Adam Saldırısı ile VoIP Görüşmelerinin Gizli Dinlenmesi

Bu uygulamada gizli dinleme saldırısı birebir gerçekleştirilecektir. İlk uygulamadaki senaryo kullanılarak yasal olmayan üçüncü bir kişinin (saldırganın) araya girip, yasal kullanıcıların konuşmalarını içeren ses paketlerini basit bir program aracılığı ile ele geçirip, ardından bu ses paketlerini yine aynı program aracılığı ile wav formatına çevirip normal dinlenebilir ses dosyası haline getirmesi gösterilecektir (Şekil 6.4).

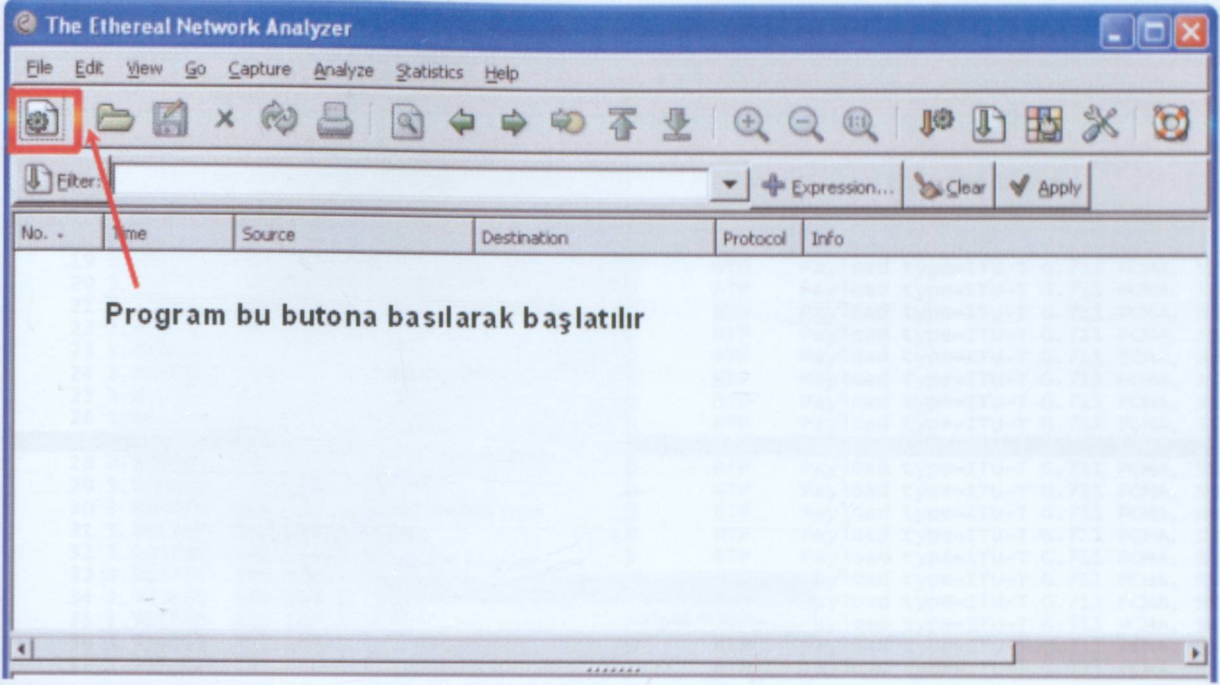
Uygulama Adımları:

1. Ağ geçitleri arasında telefon görüşmesi başlamadan önce saldırı bilgisayarındaki veri yakalama programını çalıştırır. Bu uygulamada veri yakalama programı olarak Ethereal adlı program kullanılmıştır (Şekil 6.5).
2. Program çalışır durumdayken, yani program ağda gelen giden tüm paketleri kaydediyorken, ağ geçitleri arasında bir telefon görüşmesi gerçekleşir.

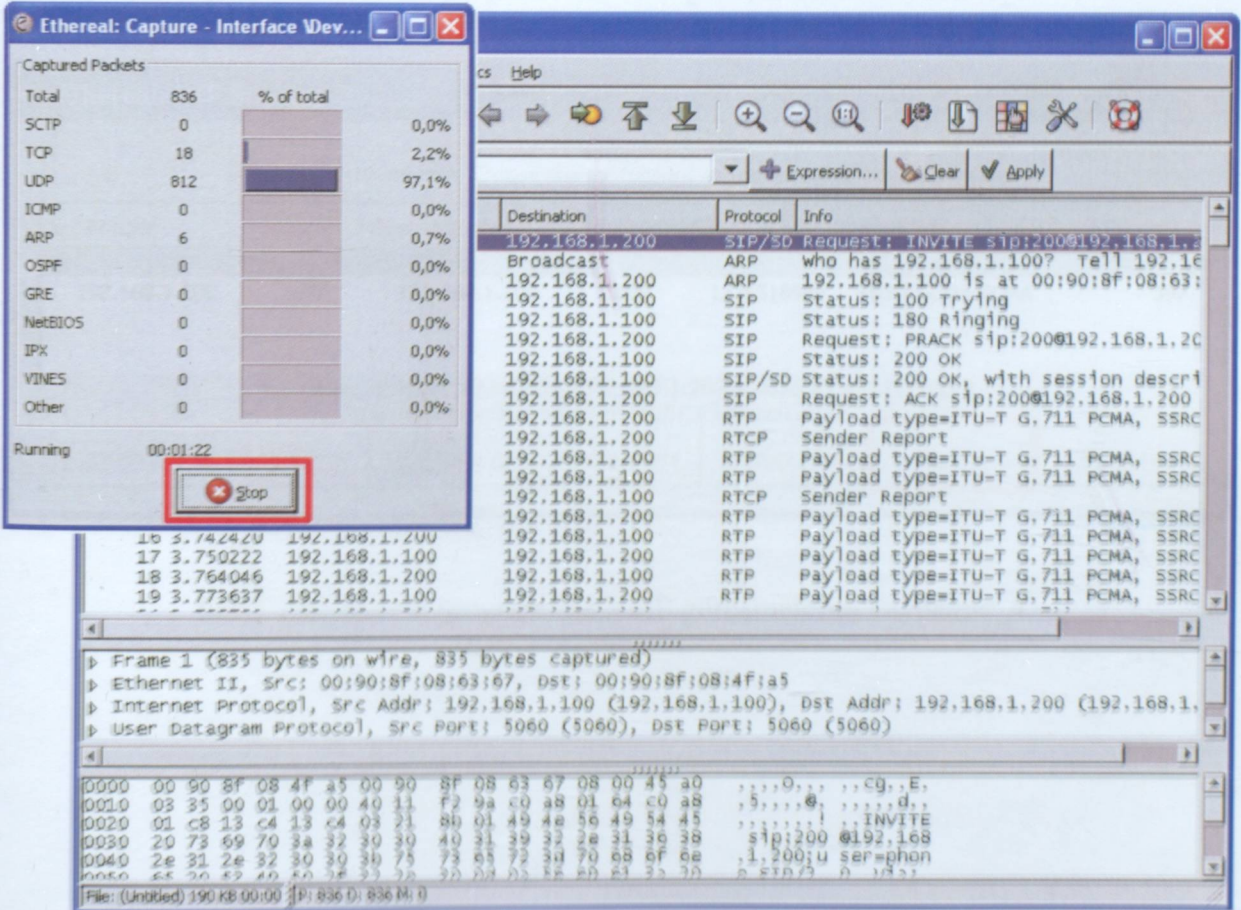


Şekil 6.4 Ortadaki adam saldırısı senaryosu

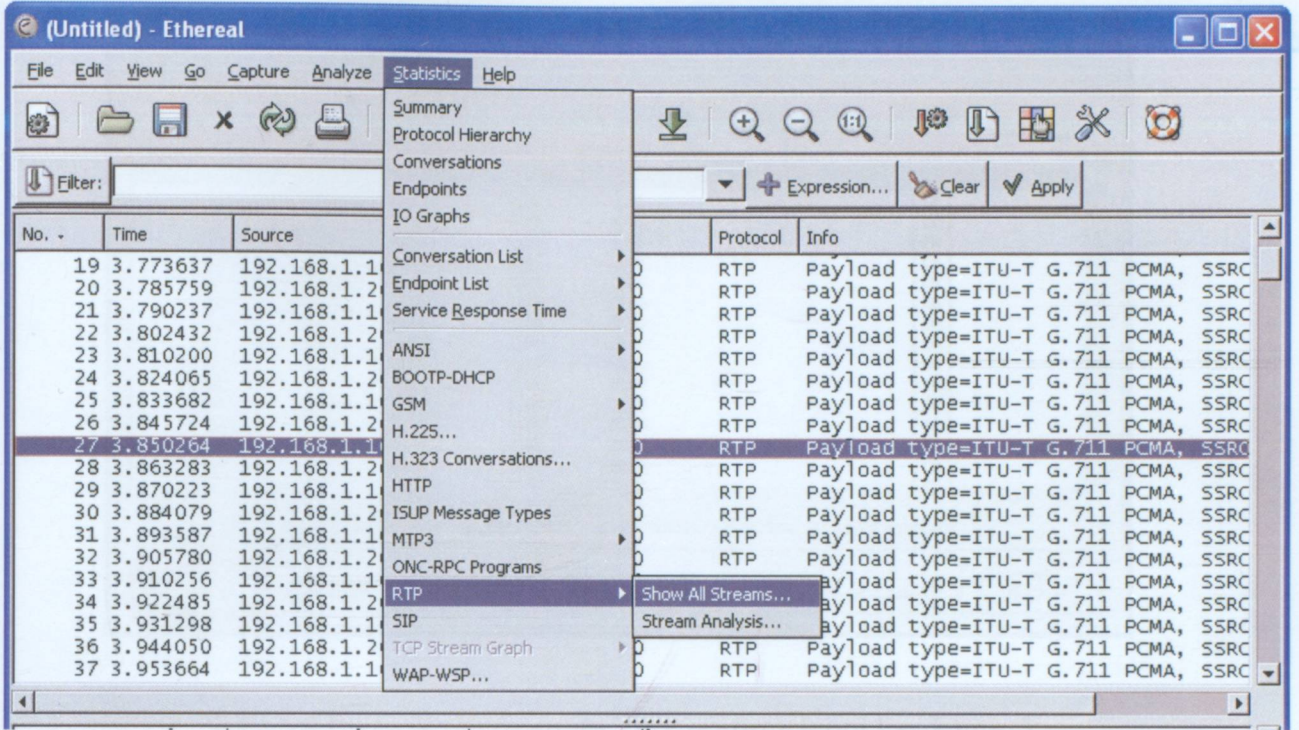
3. Görüşme gerçekleşip sonlandıktan sonra saldırgan bilgisayarı üzerinde çalışan veri yakalama programını durdurur (Şekil 6.6).
4. Sonrasında sırasıyla Şekil 6.7 ve Şekil 6.8’de gösterildiği gibi tüm RTP paketleri analiz edilir.
5. Analiz edilen RTP paketleri sırasıyla Şekil 6.9 ve Şekil 6.10’da gösterildiği gibi wav uzantılı ses dosyası haline getirilir. Kaydedilen bu ses dosyası iki yasal kullanıcının IP protokolü üzerinden gerçekleştirdiği telefon görüşmesinin bir kayıdır.



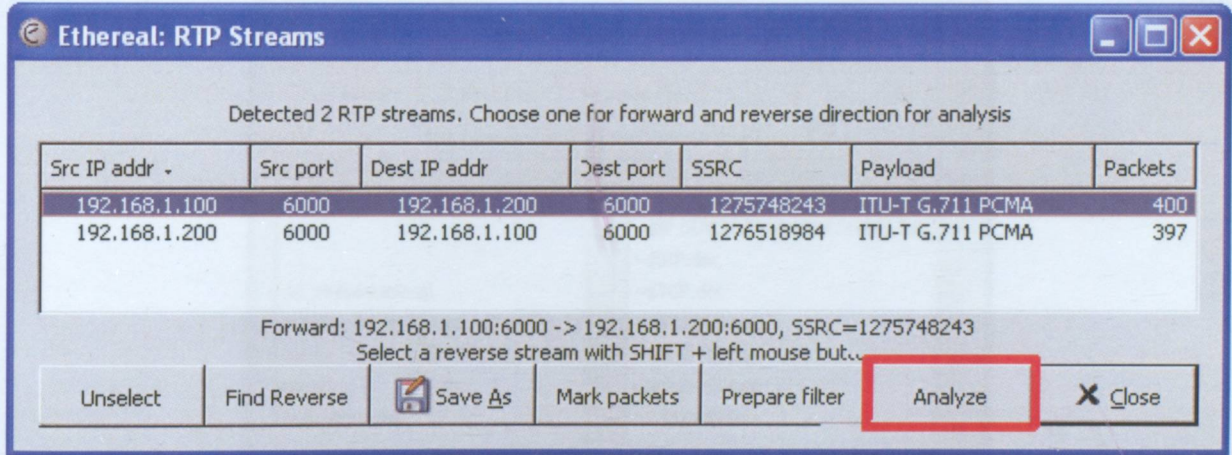
Şekil 6.5 Ethereal programı ile VoIP görüşmelerini kaydetme_1



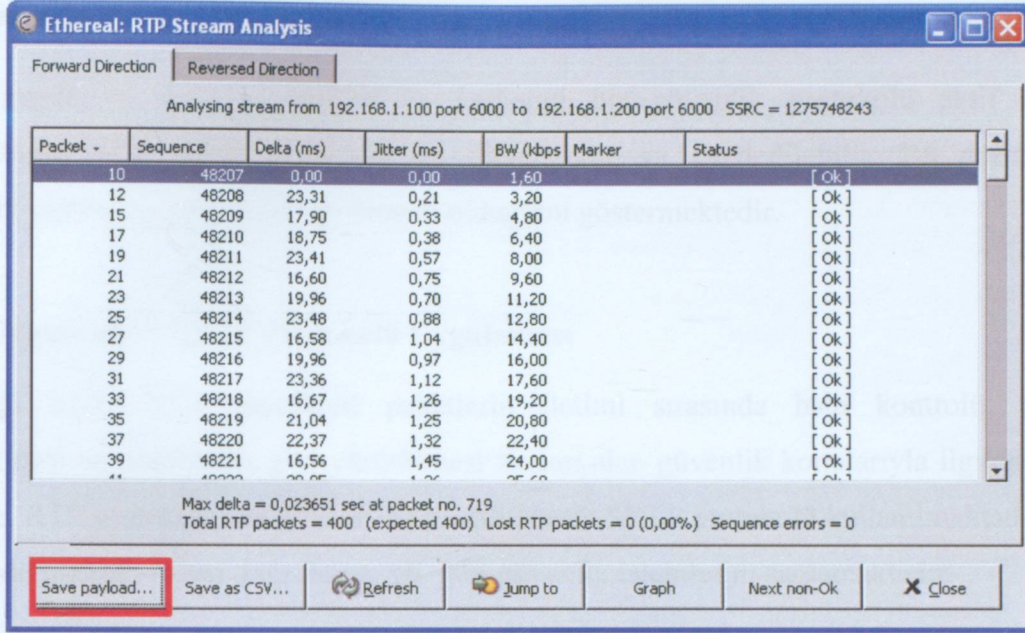
Şekil 6.6 Ethereal programı ile VoIP görüşmelerini kaydetme_2



Şekil 6.7 Ethereal programı ile VoIP görüşmelerini kaydetme_3

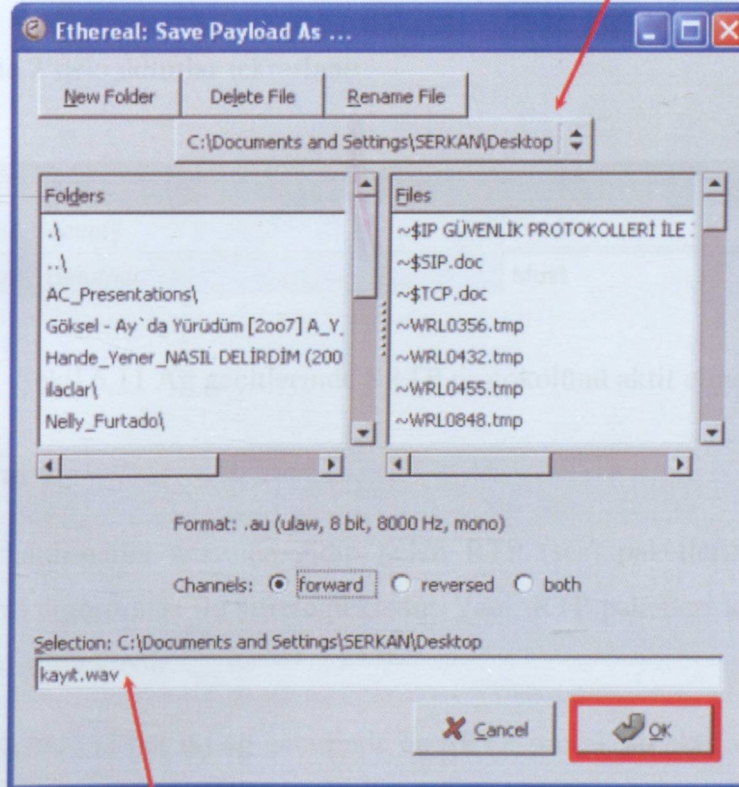


Şekil 6.8 Ethereal programı ile VoIP görüşmelerini kaydetme_4



Şekil 6.9 Ethereal programı ile VoIP görüşmelerini kaydetme_5

Dosya kayıt yeri seçilir.

.wav uzantılı bir dosya
ismi yazılır

Şekil 6.10 Ethereal programı ile VoIP görüşmelerini kaydetme_6

Uygulama Sonucu:

Bu uygulama sonucunda görüldü ki herhangi bir güvenlik protokolü aktif değilken gerçekleşen VoIP görüşmeleri kolayca dinlenebilir ve kaydedilebilir. Bu durum VoIP güvenlik protokollerinin ne kadar önemli olduğunu göstermektedir.

6.3 Uygulama 3: SRTP Protokolü Uygulaması

Bilindiği üzere RTP protokolü paketlerin iletimi sırasında hata kontrolü, hataların düzeltilmesi ve doğrulama gibi yürütülmesi zaman alan güvenlik konularıyla ilgilenmez. Bu nedenle, RTP protokolünün güvenli bir profili olarak SRTP protokolü kullanılmaktadır. SRTP protokolü gizlilik, mesaj doğrulama, vb. gibi güvenlik işlemlerini sağlamaktadır.

Bu uygulamada bir önceki uygulamada gerçekleştirilen gizli dinleme saldırısına karşı SRTP protokolünün kullanılması gösterilecektir.

Uygulama Adımları:

1. Ağ geçitlerinin her ikisinde de SRTP protokolü aktif edilir (Şekil 6.11).
2. Uygulama 2'deki adımlar tekrarlanır.

SRTP Settings	
Enable Media Security	Enable
Media Security Behavior	Must

Şekil 6.11 Ağ geçitlerinde SRTP protokolünü aktif etme

Uygulama Sonucu:

SRTP protokolü katılımcılar arasında gidip gelen RTP (ses) paketlerini AES (Advanced Encryption System) algoritması ile şifrelemektedir. Yani, RTP paketleri katılımcılar arasında şifreli bir şekilde iletilmektedir.

Bu uygulamada görüldü ki her iki ağ geçidinde de SRTP protokolü aktif edildiğinde, üçüncü bir kişi tarafından RTP paketlerinin gizlice ele geçirilmesi durumunda ele geçirme işlemi gerçekleştiren veri yakalama programı RTP paketlerini ayırt edememekte ve bu paketleri RTP paketi olarak değil de UDP paketi olarak algılamaktadır (Şekil 6.12). Bunun sebebi, RTP paketlerinin AES şifreleme metoduyla şifrelenmiş olması ve paketlerin artık normal RTP

formatında olmamasıdır.

Saldırgan tarafından bu UDP paketleri bir şekilde RTP paketlerine dönüştürülüp sonrasında da wav uzantılı ses dosyası haline getirilse dahi RTP paketlerinin şifreli olmasından dolayı bu kaydedilen ses dosyası sadece bir cızırtıdan ibarettir.

Sonuç olarak, SRTP protokolünün bu tarz gizli dinleme saldırılarına karşı ne kadar önemli olduğu açıkça görülmektedir.

No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.1.100	192.168.1.200	SIP/SD	Request: INVITE sip:200@192.168.1.
2	0.032882	192.168.1.200	192.168.1.100	SIP	Status: 100 Trying
3	0.041232	192.168.1.200	192.168.1.100	SIP	Status: 180 Ringing
4	0.073917	192.168.1.100	192.168.1.200	SIP	Request: PRACK sip:200@192.168.1.2
5	0.094217	192.168.1.200	192.168.1.100	SIP	Status: 200 OK
6	3.472677	192.168.1.200	192.168.1.100	SIP/SD	Status: 200 OK, with session descr
7	3.506693	192.168.1.100	192.168.1.200	SIP	Request: ACK sip:200@192.168.1.200
8	3.524488	192.168.1.100	192.168.1.200	UDP	Source port: 6000 Destination por
9	3.538778	192.168.1.100	192.168.1.200	UDP	Source port: 6000 Destination por
10	3.547778	192.168.1.200	192.168.1.100	UDP	Source port: 6000 Destination por
11	3.562370	192.168.1.100	192.168.1.200	UDP	Source port: 6000 Destination por
12	3.562959	192.168.1.100	192.168.1.200	UDP	Source port: 6001 Destination por
13	3.566493	192.168.1.200	192.168.1.100	UDP	Source port: 6000 Destination por
14	3.578698	192.168.1.100	192.168.1.200	UDP	Source port: 6000 Destination por
15	3.585881	192.168.1.200	192.168.1.100	UDP	Source port: 6000 Destination por
16	3.587739	192.168.1.200	192.168.1.100	UDP	Source port: 6001 Destination por
17	3.598701	192.168.1.100	192.168.1.200	UDP	Source port: 6000 Destination por

Şekil 6.12 SRTP protokolü aktif edilmiş ağ geçitleri arasındaki RTP paket akışı

6.4 Uygulama 4: IPSec Protokolü Uygulaması

IPSec protokolü OSI referans modelinin IP katmanında tüm IP paketlerini şifrelemek ve doğrulamak için kullanılan bir standarttır. VoIP'te IPSec protokolü, iki kişinin güvenli bir şekilde konuşmasını, bu konuşma sırasında her iki kişinin de gerçekten doğru kişiler olmasının sağlanması ve ilgili konuşmanın 3. bir kişi tarafından ele geçirilmemesini sağlamak amacıyla kullanılmaktadır.

VoIP üzerinden haberleşen iki nokta arasında IPSec güvenlik protokolünün kullanıldığı durumda IPSec ile ilgili aktif edilmesi gereken konfigürasyon parametreleri başlıca şu şekildedir:

1. Aşağıda belirtilen IKE protokolü parametreleri belirlenmelidir:

- IKE ana modda karşılıklı her iki noktada da tanımlı olmak zorunda olan özel bir ön paylaşım anahtar (pre-shared key) tanımlanır ve her iki nokta birbirini bu anahtar vasıtasıyla doğrular.
- IKE şifreleme metodu (DES, 3DES, vb.) belirlenir.
- IKE doğrulama protokolü (MD5 ya da SH1) belirlenir.
- IKE Diffie-Hellman (DH) protokol grubu (786 bit ya da 1024 bit) belirlenir.
- IKE güvenlik ilişkisi (SA) ömrü (saniye cinsinden) belirlenir.

2. Aşağıda belirtilen IPSec protokolü parametreleri belirlenmelidir:

- Her bir ağ geçidinde VoIP görüşmesi yapılacak diğer katılımcının IP adresi tanımlanır.
- IPSec şifreleme metodu (DES, 3DES vb.) belirlenir.
- IPSec doğrulama protokolü (MD5 ya da SH1) belirlenir.
- IPSec SA bağlantı ömrü (saniye cinsinden) belirlenir.
- IPSec iletim modları (Ulaşım modu ya da tünel modu) belirlenir.

Bu uygulamada aşağıda belirtilen hedefler amaçlanmaktadır:

1. IPSec protokolü aktif edilen iki ağ geçidinin başarılı bir şekilde haberleşebildiğini göstermek.
2. IPSec protokolü aktifken, paketler veri yakalama programıyla ele geçirilerek katılımcılar arasında gidip gelen IPSec mesajlarını görmek.
3. IPSec protokolü aktif edildiği halde katılımcılardan birinde ön paylaşım anahtarın farklı girilmesi durumunda VoIP görüşmesinin kurulamadığını göstermek.
4. IPSec protokolü aktif edildiği halde katılımcılardan birinde IKE ya da IPSec şifreleme metodunun diğerinden farklı bir metot seçilmesi durumunda VoIP görüşmesinin kurulamadığını göstermek.

Uygulama Adımları:

1. Ağ geçitlerinin her ikisinde de IPSec protokolü aktif edilir (Şekil 6.13)
2. Ağ geçitlerinin her ikisinde de aşağıda belirtilen IKE parametreleri aktif edilir (Şekil 6.14).
 - ✓ Ön paylaşımlı anahtar: **test**
 - ✓ IKE şifreleme metodu: **DES**
 - ✓ IKE doğrulama protokolü: **MD5**
 - ✓ IKE DH grubu: **DH-1024 bit**
 - ✓ SA ömür süresi: **28800 sn**

IPSec Settings	
Enable IP Security	Enable

Şekil 6.13 Ağ geçitlerinde IPSec protokolünü aktif etme

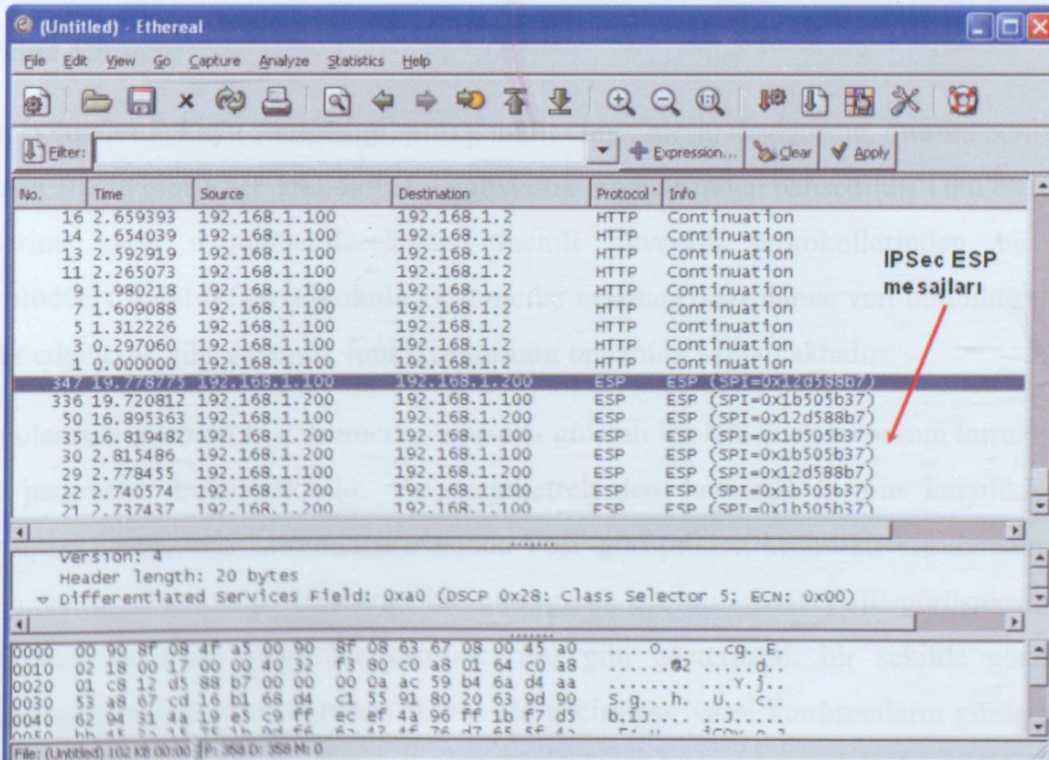
IKE Table	
Policy Index	0 State: Exists
Authentication Method	Pre-shared Key
Shared Key	*****
IKE SA LifeTime [sec]	28800
IKE SA LifeTime [KB]	0
First Proposal Encryption Type	DES-CBC
First Proposal Authentication Type	HMAC-MD5-96
First Proposal DH Group	DH-1024-BIT
Second Proposal Encryption Type	Not Defined
Second Proposal Authentication Type	Not Defined
Second Proposal DH Group	Not Defined
Third Proposal Encryption Type	Not Defined
Third Proposal Authentication Type	Not Defined
Third Proposal DH Group	Not Defined
Fourth Proposal Encryption Type	Not Defined
Fourth Proposal Authentication Type	Not Defined
Fourth Proposal DH Group	Not Defined

Şekil 6.14 Ağ geçitlerinde tanımlanması gereken IKE protokolü parametreleri

3. Ağ geçitlerinin her ikisinde de aşağıda belirtilen IPSec parametreleri aktif edilir (Şekil 6.15).
 - ✓ VoIP görüşmesi yapılacak diğer ağ geçidinin IP adresi: **192.168.1.200** (ilk ağ geçidi için).
 - ✓ IPSec şifreleme metodu: **DES**
 - ✓ IPSec doğrulama protokolü: **MD5**
4. IPSec protokolü aktif edilmiş ağ geçitleri arasındaki başarılı VoIP görüşmesi Ethereal programı vasıtasıyla yakalanarak, ağ geçitlerinin birbirlerine gönderdikleri Kapsülleme Güvenlik Yüğü (ESP-Encapsulation Security Payload) mesajları görülür (Şekil 6.16).
5. Ağ geçitlerinden birinde IKE parametrelerinden biri olan ön paylaşımlı anahtar diğerinden farklı tanımlanır. İlk ağ geçidinden diğerine doğru bir çağrı denemesi yapıldığında, diğer ağ geçidine bağlı telefonun çalmadığı yani VoIP görüşmesinin kurulamadığı görülür. Başarısız VoIP çağrısı Ethereal programı vasıtasıyla yakalanarak ağ geçitleri arasında gidip gelen İnternet Güvenlik İlişkisi ve Anahtar Yönetim Protokolü (ISAKMP- The Internet Security Association and Key Management Protocol) mesajları elde edilir (Şekil 6.17). Bu mesajlar sayesinde IKE protokolünün 1. fazında (ana modunda) gerçekleşen doğrulama mekanizmasının çalıştığını ve katılımcıların birbirlerini doğrulayamadığı için VoIP görüşmesinin kurulamadığı görülür.
6. Aynı şekilde ağ geçitlerinden birinde IPSec şifreleme metodu diğerinden farklı tanımlanır. İlk ağ geçidinden diğerine doğru bir çağrı denemesi yapıldığında diğer ağ geçidine bağlı telefonun çalmadığı yani VoIP görüşmesinin kurulamadığı görülür.

IPSec Table	
Policy Index	0 State: Exists
Related key exchange method	
Remote IP Address	192.168.1.200
Local IP Address Type	Control
Source Port	0
Destination Port	0
Protocol	0
Related Key Exchange Method Index	0
SA Lifetime [sec]	28800
SA Lifetime [KB]	0
First Proposal Encryption Type	DES-CBC
First Proposal Authentication Type	HMAC-MD5-96
Second Proposal Encryption Type	Not Defined
Second Proposal Authentication Type	Not Defined
Third Proposal Encryption Type	Not Defined
Third Proposal Authentication Type	Not Defined
Fourth Proposal Encryption Type	Not Defined
Fourth Proposal Authentication Type	Not Defined

Şekil 6.15 Ağ geçitlerinde tanımlanması gereken IPSec protokolü parametreleri



IPSec ESP mesajları

No.	Time	Source	Destination	Protocol	Info
16	2.659393	192.168.1.100	192.168.1.2	HTTP	Continuation
14	2.654039	192.168.1.100	192.168.1.2	HTTP	Continuation
13	2.592919	192.168.1.100	192.168.1.2	HTTP	Continuation
11	2.265073	192.168.1.100	192.168.1.2	HTTP	Continuation
9	1.980218	192.168.1.100	192.168.1.2	HTTP	Continuation
7	1.609088	192.168.1.100	192.168.1.2	HTTP	Continuation
5	1.312226	192.168.1.100	192.168.1.2	HTTP	Continuation
3	0.297060	192.168.1.100	192.168.1.2	HTTP	Continuation
1	0.000000	192.168.1.100	192.168.1.2	HTTP	Continuation
347	19.778775	192.168.1.100	192.168.1.200	ESP	ESP (SPI=0x12d588b7)
336	19.720812	192.168.1.200	192.168.1.100	ESP	ESP (SPI=0x1b505b37)
50	16.895363	192.168.1.100	192.168.1.200	ESP	ESP (SPI=0x12d588b7)
35	16.819482	192.168.1.200	192.168.1.100	ESP	ESP (SPI=0x1b505b37)
30	2.815486	192.168.1.200	192.168.1.100	ESP	ESP (SPI=0x1b505b37)
29	2.778455	192.168.1.100	192.168.1.200	ESP	ESP (SPI=0x12d588b7)
22	2.740574	192.168.1.200	192.168.1.100	ESP	ESP (SPI=0x1b505b37)
21	2.737437	192.168.1.200	192.168.1.100	ESP	ESP (SPI=0x1b505b37)

Version: 4
Header length: 20 bytes
Differentiated Services Field: 0xa0 (DSCP 0x28: Class Selector 5; ECN: 0x00)

0000 00 90 8f 08 4f a5 00 90 8f 08 63 67 08 00 45 a00...cg..E..
0010 02 18 00 17 00 00 40 32 f3 80 c0 a8 01 64 c0 a802.....d..
0020 01 c8 12 d5 88 b7 00 00 00 0a ac 59 b4 6a d4 aaY.j..
0030 53 a8 67 cd 16 b1 68 d4 c1 55 91 80 20 63 9d 90 S.g...h...U..C..
0040 62 94 31 4a 19 e5 c9 ff ec ef 4a 96 ff 1b f7 d5 b.ij....J...
0050 8b 88 23 18 78 1b 04 f6 63 42 4f 76 d7 65 5f a3

Şekil 6.16 IPSec protokolü aktif edilmiş ağ geçitleri arasındaki mesajlaşma

No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.1.100	Broadcast	ARP	who has 192.168.1.200? Tell 192.168.1.100
2	0.000353	192.168.1.200	192.168.1.100	ARP	192.168.1.200 is at 00:90:8f:08:4f:a5
3	0.001964	192.168.1.100	192.168.1.200	ISAKMP	Identity Protection (Main Mode)
4	0.003000	192.168.1.200	192.168.1.100	ISAKMP	Identity Protection (Main Mode)
5	0.546264	192.168.1.100	192.168.1.200	ISAKMP	Identity Protection (Main Mode)
6	1.774576	192.168.1.200	192.168.1.100	ISAKMP	Identity Protection (Main Mode)
7	2.472345	192.168.1.100	192.168.1.200	ISAKMP	Identity Protection (Main Mode)
8	2.473354	192.168.1.200	192.168.1.100	ISAKMP	Identity Protection (Main Mode)

Internet Security Association and Key Management Protocol

Initiator cookie: 0xE7E0D0ABF6F2C84F

Responder cookie: 0x0FFE5AB5B15E631C

Next payload: Security Association (1)

Version: 1.0

Exchange type: Identity Protection (Main Mode) (2)

Flags

-0 = No encryption
-0 = No commit
-0 = No authentication

Message ID: 0x00000000

Length: 92

Security Association payload

Next payload: NONE (0)

Length: 64

Domain of interpretation: IPSEC (1)

Situation: IDENTITY (1)

Proposal payload # 1

Next payload: NONE (0)

Length: 52

Proposal number: 1

Protocol ID: ISAKMP (1)

SPI size: 0

Number of transforms: 1

Transform payload # 1

Next payload: NONE (0)

Length: 44

Transform number: 1

Transform ID: KEY_IKE (1)

Encryption Algorithm (1): DES-CBC (1)

IKE Ana Modda doğrulama mekanizmasının katılımcıları doğrulayamadığı görülür.

Diğer IPsec parametreleri görülür.

Şekil 6.17 IKE protokolünün ilk fazında gerçekleşen mesajlaşma

Uygulama Sonucu:

Önceki bölümlerde kayıt sahteciliği, proxy taklit etme, mesaj değiştirme, oturum sonlandırma ve izinsiz erişim gibi VoIP teknolojisinin güvenlik tehditlerinden bahsedildi. Tüm bu güvenlik tehditlerine karşı uygulanabilecek en önemli güvenlik protokollerinden biri IPsec protokolüdür. Çünkü IPsec protokolü katılımcılar arasında doğrulama, veri bütünlüğü, gizlilik ve inkar edememe gibi güvenlik fonksiyonlarının tamamını sağlamaktadır.

Bu uygulamada görüldü ki katılımcılar arasında güvenli bir IPsec oturumunun kurulması için birçok parametre bulunmaktadır. Bu parametrelerden herhangi birinin karşılıklı olarak eşleşmemesi durumunda katılımcılar arasında VoIP görüşmeleri kesinlikle kurulamamaktadır. Bu şu anlama gelmektedir: Herhangi bir saldırganın mevcut yasal VoIP görüşmesine dahil olması, yani kendisini yasal bir katılımcıymış gibi göstermesi, bir şekilde görüşmeleri kendisine yönlendirip tüm çağrı kayıtlarını ele geçirmesi, yasal katılımcıların görüşmelerine müdahale edip çağrıların kurulmasını engellemesi ya da kurulmuş çağrıları sonlandırması imkansızdır. Çünkü, saldırganın tüm bu işlemleri gerçekleştirebilmesi için katılımcılar arasında tanımlanmış olan tüm IPsec parametrelerini biliyor olması gerekmektedir.

7. ŞİFRELEME ALGORİTMALARININ PERFORMANS ANALİZİ

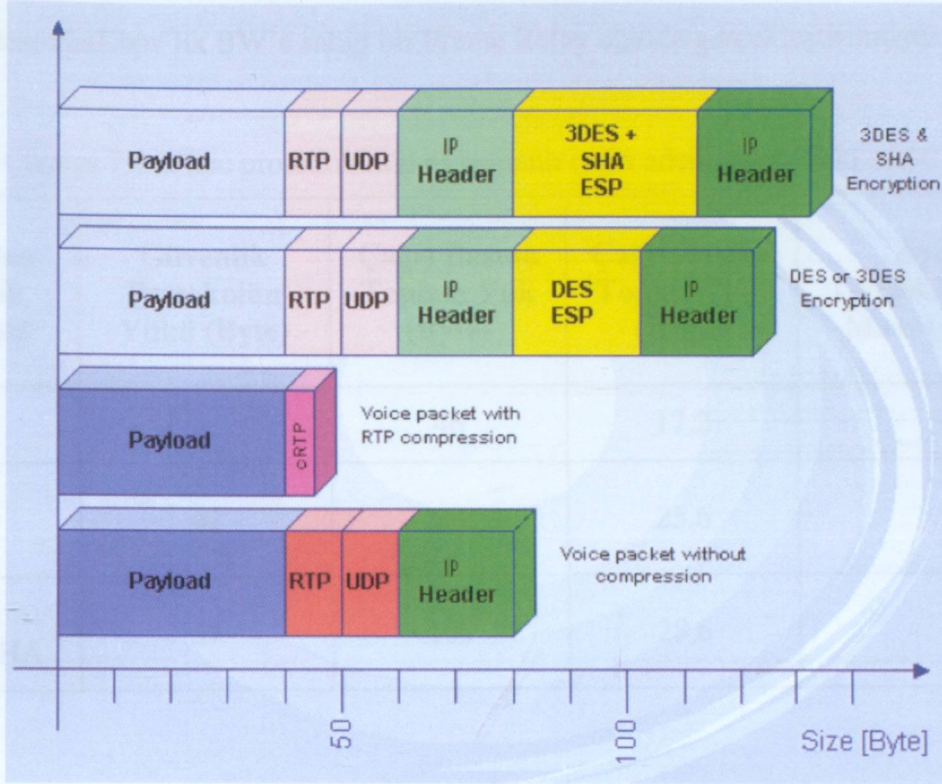
Bir önceki bölümde VoIP sistemlerine karşı gerçekleştirilebilecek muhtemel saldırıların VoIP güvenlik protokollerinin kullanımı ile nasıl başarısız olduğu açıkça görülmüştür. Bu bölümde VoIP güvenlik protokollerinin kullandığı DES, 3DES, SHA ve MD5 gibi şifreleme algoritmalarının VoIP görüşmeleri üzerindeki olumsuz etkileri incelenecektir. Bu analiz IPSec protokolü ve kullandığı algoritmalar baz alınarak gerçekleştirilmiştir.

7.1 IPSec Güvenlik Protokolünün Ses İletimi Üzerindeki Olumsuz Etkileri

IPSec güvenlik protokolü ses trafiğini olumsuz etkileyen iki temel faktörü de beraberinde getirmektedir. Bunlardan ilki artan paket büyüklüğü iken diğeri çağrı kurulum süresinin artması yani gecikmedir.

IPSec bağlantılarının oluşturulması esnasında karşı taraf ile bir tünel anlaşması yapılır. Tünel işleminde paketler bir çerçeve içerisine alınarak saklanır. İki nokta arasında güvenli iletişimi sağlayan bu IPSec tüneli, orijinal IP paketine ilave bir IP başlığı (IP header) ekler. Bununla birlikte, yük doğrulama (payload authentication), veri bütünlüğü (data integrity) ve güvenilirlik/şifreleme (confidentiality/encryption) işlemlerinin tümünü gerçekleştiren Kapsülleme Güvenlik Yüğü (ESP-Encapsulation Security Payload) de beraberinde kendi başlık yükünü getirir.

Şekil 7.1 IPSec güvenlik protokolünün uygulanmadığı durumdaki bir ses datasının toplam paket büyüklüğünü ve IPSec protokolünün çeşitli kombinasyonlarının uygulanması durumundaki paket büyüklüklerini göstermektedir. Bu kombinasyonlardan birinde şifreleme algoritması olarak DES protokolü kullanılıp, herhangi bir doğrulama (özetleme) algoritması kullanılmazken; diğesinde ise şifreleme algoritması olarak 3DES protokolü kullanılıp doğrulama (özetleme) algoritması olarak da SHA kullanılmıştır. Buradan görülmektedir ki her bir şifreleme/doğrulama algoritması orijinal paket büyüklüğüne kendi başlık bilgisini ilave etmektedir. Ayrıca, oluşturulan IPSec tüneli de orijinal IP başlığına ilaveten yeni bir IP başlığı yükü getirmektedir.



Şekil 7.1 IPsec protokolünün paket yükü üzerine etkisi (Barbieri ve Bruschi, 2005)

Şekil 7.1’de görüldüğü üzere RTP paketlerinin sıkıştırılmasını sağlayan cRTP (Compressed RTP) protokolünün kullanılması durumunda minimum paket büyüklüğü elde edilirken; IPsec güvenlik protokolünün kullanılması durumunda ise 120-130 Byte değerlerine yükselen bir paket büyüklüğü oluşmaktadır.

Paket büyüklüğünün artması hem VoIP çağrılarının fazla bant genişliği kullanmasına sebep olurken hem de çağrı iletim sürelerinin uzamasına yani gecikmenin ortaya çıkmasına sebep olmaktadır. Kullanılan bant genişliklerinin artması sınırlı bant genişliğine sahip hatlarda hem aynı anda kurulan çağrı sayısını düşürürken hem de ses kalitesinin olumsuz etkilenmesine sebep olmaktadır.

Çizelge 7.1’de 128Kbps’lik bant genişliğine (BW-Bandwidth) sahip bir hatta gerçekleştirilen bir VoIP uygulamasında hem IPsec kullanılması durumunda hem de kullanılmaması durumunda aynı anda gerçekleştirilebilen maksimum çağrı adedi karşılaştırılması yapılmıştır.

Bu karşılaştırma testi yapılırken aşağıda belirtilen hususlar dikkate alınmıştır.

- 8Kbps BW’e sahip G.729 ses kodlayıcısı kullanılmıştır.
- Örnekleme büyüklüğü (sample size) 40pps (packets per seconds) seçilmiştir.

- Bu test 128Kbps'lik BW'e sahip bir Frame Relay ağında gerçekleştirilmiştir.

Çizelge 7.1 IPSec protokolünün eş zamanlı çağrı adedi üzerindeki etkisi

Kullanılan Güvenlik Protokolü	Güvenlik Protokolün Yüğü (Byte)	Çağrı Başına Toplam Yüğü (Byte)	Çağrı Başına Toplam BW (Kbps)	Aynı Anda Gerçekleştirilebilen Max. Çağrı Adedi
-	-	46	17,2	7
IPSec DES	42	88	25,6	5
IPSec DES + SHA	57	103	28,6	4

Çağrı Başına Toplam yüğü, Çağrı Başına Toplam BW ve Aynı anda gerçekleştirilebilen maksimum çağrı adedi değerleri sırasıyla (7.1), (7.2) ve (7.3) eşitliklerine dayanılarak hesaplanmıştır.

Çağrı Başına Toplam Yüğü = IP + RTP + UDP + Frame Relay başlık yüğü + diğer protokollerin başlık yükleri (7.1)

NOT: IP + RTP + UDP protokollerinin toplam başlık yüğü değeri 40Byte iken Frame Relay uygulaması 6Byte'lık bir ilave paket yüğü getirmektedir.

→ Çağrı Başına Toplam Yüğü = 40 + 6 + diğer protokollerin başlık yükleri

→ Çağrı Başına Toplam Yüğü = 46 + diğer protokollerin başlık yükleri

Çağrı Başına Toplam BW = Codec BW x [Çağrı Başına Toplam Yüğü + örnekleme büyüklüğü] / örnekleme büyüklüğü (7.2)

→ Çağrı Başına Toplam BW = 8Kbps x [46 + diğer protokollerin başlık yükleri + 40]/40

→ Çağrı Başına Toplam BW = 8Kbps x [86 + diğer protokollerin başlık yükleri] /40

Aynı Anda Gerçekleştirilebilen Maksimum çağrı adedi = Hat kapasitesi / Çağrı Başına Toplam BW (7.3)

→ Eş zamanlı çağrı adedi = 128 Kbps / Çağrı Başına Toplam BW

Görüldüğü gibi kullanılan şifreleme ve doğrulama algoritmalarının karmaşıklığına göre çağrı başına BW tüketimi artış göstermekte, bu durum da eş zamanlı kurulabilen çağrı adedi miktarını düşürmektedir.

Şimdiye kadar IPSec protokolünün paket büyüklüğü üzerine etkisinden bahsedildi. Paket büyüklüğünü arttırmasının yanında IPSec protokolü çağrı kurulum sürelerinin artmasına yani gecikmeye de sebep olmaktadır. Bu gecikmenin iki sebebi bulunmaktadır. Bunlardan ilki IPSec protokolünün paket büyüklüğünü arttırması iken diğeri ve en önemlisi şifreleme işlemlerini gerçekleştiren VoIP cihazlarının sebep olduğu gecikmedir. Bunu biraz daha açacak olursak; IPSec güvenlik protokolü aktif edilmiş VoIP cihazları şifreleme işlemlerini gerçekleştirirken paket şifreleme ve yeni başlık bilgilerinin (ESP ve IP tüneli) eklenmesi gibi bazı operasyonları gerçekleştirir. Bu operasyonlar VoIP cihazlarının CPU kullanımını normalinkinden çok daha fazla arttırır. Bu durum da çağrıların geç analiz edilmesine ve dolayısıyla da çağrıların geç kurulmasına sebep olmaktadır.

IPSec güvenlik protokolünün gecikme üzerine olan etkisini daha iyi anlayabilmek için IPSec konuşan iki VoIP ağ geçidinde farklı şifreleme ve doğrulama algoritmaları aktif edilerek farklı VoIP senaryoları oluşturuldu. Buradaki amaç, kullanılan farklı şifreleme ve doğrulama algoritmalarının her birinin gecikme üzerindeki etkilerini ayrı ayrı gözlemlemektir.

Analiz sırasında hiçbir şifreleme ve doğrulama algoritmasının kullanılmadığı, doğrulama algoritması kullanılmaksızın sadece DES şifreleme algoritmasının ve sadece 3DES şifreleme algoritmasının kullanıldığı, şifreleme algoritması kullanılmaksızın sadece SHA doğrulama algoritmasının ve sadece MD5 doğrulama algoritmasının kullanıldığı ve son olarak da şifreleme algoritması olarak 3DES ve doğrulama algoritması olarak da SHA'nın kullanıldığı farklı senaryolar tek tek denendi. Her bir senaryoda bir VoIP cihazından diğerine doğru çağrı başlatıldığı andan diğer VoIP cihazının portuna bağlı telefonun çalmaya başladığı ana kadar geçen süre tek tek gözlemlendi ve Çizelge 7.2'deki karşılaştırma tablosu oluşturuldu.

Çizelge 7.2 Şifreleme ve doğrulama algoritmalarının çağrı kurulum süresi üzerine etkileri

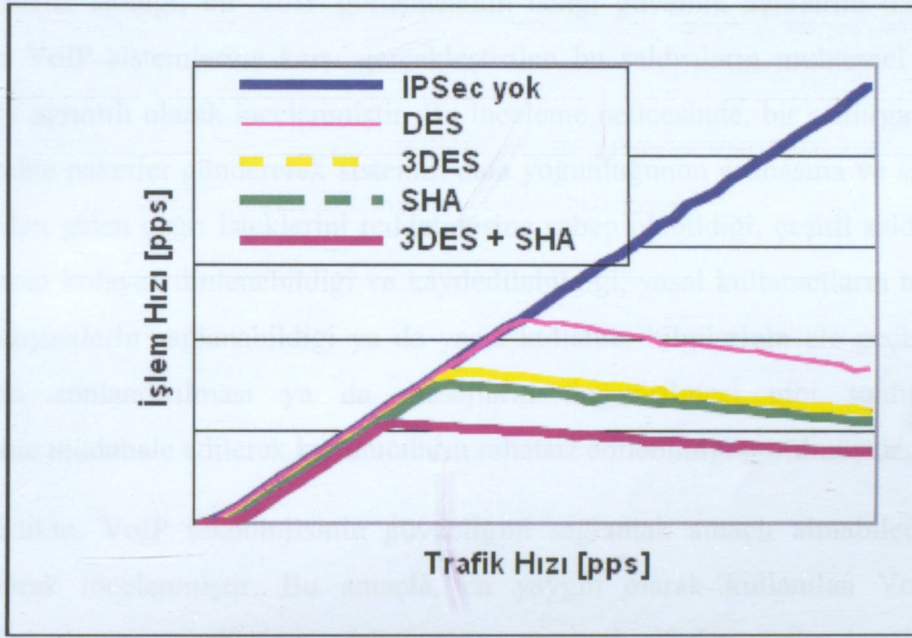
Kullanılan Şifreleme Algoritması	Kullanılan Doğrulama Algoritması	Uçtan Uca Çağrı Kurulum Süresi (ms)
-	-	315
DES	-	482
3DES	-	515
-	SHA	598
-	MD5	576
DES	MD5	826
3DES	SHA	956

Gerçekleştirilen bu analiz neticesinde aşağıdaki sonuçlar elde edildi:

- 3DES şifreleme algoritması DES şifreleme algoritmasına nazaran daha fazla gecikmeye sebep olmaktadır. Bu durum 3DES algoritmasının DES logaritmasından daha kompleks bir yapıya sahip olması nedeniyle VoIP ağ geçitlerinin CPU kullanımının 3DES algoritmasında daha fazla olduğunu göstermektedir.
- SHA doğrulama algoritması MD5 doğrulama algoritmasına nazaran daha fazla gecikmeye sebep olmaktadır. Bu durum SHA algoritmasının MD5 algoritmasından daha kompleks bir yapıya sahip olması nedeniyle VoIP ağ geçitlerinin CPU kullanımının SHA algoritmasında daha fazla olduğunu göstermektedir.
- En fazla gecikme 3DES şifreleme algoritması ve SHA doğrulama algoritmasının aynı anda kullanıldığı durumda yaşanmaktadır ve bu süre IPSec güvenlik protokolünün kullanılmadığı durumdaki sürenin 3 katıdır.

Bu performans analizi iki VoIP ağ geçidi arasında aynı anda sadece 1 çağrı gerçekleştirilerek yapılmıştır. Ancak pratikte iki VoIP cihazı arasında aynı anda gerçekleştirilen çağrı adedi mutlaka daha fazla olmaktadır. Ağ geçitleri arasındaki eş zamanlı çağrı adedinin artması demek VoIP ağ geçitlerinin CPU kullanımının çok daha fazla olması ve dolayısıyla da çağrı kurulum sürelerinin çok daha fazla artacağı anlamına gelmektedir.

Şekil 7.2, doğrulama algoritmalarının kullanımına bağlı olarak değişen (düşen) işlem hızı (Throughput) ile bant genişliği (trafik hızı) arasındaki ilişkiyi göstermektedir. İşlem hızı, belli bir sürede iki cihaz arasında transfer edilen data miktarını ifade etmektedir ve birimi pps (packets per seconds) olarak verilmektedir. Kısacası işlem hızı belirli bir bant genişliğinin verimli olarak kullanıldığı kısmıdır. Ağ şebekesinden kaynaklanan problemler, şifreleme ve doğrulama algoritmalarının kullanılması, vb. gibi nedenlerden dolayı bant genişliği tam olarak verimli kullanılamaz. Yani, zamanın herhangi bir anında iki nokta arasındaki data hızı değerine işlem hızı adı verilir.



Şekil 7.2 Şifreleme ve doğrulama algoritmalarının işlem hızı üzerine etkileri (Barbieri ve Bruschi, 2005)

Şekil 7.2'den görüldüğü gibi kullanılan algoritmaların kopleksliğine bağlı olarak elde edilen işlem hızı değeri düşmektedir. İşlem hızı üzerinde en az etkiyi DES algoritması yapmaktadır.

8. SONUÇLAR

Günümüzde yerel telekom operatörlerinin sunduğu klasik PSTN ses hizmetine alternatif olarak sunulan VoIP tabanlı ses hizmetleri, telefon görüşmelerinin mevcut data hattı üzerinden yapılması nedeniyle maddi anlamda bir çok işletmenin ilgisini çekmiştir. Bununla birlikte, firmaların kendi şubeleri arasında ücretsiz görüşebilmelerine imkan sağlaması sebebiyle de, VoIP günümüzde çok yaygın olarak tercih edilmektedir.

Bu çalışmada, VoIP teknolojisinin avantajlarının yanında hem VoIP hizmeti veren alternatif telekom operatörlerinin hem de bu hizmeti alan işletmelerin ve son kullanıcıların hangi tehditlere maruz kaldığı, bir VoIP görüşmesinin hangi güvenlik açıklarını da beraberinde getirdiği ve VoIP sistemlerine karşı gerçekleştirilen bu saldırıların muhtemel sonuçlarının neler olduğu ayrıntılı olarak incelenmiştir. Bu inceleme neticesinde, bir saldırganın bir hedef VoIP sistemine paketler göndererek sistemin data yoğunluğunun artmasına ve sistemin yasal kullanıcılardan gelen çağrı isteklerini reddetmesine sebep olabildiği, çeşitli saldırılarla VoIP görüşmelerinin kolayca dinlenebildiği ve kaydedilebildiği, yasal kullanıcıların taklit edilerek ücretsiz görüşmelerin sağlanabildiği ya da yasal kullanıcı bilgilerinin ele geçirilebildiği ve görüşmelerin sonlandırılması ya da mesajların değiştirilmesi gibi saldırılarla VoIP görüşmelerine müdahale edilerek kullanıcıların rahatsız edilebildiği görülmüştür.

Bununla birlikte, VoIP teknolojisinin güvenliğini sağlamak amaçlı alınabilecek önlemler ayrıntılı olarak incelenmiştir. Bu amaçla, en yaygın olarak kullanılan VoIP güvenlik protokollerine, bu protokollerin temelini oluşturan veri şifreleme algoritmalarına ve bu algoritmaların temel özelliklerine ayrıntılı olarak değinilmiştir. Bu inceleme neticesinde, güvenli bir VoIP oturumunun kurulabilmesi için her bir VoIP katılımcısının veri şifrelemede kullanılan şifreleme metotları, şifrelemede ve şifre çözmede kullanılan anahtarların takası için kullanılan metotlar ve bu metotların kendilerine özgü kullandıkları güvenlik parametreleri konusunda mutabakata vardıkları, veri şifreleme algoritmalarının ve VoIP güvenlik protokollerinin katılımcılar arasındaki gizliliği, kimlik doğrulamayı ve veri bütünlüğünü farklı yöntemlerle sağladıkları görülmüştür.

VoIP uygulamalarında güvenlik duvarı ihtiyacı incelenerek, VoIP uygulamalarında güvenlik duvarının önemi, bu amaçla kullanılabilen güvenlik duvarı modelleri, VoIP teknolojisinde güvenlik duvarı kullanımının faydalarının yanında getirdiği zorluklar, bu zorlukların nasıl aşılabileceği ve bu amaçla kullanılabilecek cihazların neler olduğu ayrıntılı olarak incelenmiştir.

Çalışmanın sonunda VoIP güvenlik protokollerinin önemini gösteren uygulamalar gerçekleştirilmiştir. İlk uygulamada bir yerel alan ağı içerisinde bulunan iki VoIP ağ geçidinin SIP protokolü üzerinden konuştukları basit bir VoIP senaryosu gerçekleştirilmiştir. İkinci uygulamada, ağ geçitleri üzerinde herhangi bir VoIP protokolü aktif değilken, ağ geçitleri arasındaki görüşmenin nasıl kolayca kaydedilebileceği gösterilmiştir. Üçüncü uygulamada ağ geçitleri üzerinde Güvenli Gerçek Zamanlı Taşıma Protokolü (SRTP-Secure Real-Time Transport Protocol) aktif edilerek, ikinci uygulamada gerçekleştirilen gizli dinleme saldırısının nasıl başarısız olduğu gösterilmiştir. Dördüncü ve son uygulamada ise kayıt sahteciliği, proxy taklit etme, mesaj değiştirme, izinsiz erişim, vb. gibi VoIP teknolojisinin diğer güvenlik tehditlerine karşı uygulanabilecek en önemli güvenlik protokollerinden biri olan İnternet Protokolü Güvenliği (IPSec) ile ilgili bir uygulama gerçekleştirilerek uygulama sonucunda, yasal kullanıcılar arasında karşılıklı olarak IPSec protokolünün aktif edilmesi durumunda bahsedilen saldırıların gerçekleştirilmesinin mümkün olmadığı görülmüştür.

Son bölümde gerçekleştirilen performans analizleri neticesinde, VoIP güvenlik protokollerinin kullandıkları DES, 3DES, SHA, MD5, vb. gibi şifreleme/doğrulama algoritmalarının ses kalitesinin bozulması ve çağrı kurulum sürelerinin artması gibi olumsuz etkilerinin olduğu görülmüştür.

Tüm bu işlemler ve gerçekleştirilen uygulamalar neticesinde; günümüzde gittikçe önem kazanan VoIP teknolojisinin birçok güvenlik problemini de beraberinde getirdiği, herhangi bir önlem alınmaması durumunda bu güvenlik problemlerinin hem son kullanıcılar hem de işletmeler açısından önemli tehditler oluşturabileceği görülmüştür. Bu güvenlik tehditlerine karşı uygulanabilecek VoIP güvenlik protokollerinin her birinin farklı işlevlerinin olduğu, yani VoIP sistemleri üzerine gerçekleştirilebilen farklı saldırı tipleri için farklı güvenlik protokollerinin kullanılması gerektiği görülmüştür. Bunun nedeni, güvenlik protokollerinin görev yaptıkları katmanların birbirinden farklı olmasıdır. Örneğin, ses datalarını taşıyan RTP paketlerinin şifrlenmesini sağlayan SRTP protokolü, OSI referans modelinin 5. katmanında görev alırken; katılımcılar arasında sanal bir tünel oluşturarak yasal olmayan kişilerin araya girmesine ya da görüşmelere müdahale etmesine izin vermeyen IPSec protokolü, OSI referans modelinin 3. katmanında görev almaktadır.

Buradan görülmektedir ki, VoIP sistemlerinin tam anlamda güvenliğini sağlamak için sadece tek bir güvenlik protokolünün kullanılması yeterli olmamaktadır. %100 bir güvenlik için farklı katmanlarda görev yapan ve farklı işlevleri yerine getiren farklı güvenlik protokollerinin aktif edilmesi gerekmektedir. Örneğin, sadece SRTP protokolünün aktif edilip diğer

protokollerin aktif edilmemesi, VoIP görüşmelerinin gizli dinlenilmesi problemini çözmenin ötesine gidemeyecek ve diğer saldırılar için hala açık kapılar mevcut olacaktır.

KAYNAKLAR

- Arkko, J., Carrara, E., Lindholm, F., Naslund, M. ve Norrman, K. (2004), "MIKEY: Multimedia Internet KEYing", Internet Engineering Task Force, <http://www.ietf.org/rfc/rfc2830.txt>.
- Barbieri, R. ve Bruschi, D. (2005), "Voice over IPsec: Analysis and Solutions", Dipartimento di Scienze dell'Informazione Università degli Studi di Milano
- Baughner, M. ve McGrew, D. (2004), "The Secure Realtime Transport Protocol (SRTP)", Internet Engineering Task Force, <http://www.ietf.org/rfc/rfc3711.txt>.
- Baykal, N. (2001), Bilgisayar Ağları, SAS Bilişim Yayınları, Ankara.
- Dierks, T. ve Allen, C. (1999), "The TLS Protocol Version 1.0", Internet Engineering Task Force, <http://www.ietf.org/rfc/rfc2246.txt>.
- Handley, M. ve Jacobson, V. (1998), "SDP: Session Description Protocol", Internet Engineering Task Force, <http://www.ietf.org/rfc/rfc2327.txt>.
- Harkins, D. ve Carrel, D. (1998) "The Internet Key Exchange (IKE)", Internet Engineering Task Force, <http://www.ietf.org/rfc/rfc2409.txt>.
- Kent, S. ve Atkinson, R. (1998), "IP Authentication Header", Internet Engineering Task Force, <http://www.ietf.org/rfc/rfc2402.txt>.
- Kent, S. ve Atkinson, R. (1998), "Security Architecture for the Internet Protocol", Internet Engineering Task Force, <http://www.ietf.org/rfc/rfc2401.txt>.
- Kuhn, R. ve Thomas, J. (2005), "Security Considerations for Voice Over IP", National Institute of Standards and Technology, Special Publication 800-58, Gaithersburg.
- Kultti, J. (2005), "Secure Text in SIP Based VoIP", Lulea University of Technology Department of Computer Science and Electrical Engineering, 2008:183 CIV
- Kurt, E., (2001), "Asimetrik Kriptografi", www.olympus.org/article/articleview/263/1/10
- Luthra, A. ve Ashraf, W. (2005), Security in VoIP Systems, Technical University of Denmark Informatics and Mathematical Modelling Building 321, DK-2800 Lyngby, Denmark.
- Orrblad, J. (2004), Alternatives to MIKEY/SRTP to secure VoIP (IKE/IPSEC and others), KTH Microelectronics and Information Technology, Stockholm.
- Porter, T., Baskin, B. ve Chaffin, L. (2006), Practical VoIP Security, Syngress Publishing, Inc. 800 Hingham Street Rockland, MA 02370.
- Rosenberg, J. ve Huitema, C. (2003), "STUN - Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs)", Internet Engineering Task Force, <http://www.ietf.org/rfc/rfc3489.txt>.
- Rosenberg, J. ve Schulzrinne, H. (2002), "An Offer/Answer Model with the Session Description Protocol (SDP)", Internet Engineering Task Force, <http://www.ietf.org/rfc/rfc3264.txt>.
- Schulzrinne, H. ve Rosenberg, J. (1998), "A comparison of SIP and H.323 for Internet telephony", In Proc. International Workshop on Network and Operating System Support for Digital Audio and Video (NOSSDAV), Cambridge, England.

Singhai, R ve Sahoo, A. (2002), “VoIP Security”, Kanwal Rekhi School of Information Technology, Indian Institute of Technology Bombay, Powai, Mumbai-400076.

Thalhammer, J.(2000), “Security inVoIP-Telephony Systems”, Institute for Applied Information Processing and Communication, Graz-Austria

Tübitak UEKAE (2006), “Açık Anahtar Altyapısı Eğitim Kitabı”, <http://www.kamusm.gov.tr/tr/Bilgideposu/Belgeler/teknik/aaa/index.html>

Won, Y. (2006), “VoIP Security and Privacy”, Global IPv6 Summit, Korea

ÖZGEÇMİŞ

Doğum tarihi 14.10.1982

Doğum yeri İstanbul

Lise 1996-1999 İstanbul Bahçelievler Lisesi

Lisans 1999-2004 Yıldız Teknik Üniversitesi Elektrik-Elektronik Fak.,
Elektronik ve Haberleşme Mühendisliği Bölümü.Yüksek Lisans 2004-2007 Yıldız Teknik Üniversitesi Fen Bilimleri Enstitüsü,
Elektronik ve Haberleşme Mühendisliği Anabilim Dalı,
Haberleşme Programı.**Çalıştığı kurumlar**

2005-2005 Netone Telekom A.Ş.

2005-2007 Karel Elektronik Sanayi ve Ticaret A.Ş.

2007- KoçNet Haberleşme A.Ş.

