



# VoIP Hacking & VoIP Güvenliđi

İ. Melih TAŞ

G. Eren AKÇA

Siber Güvenlik Konferansı, Ankara ODTÜ / 22 Aralık 2012

## Biz Kimiz?

- İ. Melih TAŞ  
NETAŞ ARGE / Yazılım Tasarım Mühendisi  
ICT & Güvenlik & Adli Bilişim Araştırmacısı  
Email: [meliht@netas.com.tr](mailto:meliht@netas.com.tr)
- G. Eren AKÇA  
NETAŞ ARGE / Yazılım Tasarım Mühendisi  
ICT Araştırmacısı  
Email: [eakca@netas.com.tr](mailto:eakca@netas.com.tr)
- NETAŞ
  - 44 yıldır bilgi ve iletişim teknolojileri geliştiriyor.
  - Yeni nesil teknolojiler (VoIP, SIP, IMS, NGN, IPTV,...)
  - Yakınsama (sabit, mobil / veri, ses, görüntü)
  - Türkiye’de yazılım ihracat lideri.
  - Probil’i satın aldı.

# AJANDA

## 1. Kısım:

- VoIP'e Giriş
- VoIP Güvenlik Saldırılarının Etkileri
- Saldırı Kategorileri
- VoIP Güvenliğinin Farklı Olmasının Nedenleri
- VoIP Güvenliği Efsaneleri
- VoIP ve IT Audit
- Yeni Nesil VoIP Güvenlik Cihazları
- Yaşanmış VoIP Fraud ve Outage Örnekleri

## VoIP'in Kısa Tarihi

- İlk IP telephony servisi 1995'te Vocaltec tarafından verilmiştir.
- İlk PC'den telefona arama 1998'de gerçekleştirilmiştir.
- Cisco, Nortel ve Lucent ilk VoIP switch'leri geliştirmişlerdir.
- 2000 yılında toplam ses trafiğinin %3'u VoIP trafiğidir.
- Bugün toplam ses trafiğinin %30'unun VoIP olduğu düşünülüyor.

## VoIP'in Tanımı

- Paket anahtarlamaalı IP ađı üzerinden ses grşmelerinin tařınmasıdır.
- Analog iřaretler sayısal iřaretlere dnřtrlp sıkıřtırılır, paketler blnerek IP ađı üzerinden alıcıya gnderilir ve alıcıda tekrar analog iřaretlere dnřtrlr.
- Tek bir IP ađı üzerinden veri, ses ve video iletimi sađlanır.

## VoIP Hacking'in Kısa Tarihi

- Geçmişte de telefon sistemleri hacker'ların hedefi olmuştur.
- Telefon hackleme = "Phreaking"
- Yaygın olarak 1970 – 1980'lerde başlıyor.
- Altkültür illegal yollardan telefon network'lerini kontrol etmeyi başarmış.
- Bazıları phreaking'i sadece hobi olarak görmüş, gerçekten zarar vermek değil.
- Diğerleri illegal yollardan uzak mesafe servislere erişmiş ve toll charge'ları bypass etmişler.
- Bazıları da sinsi işler çevirmiş. (Call diverting, rerouting, eavesdropping gibi)
- PSTN network'ündeki zaafiyetler VoIP network'ünde de var.

# VoIP'in Popüler Olmasının Sebepleri

- **Düşük Maliyet**
  - Donanım ve operasyon giderlerinin azalması
  - Toplam sahip olma maliyetinin azalması
- **Tümleşik İletişim (Unified Communication)**
  - Bilgisayar sistemleri ile yakınsama
  - Yeni servislerin ve uygulamaların eklenme kolaylığı
  - Yeni katma değerli çözümler (IPTV, video konferans, IMS, presence...)

## Ek Bilgi:

- Orta ölçekli ve büyük ölçekli işletmelerin %50'si, VoIP'in bazı formlarını benimsiyor. Büyük işletmelerin diğer yarısı ise, 5'ten fazla lokasyonda VoIP çözümlerini kullanıyorlar.
- Bugün yeni kurulan telefon sistemlerinin %80'i VoIP sistemidir.
- Ortalama olarak her 7 yılda bir şirketler telefon sistemlerini değiştirme gereği duyarlar.

# VoIP Protokolleri

- **Sinyalleşme Protokolleri:**
  - SIP, H.323, MGCP, H.248, SCCP (Cisco)
- **Media İletim Protokolleri:**
  - RTP, RTCP, SRTP (AES)

# VoIP Güvenlik Saldırılarının Etkileri

- **Residential (Skype, MSN, Yahoo Messenger, Google Talk...)**
  - Telekulak ile kimlik hırsızlığı, scam,...
  - Kritik servislere erişimi engelleme
- **Enterprise (Finans kurumları, Bankalar, Kamu kuruluşları, İşletmeler...)**
  - Kısa veya uzun süreli outage saldırıları (call center shutdown, müşteri servis kalitesinin düşmesi, SLA'ler)
  - Telekulak ile şirket gizli bilgilerinin sızdırılması, gelir kaybı riski
- **Business (Servis sağlayıcılar, Technology sağlayıcılar, Trafik taşımacılığı,...)**
  - Worm, virus saldırıları vb ile servis bozma ve SLA'lere etkisi
  - Kritik servis sağlayan SP'ler için yıkıcı düzeydeki riskler
  - İtibar kaybı, gelir kaybı riski
- **Government**
  - Araya girme yada sahte tavır ile ülke güvenliği ile ilgili gizli bilgilerin sızdırılması,
  - Vatandaşlık gizli bilgileri gibi hassas bilgilere erişim.

**NOT:** Email ile gönderirken şifreleme gereği duyduğunuz birçok önemli bilgi telefon görüşmelerinde güvensiz. (kredi kartı bilgileri, network altyapısı, şirket gizli bilgileri,...)

# Saldırı Kategorileri

- **Servis Bozma (DoS/DDoS)**
  - Telefonlar, proxy'ler ve router'lar hedef olabilir.
  - SIP/MGCP/H.323/RTP protokolleri kullanılabilir.
  - Edge-cihazları etkiler, sinyalleşme elementlerini overload eder ve band genişliğini tüketir.
- **Yetkisiz Erişim**
  - Abone cihazları, voice mail, email, DNS, DHCP server'lar gibi network elementleri
  - Servisler (SSH, HTTP,...)
  - Uygulamalar (SQL injection, CSS-CSRF,...)
  - Yönetim sistemleri, Provisioning sistemleri, Ücretlendirme sistemleri
- **Telekulak (Eavesdropping), Trafik Analizi ve Çağrı Kaydetme**
  - Sinyalleşme/media manipulasyonu, sahte tavr, registration çalma, kimlik hırsızlığı, IPTV içerik hırsızlığı/değiştirme
- **Fraud**
  - Sinyalleşme mesajları ve/veya çağrı akışı manipule edilebilir.
  - Call injection ile faturalara etki, şirket itibarını etkileyici aktiviteler (caller ID spoofing).
- **SPIT**

## VoIP Güvenliđinin Farklı Olmasının Nedenleri (1/4)

- VoIP güvenliđi gereksinimleri, data network'tekilere benzer iken, VoIP için bazı spesifik konular da vardır.

## VoIP Güvenliğinin Farklı Olmasının Nedenleri (2/4)

- **VoIP'in Gerçek-Zamanlı Doğası:**
  - VoIP gerçek-zamanlı bir servistir (eş-zamanlı ve time-kritik).
  - Herhangi bir bilgi kaybı recover edilemez, tekrarlanamaz.
  - Yüksek erişilebilirlik için otomatikleştirilmiş ve gerçek-zamanlı cevap gerektirir.
  - Data dünyasındaki outage durumları, VoIP söz konusu olduğunda kabul edilemez.
- **Yeni Donanım ve Bileşenler:**
  - Geniş bir alanda bileşen ve uygulamaları kapsar.
  - VoIP trafiği paketlenmiş ses formunda taşındığı için telekulak (eavesdropping), media manipülasyonu ve kimlik hırsızlığı gibi zararlı aktiviteler için potansiyel riskler vardır.

## VoIP Güvenliğinin Farklı Olmasının Nedenleri (3/4)

- **Yeni Tip Tehditler ve Yeni Teknolojiler:**
  - Toll Fraud, SPIT, servis hırsızlığı, kimlik hırsızlığı gibi yeni tip tehditler var.
  - VoWi-Fi, IMS, IPTV, konferans gibi teknolojiler ile yeni tip güvenlik sıkıntıları.
- **Gecikme , Paket Kaybı ve Jitter**
  - QoS parametrelerine yüksek duyarlılığı vardır.
  - Mevcut firewall ve NAT'lar çağrı kurulumlarını geciktirir yada bloke eder.
  - Şifreleme makinaları ek olarak jitter yapar.
  - IPS/IDS cihazları inspected paketler için ek olarak gecikmeye sebep olur.

## VoIP Güvenliğinin Farklı Olmasının Nedenleri (3/4)

- **Gateway'ler:**
  - Taşıyıcı IP network'leri ve TDM network'leri arasındaki internetworking için Media Gateway'ler gereklidir.
  - Network'ler arası güvenlik saldırıları (kritik PSTN network'lerinin güvenliği)
  - VoIP ve SS7 etkileşiminden doğacak yeni saldırı vektörleri

## VoIP Güvenliđi Efsaneleri (1/8)

- VoIP güvenlik ihtiyaçları geniş bir çevrede anlaşılmış iken henüz erken safhalarda.
- VoIP güvenliđi hala VoIP ve UC uygulamalarının bir bileşeni deđil.
- VoIP güvenliđini geliřtirmeyen birçok asılsız bilgi dolařıyor.

## VoIP Güvenliđi Efsaneleri (2/8)

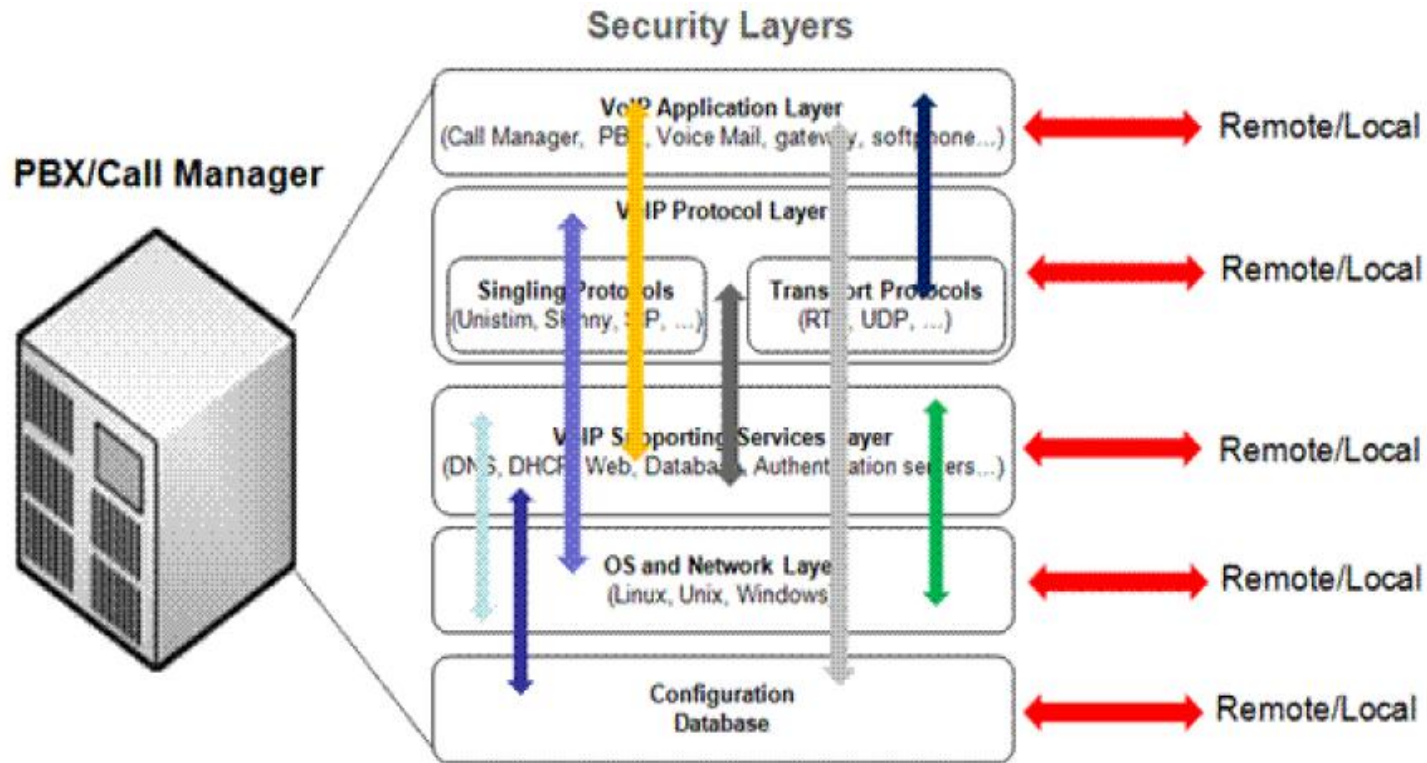
**1- PBX'im direk olarak PSTN network'e bađlı ve SIP/H.323 trunk kullanmıyorum.**

Hiçbir trunk'ının olmaması VoIP'in güvenli olduđu anlamına gelmez.

- VoIP'in çok katmanlı ve karmaşık bir yapısı vardır.
- IP trunk'lara nazaran PBX zaafiyetlerini exploit etmek için çok daha ilgi çekici vektör vardır.
- Saldırıları nerelere yapılabilir?
- Saldırıları nerelerden gelebilir?
- Sadece IPS/Firewall ile VoIP güvenliđi sağlamak geçerli bir çözüm değildir.

**Sonuç:** VoIP eninde sonunda PSTN'in yerini alacaktır. Şimdiden hazır olun.

# VoIP Güvenliği Efsaneleri (3/8)



## VoIP Güvenliđi Efsaneleri (4/8)

**2- VoIP'imiz VLAN altyapısı kullanılarak implemente edildi ve data network'ümüzden tamamen izole edildi.**

- VoIP deployment'daki VLAN rollerini hackleyebilecek hazır araçlar var.
- Softphone'ların gelmesi izolasyonu kırdı.
- Softphone'lar artık tamamen hardphone'ların yerini alacaktır.
- RTP'nin bypass edilmesi ve P2P mode çalışan endpoint'ler

**Sonuç:** VLAN, VoIP'inizi güvenli yapacak harika bir çözüm değildir.

## VoIP Güvenliđi Efsaneleri (5/8)

### 3- Data network'um üzerinde güçlü bir altyapım var ve VoIP onun bir parçası.

- VoIP sadece başka bir data uygulaması değildir.
- Sinyalleşme protokollerinin kendilerine özgü karakteristikleri vardır.
- Mevcut data güvenlik çözümleri VoIP spesifik zaafiyetler için dizayn edilmemiştir.
- RTP'nin bypass edilmesi ve RTP karakteristiđi
- QoS etkilerini minimize etmek gerekir.
- SPIT vs SPAM – SPIT çözülmesi çok zor bir problemdir.
- Güvenlik policy ve prosedürleri VoIP ve UC'yi kapsıyor mu?
- IT Güvenlikçiler vs Telekomcular
- Kullanıcı eğitimleri

**Sonuç:** VoIP, email ve web güvenliđi gibi görülmemelidir . Tedbir almalısınız.

## VoIP Güvenliđi Efsaneleri (6/8)

### 4- VoIP firewall ve SBC yükledim.

- Birbirine benzer fonksiyonları olan cihazlardır. Genellikle VoIP firewall kurumsal yapıda, SBC ise VoIP servis sağlayıcıların network'larında konumlandırılmıştır.
- SBC, SIP trafiđi yönetir, firewall ve NAT dönüşümü sağlar. Normal firewall'lar bu bilgileri göremezler.
- SBC'ye güvenlik sonradan eklenmiştir. İmza tabanlı motorları yoktur.
- Pahalı SBC'lerde anormallik tespiti vardır.

### Sonuç ve Öneriler:

- Çok katmanlı güvenlik mimarisi için ek güvenlik uygulama/cihazları lazım.
- Risk yönetimi yaklaşımı ile VoIP VA ve uyumluluk değerlendirme araçları gereklidir.
- Güvenlik politika ve prosedürleri VoIP'i kapsamalıdır.

## VoIP Güvenliđi Efsaneleri (7/8)

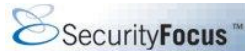
**5- X vendor'undan aldığım uygulamalar ve tescilli protokolleri kullanarak VoIP altyapımı deploy ettim. VoIP'imın tamamen güvenli olduğunu söylediler.**

- VoIP vendor'ları ile ilgili bilinen yüzlerce zaafiyetler var.
- Vendor'lar satış sonlana kadar güvenlikten hiç bahsetmezler.
- Data network'ündeki zaafiyetler, VoIP yapınızda exploit edilebilir yada tam tersi.

### **Sonuç ve Öneriler:**

- Risk analizi prosesi ile başlayın. Asset'lerinizi çıkarın.
- Risk alanlarını belirleyin ve minimize etme yollarını çıkarın.
- Lab ortamında VoIP VA gerçekleştirin. Kurulum sonrasında periyodik VoIP VA planlayın.
- Sonuçlar için uygun aksiyonları alın.
- VoIP'i tanıyan ve çok katmanlı güvenlik mimarisi uygulayın.

# VoIP Güvenliği Efsaneleri (8/8)


[About](#) [Contact](#)

## Symantec Connect

A technical community for Symantec customers, end-users, developers, and partners.

[Join the conversation](#)

### Vulnerabilities

Vendor:

Title:

Version:

### Search by CVE

CVE:

#### Asterisk SIP 'automon' NULL Pointer Dereference Denial Of Service Vulnerability

2011-12-08  
<http://www.securityfocus.com/bid/50989>

#### Asterisk SIP Endpoints NAT Settings User Enumeration Weakness

2011-12-08  
<http://www.securityfocus.com/bid/50990>

#### Asterisk Uninitialized Variable SIP Channel Driver Denial of Service Vulnerability

2011-11-15  
<http://www.securityfocus.com/bid/50177>

#### Asterisk Manager Interface Remote Denial of Service Vulnerability

2011-10-24  
<http://www.securityfocus.com/bid/46897>

#### Asterisk SIP Authentication Request User Enumeration Weakness

2011-10-24  
<http://www.securityfocus.com/bid/48485>

#### Asterisk Multiple Remote Denial of Service Vulnerabilities

2011-10-24  
<http://www.securityfocus.com/bid/48431>

#### Asterisk UPDTL Packets Buffer Overflow Vulnerabilities

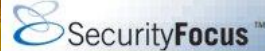
2011-10-24  
<http://www.securityfocus.com/bid/46474>

#### Asterisk Manager Interface Arbitrary Command Execution Security Bypass

2011-10-24  
<http://www.securityfocus.com/bid/47537>

#### Asterisk TCP/TLS Server NULL Pointer Dereference Denial Of Service Vulnerability

2011-10-24


[About](#) [Contact](#)

## Symantec Connect

A technical community for Symantec customers, end-users, developers, and partners.

[Join the conversation](#)

### Vulnerabilities

(Page 1 of 2) 1 2 [Next >](#)

Vendor:

Title:

Version:

### Search by CVE

CVE:

#### OpenSSL PKCS Padding RSA Signature Forgery Vulnerability

2011-05-09  
<http://www.securityfocus.com/bid/19849>

#### OpenSSL SSLv2 Null Pointer Dereference Client Denial of Service Vulnerability

2011-05-09  
<http://www.securityfocus.com/bid/20246>

#### OpenSSL ASN.1 Structures Denial of Service Vulnerability

2011-05-09  
<http://www.securityfocus.com/bid/20248>

#### OpenSSL Public Key Processing Denial of Service Vulnerability

2011-05-09  
<http://www.securityfocus.com/bid/20247>

#### OpenSSL SSL\_Get\_Shared\_Ciphers Buffer Overflow Vulnerability

2011-05-09  
<http://www.securityfocus.com/bid/20249>

#### MS Index Server and Indexing Service ISAPI Extension Buffer Overflow Vulnerability

2009-11-26  
<http://www.securityfocus.com/bid/2880>

#### Cisco Voice Product IBM Director Agent Port Scan Denial Of Service Vulnerability

2009-07-12  
<http://www.securityfocus.com/bid/9469>

#### Cisco Voice Product IBM Director Agent Unauthorized Remote Administrative Access Vulnerability

2009-07-12  
<http://www.securityfocus.com/bid/9468>

#### Microsoft Windows Workstation Service Remote Buffer Overflow Vulnerability

2009-07-12

## VoIP ve IT Audit (1/3)

### Denetçiler değerlendirmek için yeni elementler eklemeye başlamışlardır:

- VoIP deployment'ın doğası
- Çağrı cevaplama ünitesinin nasıl olduğu – finansal kurumların telefon bankacılığı sistemi
- VoIP operasyon ve konfigürasyon değişikliklerini yönetmek için policy ve prosedürlerin olup olmadığı
- Voice-Data network topolojisinde exploit edilebilecek gap'ler olup olmadığı

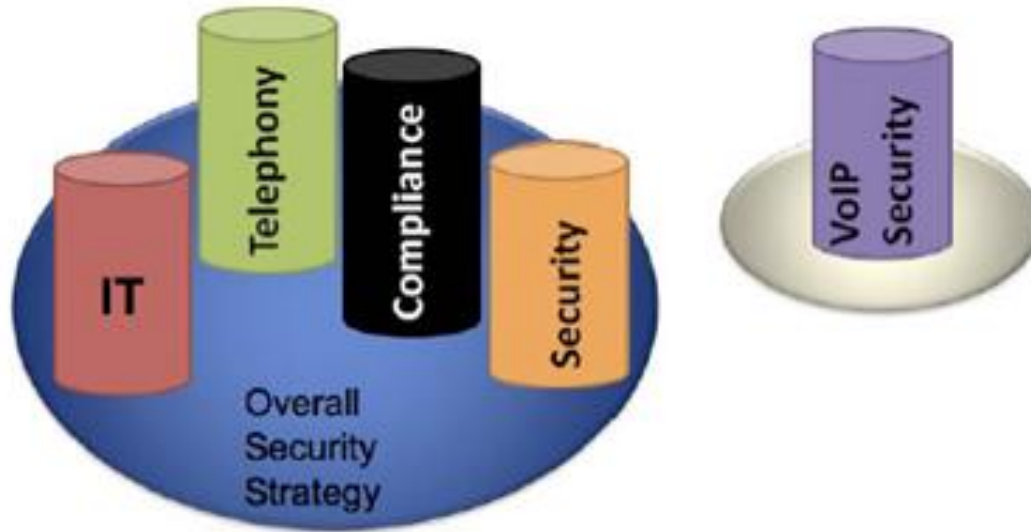
## VoIP ve IT Audit (2/3)

### **VoIP güvenlik riskini minimize etmek ve compliance gereksinimlerinizi hazırlamak için:**

- VoIP mimariyi güvenlik bakış açısıyla gözden geçirin.
- VoIP spesifik VA ve pen-test yapın. Raporlanan zafiyetleri tedavi edin.
- VoIP için regülasyon gereksinimlerinizi tespit edip inceleyin. VoIP güvenliğini audit ve compliance raporlamasına dahil edin.
- VoIP tehdit farkındalığı için çalışanların eğitimlerini yürütün, güvenlik takımınıza VoIP uzmanlığını kazandırın.
- Görevler arası toplantılar düzenleyin. (network, telekom, güvenlik ve audit departmanları dahil olsun ve ortaklaşa VoIP güvenlik koruması ve mitigation stratejileri planlayın.)

## VoIP ve IT Audit (3/3)

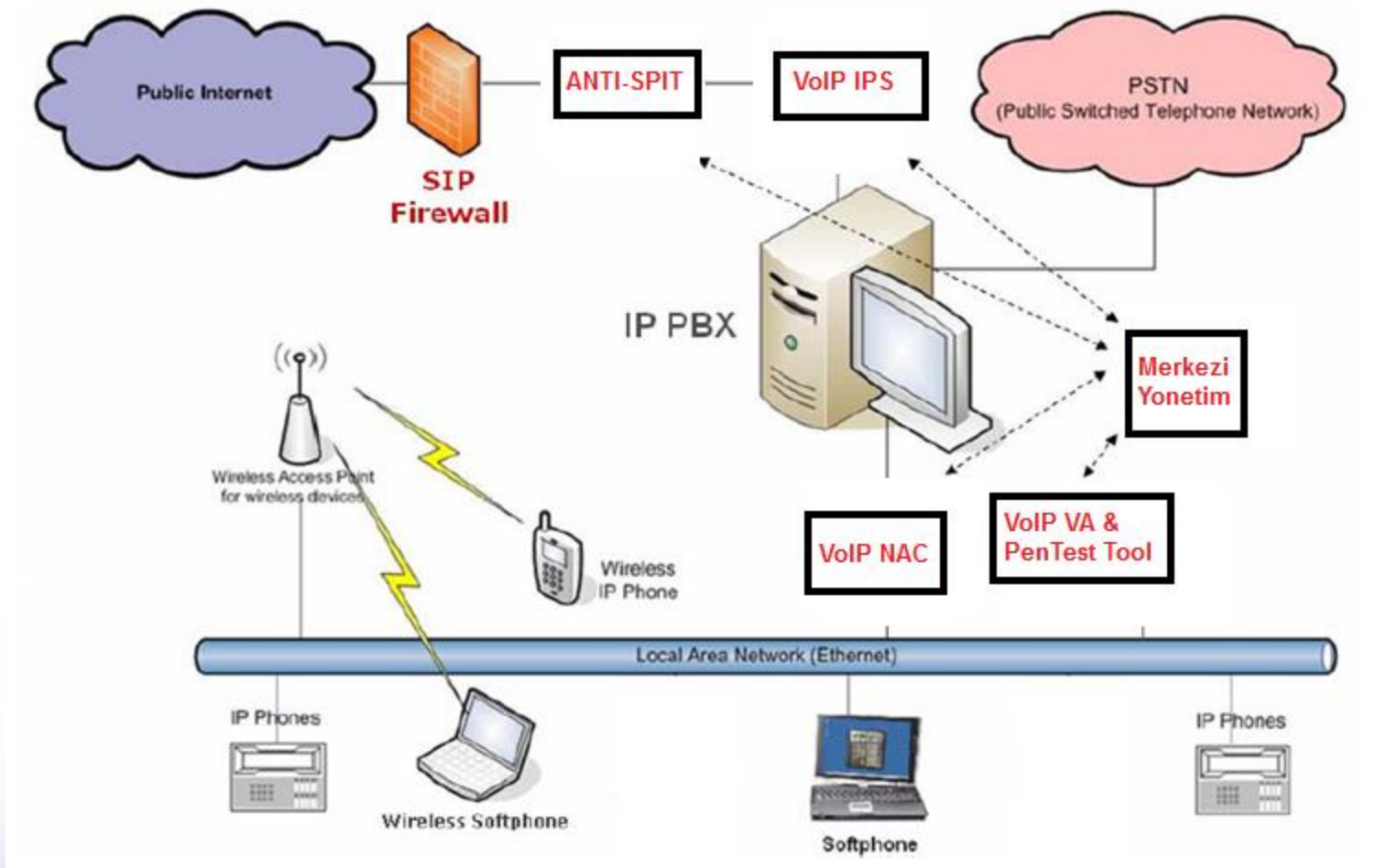
- Finansal kurumlar ve organizasyonlar, VoIP teknolojisi hızla yayıldığı ve ihlallerin de hızla çoğalması ile uçtan uca network güvenlik stratejilerinin bir parçası olarak VoIP'i dikkate almalıdırlar.



## Yeni Nesil VoIP Güvenlik Cihazları (1/2)

- **VoIP VA & PenTest Tool:** Zaafiyet analizi ve penetrasyon test aracı. VoIP network'ündeki tüm cihazları tarar ve potansiyel güvenlik tehlikelerini tanımlar. VoIP network'ünün sağlığını gösteren birden fazla rapor ve grafik üretir.
- **VoIP NAC:** Network Access Control uygulaması. Yetkilendirme yapar, VoIP network'une bağlanmaya çalışan her cihazı zafiyetler için inceler.
- **VoIP IPS:** Intrusion Prevention System'idir. PBX'e gelen ve PBX'den çıkan tüm trafiği inceler ve zararlı aktiviteleri durdurur.
- **Anti-SPIT:** Anti-SPIT (Spam over Internet Telephony) uygulaması. SPIT sesli mesajları tanır ve siler.
- **Merkezi Yönetim:** Enterprise network'ündeki tüm VoIP uygulamalarının yönetildiği ve konfigüre edildiği yönetim konsoludur.

## Yeni Nesil VoIP Güvenlik Cihazları (2/2)



-Yeni nesil VoIP ürünleri ile birlikte enterprise network şeması-

## Yaşanmış VoIP Fraud Olayları

- 11 milyon Euro zarara uğratan VoIP Fraud Çetesi Romanya'da yakalandı.  
*Softpedia News – Aralık 2010*
- 10 milyon dakika hijack edildi. (Amerika)  
*The Register – Sep 2010*
- Hacker'ların %98'i aynı zamanda phreaking yaparak iş dünyasını etkiliyorlar.  
*Telecommunications UK Fraud Forum - Şubat 2010*

Benim başıma gelmez demeyin!

## Yaşanmış VoIP Outage Olayları

- Ooma (Ağustos 2011): US-based VoIP service provider Ooma, datacenter'larında DDoS'tan dolayı 3 saat boyunca outage yaşadı. Tüm inbound ve outbound çağrılar etkilendi. Hem telefon network'u hem de şirket sitesi hacklendi.
  - *Daha önce 2010, 2009 (6 saat) yılında da network outage yaşamışlar.*
- AT&T (Mayıs 2010): U-verse VoIP servisinde major outage yaşandı. 5 saat boyunca 1 milyondan fazla kullanıcı etkilendi. Servis güvenilirliği etkilendi. Outage nedeni ile ilgili açıklama yapılmadı.
- Skype (Haziran 2011): 170 milyon kullanıcısı etkilendi. Konfigürasyon problemi olduğu açıklandı.
  - *1 hafta oncesinde Rus hacker Skype protokol kodlarını internette paylaşmıştı.*



## 2. Kısım

- En Bilinen VoIP Zaafiyetleri
- Saldırı Örnekleri
- Bir Saldırının Anatomisi
- VoIP Güvenlik Araçları
- Ek Bilgiler

# En Bilinen VoIP Zaafiyetleri

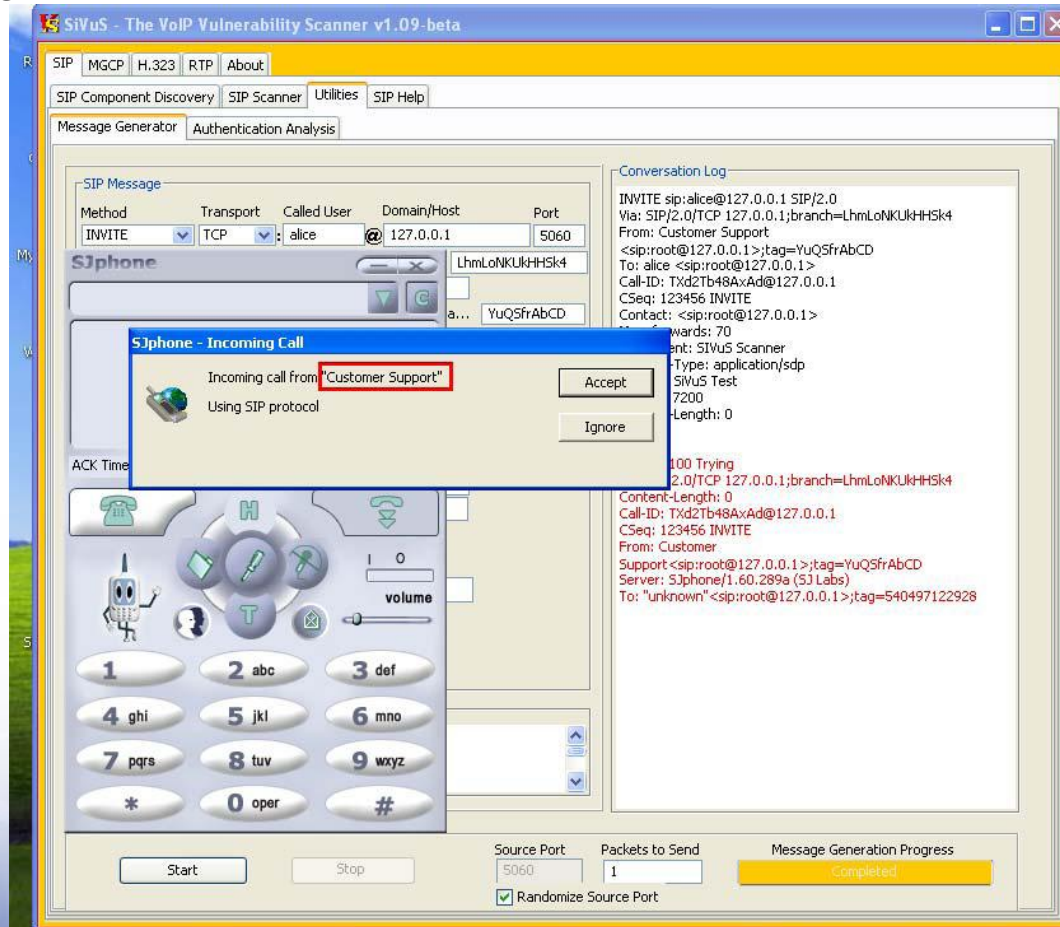
1. Yetersiz data verifikasyonu
2. Execution açıkları
3. String/array/pointer manipulasyon açıkları
4. Düşük kaynaklar (işlemci, memory)
5. Düşük band genişliği
6. Dosya/kaynak manipulasyon açıkları
7. Şifre yönetimi
8. İzinler ve öncelikler
9. Krypto
10. Yetkilendirme ve sertifika hataları
11. Hata kontrolü
12. Homojen network
13. Fallback sistem eksikliği
14. Fiziksel bağlantı kalitesi ve paket çakışması

# Saldırı Örnekleri

- Caller-ID Spoofing
- Presence Hijacking
- Eavesdropping (Telekulak)

# Sivus ile Spoofing Caller-ID

- FROM header bilgisini manipule et
- Telefonlara INVITE gönder



## Saldırılar – Presence Hijacking

- Presence Hijacking/SIP kullanarak masquerading (sahte tavır) saldırı
- REGISTER request'i spoof etmek
- REGISTER request "Contact:" header'ında SIP cihazının adresi belirtilir.

# Sivus ile Presence Hijacking – Regular Register Request

Frame 1 (611 bytes on wire, 611 bytes captured)

Ethernet II, Src: 00:12:17:e5:7e:00, Dst: 00:05:00:e5:6b:00

Internet Protocol, Src Addr: 192.168.1.5 (192.168.1.5), Dst Addr: 192.168.1.2 (192.168.1.2)

User Datagram Protocol, Src Port: 5061 (5061), Dst Port: 5061 (5061)

Session Initiation Protocol

**Request-Line: REGISTER sip:atlas4.voipprovider.net:5061 SIP/2.0**

Method: REGISTER  
Resent Packet: False

Message Header

Via: SIP/2.0/UDP 192.168.1.5:5061;branch=z9hG4bK-49897e4e

**From: 201-853-0102 <sip:12018530102@atlas4.voipprovider.net:5061>;tag=802030536f050c56o0**  
SIP Display info: 201-853-0102  
SIP from address: sip:12018530102@atlas4.voipprovider.net:5061  
SIP tag: 802030536f050c56o0

**To: 201-853-0102 <sip:12018530102@atlas4.voipprovider.net:5061>**  
SIP Display info: 201-853-0102  
SIP to address: sip:12018530102@atlas4.voipprovider.net:5061

Call-ID: e4bb5007-b7335032@192.168.1.5  
CSeq: 3 REGISTER  
Max-Forwards: 70

**Contact: 201-853-0102 <sip:12018530102@192.168.10.5:5061>;expires=60**

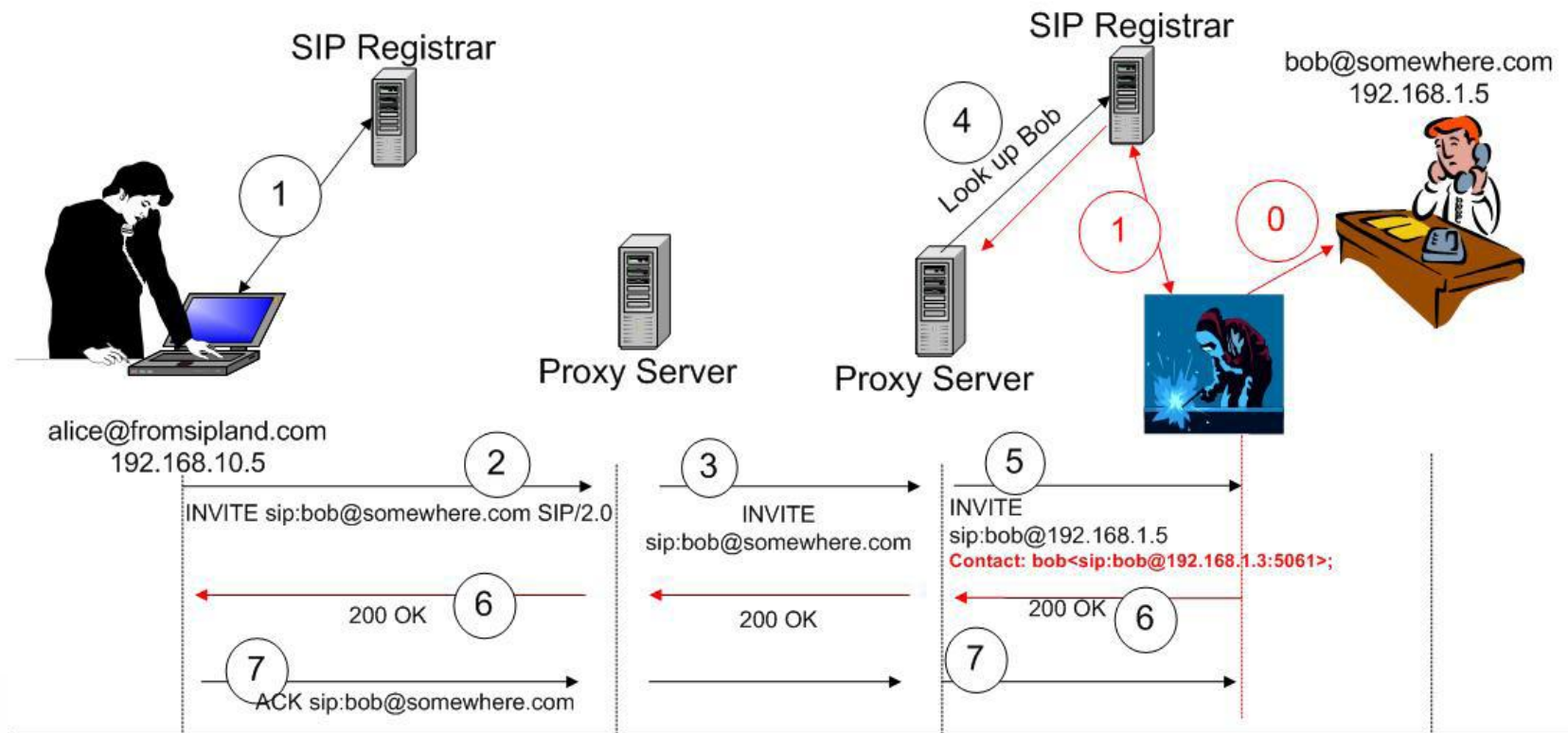
User-Agent: 001217E57E31 Linksys/RT31P2-2.0.13(LIVD)  
Content-Length: 0  
Allow: ACK, BYE, CANCEL, INFO, INVITE, NOTIFY, OPTIONS, REFER  
Supported: x-sipura

Request to REGISTER and announce contact address for the user. In the REGISTER request the From and To headers must use the same user information.

Indicates that the registration will expire in 60 seconds. Another REGISTER Request should be sent to refresh the user's registration.

The Contact header contains a SIP or SIPS URI that represents a direct route to the device, usually composed of a username at a fully qualified domain name (FQDN).

# Bir Saldırının Yapısı



- 0 – DoS Attack
- 1 – User Registration
- 2 – Caller - Session Initiation Request
- 3 – Proxy - Domain look up and routing
- 4 – Proxy - user lookup (SIP Proxy retrieves the attacker's IP address)
- 5 – Proxy - Proxy contacts user
- 6 – Callee answers
- 7 – Proxy forwards caller response – The connection has been established and media is routed between the two phones.

# Manipule edilmiş REGISTER request özellikleri

IP address of the VoIP device on which a POTS phone is attached

```
REGISTER sip:216.1.2.5 SIP/2.0  
Via: SIP/2.0/UDP 192.168.1.6;branch=xajB6FLTEHlcd0  
From: 732-835-0102 <sip:12125550102@voip-service-provider.net:5061>;tag=5e374a8bad1f7c5x1  
To: 732-835-0102 <sip:12125550102@voip-service-provider.net:5061>  
Call-ID: QTEv5G5dOHYc@192.168.1.2  
CSeq: 123456 REGISTER
```

```
Contact: 2125550102 <sip:12125550102@192.168.1.3:5061>;  
Digest username="12125550102",realm="216.1.2.5",nonce="716917624",  
uri="sip:voip-service-provider.net:5061",algorithm=MD5,  
response="43e001d2ef807f1e2c96e78adfd50bf7"
```

```
Max_forwards: 70
```

```
User Agent: 001217E57E31 VoIP-Router/RT31P2-2.0.13(LIVd)
```

```
Content-Type: application/sdp
```

```
Subject: SiVuS Test
```

```
Expires: 7200
```

```
Content-Length: 0
```

IP address that calls will be routed to (attacker)

Authentication MD5 digest can be intercepted and used to replay messages

# Sivus ile Presence Hijacking – The register message

The screenshot displays the SiVuS - The VoIP Vulnerability Scanner v1.09-beta interface. The main window is titled "SIP Message" and contains several fields for configuring a SIP REGISTER message. The "Method" is set to "REGISTER", "Transport" to "UDP", "Called User" to "alice", and "Domain/Host" to "atlas4.voipprovider.net". The "Port" is set to "5061". The "Via" field is "SIP/2.0/UDP 192.168.1.5", "Branch" is "z9hG4bK-49897e4e", "To" is "2018530102 <sip:root@192.168.1.5>", "From" is "2018530102 <sip:root@192.168.1.5>; tag=3536f050c56o0", "Authentication" is "nonce=43e001d2ef807f1e2c96e78adfd50bf7", "Call-ID" is "pQbYd9KY6ktV@192.168.1.5", "Cseq" is "123456 REGISTER", "Contact" is "2018530102<sip:2018530102@192.168.1.3>", "Record-Route" is empty, "Subject" is "SiVuS Test", "Content-type" is "application/sdp", "User Agent" is "001217E57E31 Linksys/RT31P2-2.0.13(LIVd)", "Expires" is "7200", and "Max-Forwards" is "70". There is a checkbox for "Use SDP?". Below the main fields is an "SDP message" field containing "v=0", "o=user 29739 7272939 IN IP4 192.168.1.2", and "s=". To the right of the main fields is a "Conversation Log" section showing a "REGISTER sip:192.168.1.2 SIP/2.0" message with its headers and body. At the bottom of the window, there are "Start" and "Stop" buttons, a "Source Port" field set to "5061", a "Packets to Send" field set to "1", and a "Message Generation Progress" bar labeled "Completed". A checkbox for "Randomize Source Port" is checked. A footer note states "Generates single SIP messages using various parameters".

SiVuS - The VoIP Vulnerability Scanner v1.09-beta

SIP MGCPC H.323 RTP About

SIP Component Discovery SIP Scanner Utilities SIP Help

Message Generator Authentication Analysis

SIP Message

Method	Transport	Called User	Domain/Host	Port
REGISTER	UDP	alice	@atlas4.voipprovider.net	5061

Via: SIP/2.0/UDP 192.168.1.5 Branch z9hG4bK-49897e4e

To: 2018530102 <sip:root@192.168.1.5>

From: 2018530102 <sip:root@192.168.1.5>; tag=3536f050c56o0

Authentication: nonce=43e001d2ef807f1e2c96e78adfd50bf7

Call-ID: pQbYd9KY6ktV@192.168.1.5

Cseq: 123456 REGISTER

Contact: 2018530102<sip:2018530102@192.168.1.3>

Record-Route:

Subject: SiVuS Test

Content-type: application/sdp

User Agent: 001217E57E31 Linksys/RT31P2-2.0.13(LIVd)

Expires: 7200 Max-Forwards: 70

Event:

Refer-To:

Content Length: 0

Use SDP?

SDP message

```
v=0
o=user 29739 7272939 IN IP4 192.168.1.2
s=
```

Conversation Log

```
REGISTER sip:192.168.1.2 SIP/2.0
Via: SIP/2.0/UDP 192.168.1.5;branch=z9hG4bK-49897e4e
From: 2018530102
<sip:root@192.168.1.5>;tag=802030536f050c56o0
To: 2018530102 <sip:root@192.168.1.5>
Call-ID: pQbYd9KY6ktV@192.168.1.5
CSeq: 123456 REGISTER
Contact: 2018530102<sip:2018530102@192.168.1.3>
"2018530102",realm="192.168.1.0",nonce="716917624",uri="sip
:atlas4.voipprovider.net:5061",algorithm=MD5,response="43e00
1d2ef807f1e2c96e78adfd50bf7"
Max_forwards: 70
User Agent: 001217E57E31 Linksys/RT31P2-2.0.13(LIVd)
Content-Type: application/sdp
Subject: SiVuS Test
Expires: 7200
Content-Length: 0

SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.168.1.5;branch=z9hG4bK-49897e4e
From: 2018530102
<sip:2018530102@atlas4.voipprovider.net:5061>;tag=8020305
36f050c56o0
To: 2018530102<sip:
2018530102@atlas4.voipprovider.net:5061>
Call-ID: pQbYd9KY6ktV@192.168.1.5
CSeq: 123456 REGISTER
Contact: 2018530102<sip:
2018530102@192.168.1.3:5061>;expires=20
Content-Length: 0
```

Start Stop

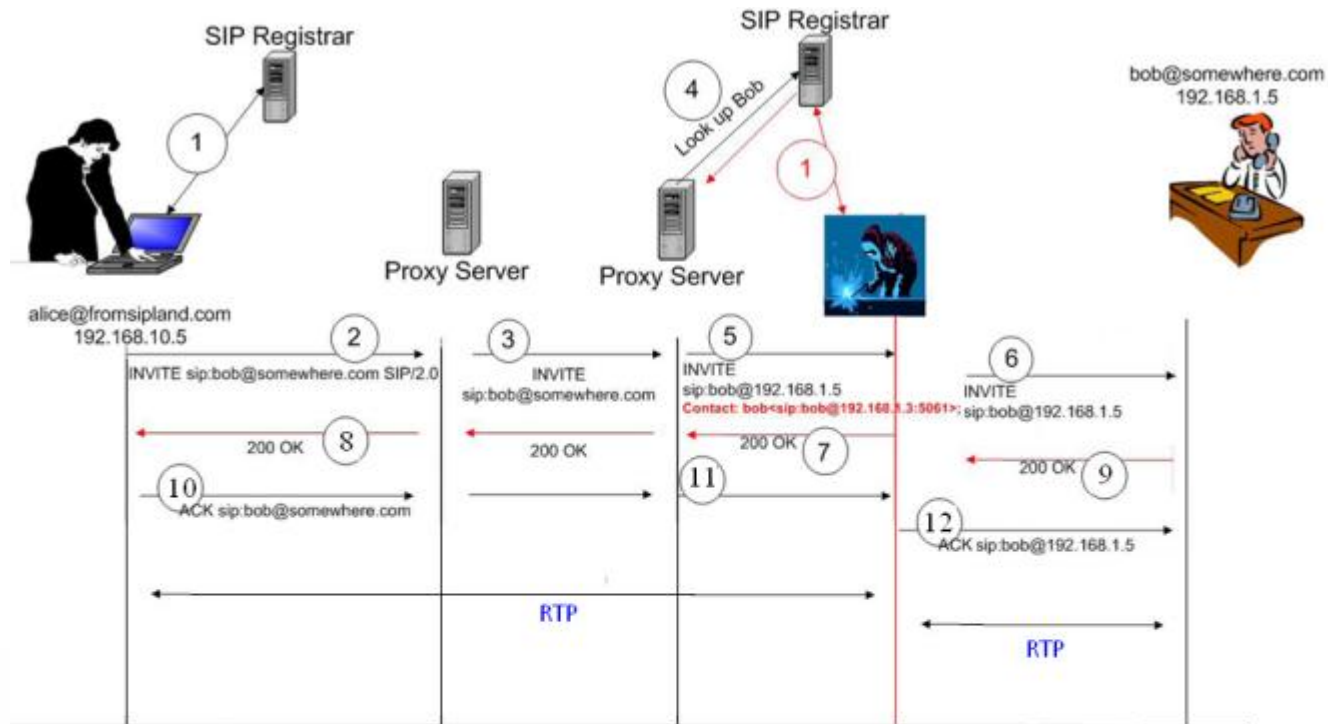
Source Port 5061 Packets to Send 1 Message Generation Progress Completed

Randomize Source Port

Generates single SIP messages using various parameters

# Saldırılar – Eavesdropping (Telekulak)

- Wireshark ile görüşmeyi decode etmek



- 1 - User Registration
- 2 - Caller - Session Initiation request
- 3 - Proxy - Domain look up and routing
- 4 - Proxy - user lookup (SIP Proxy retrieves the attacker's IP address)
- 5 - Proxy contacts attacker
- 6 - Attacker initiates a second call to the victim
- 7 - Attacker answers
- 8 - Proxy forwards 200 OK
- 9 - Victim answers call of the attacker
- 10 - Proxy forward caller response
- 11 - Attacker receives ACK from Caller, connection and media is established for first call.
- 12 - Connection between attacker and victim is established. Attacker can now redirect RTP packets between each call and capture them for eavesdropping purposes.

# Wireshark ile Eavesdropping (1/4)

The screenshot shows the Wireshark interface with a packet capture of an RTP stream. The packet list pane shows a list of packets, with the selected packet (No. 690) expanded in the packet details pane. The packet details pane shows the following structure:

- Frame 1 (326 bytes on wire)
- Ethernet II, Src: Cisco-Li
- Internet Protocol, Src: 19
- User Datagram Protocol, Sr
- Hypertext Transfer Protoco
- BOOTP-DHCP...
- Destinations...
- Flow Graph...
- HTTP
- IP address...
- ISUP Messages...
- Multicast Streams
- ONC-RPC Programs
- Packet Length...
- Port Type...
- TCP Stream Graph

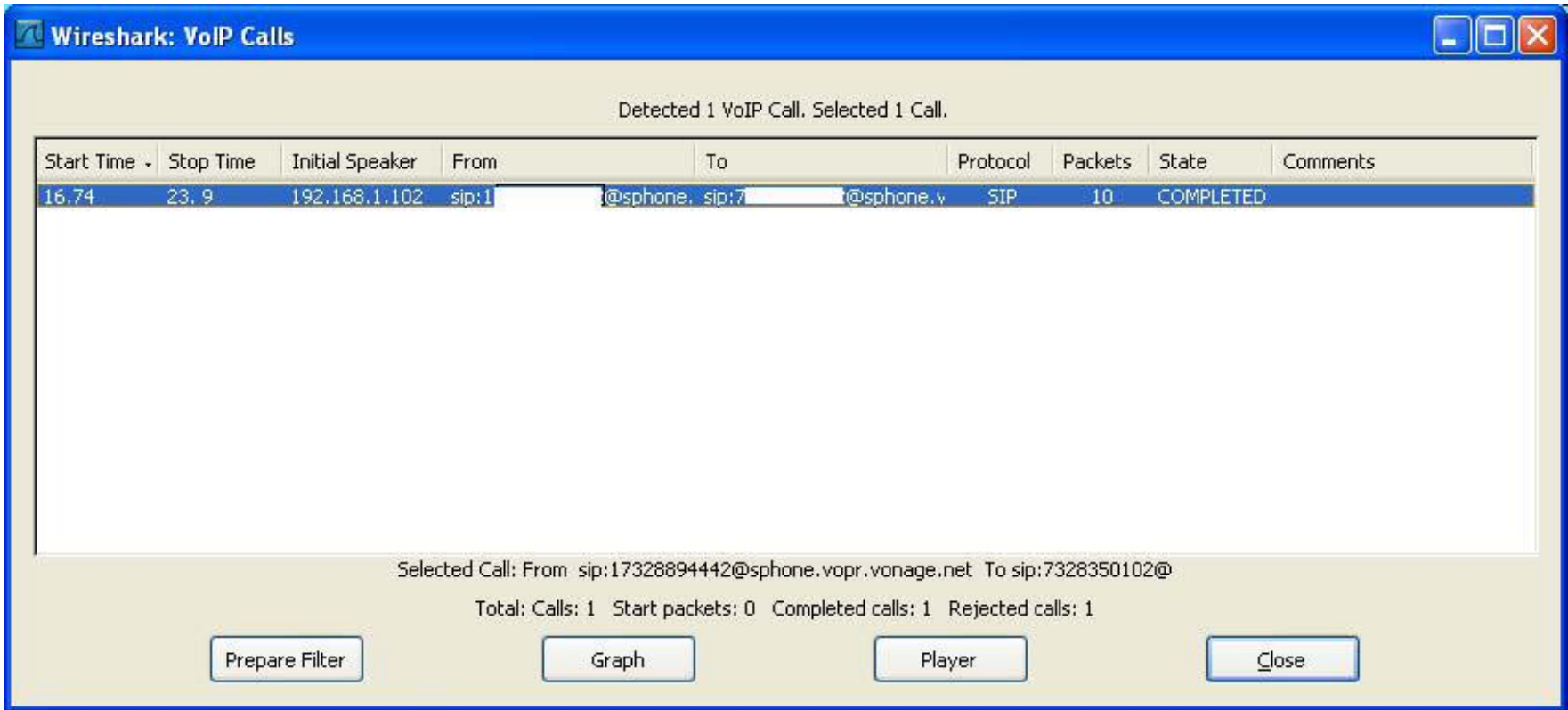
The packet bytes pane shows the raw data of the selected packet, which is an RTP payload. The data is displayed in hexadecimal and ASCII format. The ASCII portion of the data is as follows:

```

0000 01 00 5e 7f ff fa 00 18 f8 dd 2b 27 08 00 45 00 ..^.....+'.E.
0010 01 38 f1 86 00 01 11 15 8b c0 a8 01 01 ef ff .8.....
0020 ff fa 04 09 07 6c 01 24 fc 83 4e 4f 54 49 46 59 .....l.$..NOTIFY
0030 20 2a 20 48 54 50 2f 31 2e 31 0d 0a 48 4f 53 * HTTP/ 1.1..HOS
0040 54 3a 20 32 33 39 2e 32 35 35 2e 32 35 35 2e 32 T: 239.2 55.255.2
0050 35 30 3a 31 39 30 30 0d 0a 43 41 43 48 45 2d 43 50:1900..CACHE-C
0060 4f 4e 54 52 4f 4c 3a 20 6d 61 78 2d 61 67 65 20 ONTROL: max-age
0070 3d 20 31 32 36 0d 0a 4c 4f 43 41 54 49 4f 4e 3a = 126..L OCATION:
0080 20 68 74 74 70 3a 2f 2f 31 39 32 2e 31 36 38 2e http:// 192.168.
0090 31 2e 31 3a 32 38 36 39 2f 49 47 61 74 65 77 61 1.1:2869 /IGatwa
00a0 79 44 65 76 69 63 65 44 65 73 63 44 6f 63 0d 0a ydeviceD escDoc..
00b0 4e 54 3a 20 75 70 6e 70 3a 72 6f 6f 74 64 65 76 NT: upnp :rootdev
00c0 69 63 65 0d 0a 4e 54 53 3a 20 73 73 64 70 3a 61 ice..NTS : sspdp:a
    
```

The status bar at the bottom of the interface shows the current file path and statistics: "File: 'C:\DOCUME~1\PETER~1\LOCAL5~1\Temp\etherXXX\04364' 152 KB 00:00:25" and "P: 731 D: 731 M: 0 Drops: 0".

# Wireshark ile Eavesdropping (2/4)



Wireshark: VoIP Calls

Detected 1 VoIP Call. Selected 1 Call.

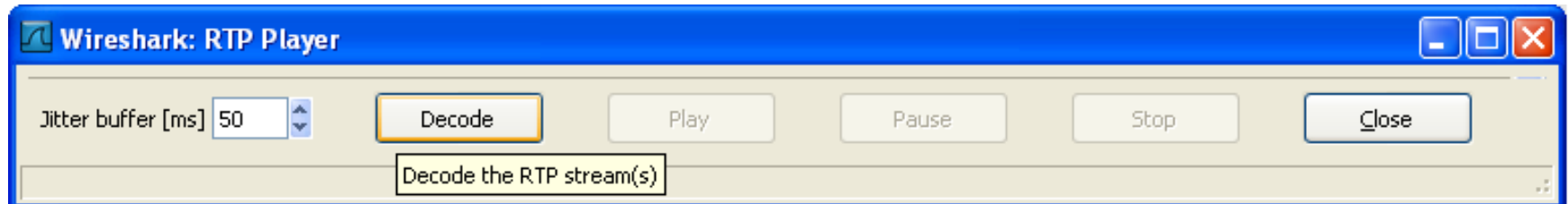
Start Time	Stop Time	Initial Speaker	From	To	Protocol	Packets	State	Comments
16.74	23.9	192.168.1.102	sip:1	@sphone. sip:7	@sphone.v	SIP	10	COMPLETED

Selected Call: From sip:17328894442@sphone.vopr.vonage.net To sip:7328350102@

Total: Calls: 1 Start packets: 0 Completed calls: 1 Rejected calls: 1

Prepare Filter Graph Player Close

# Wireshark ile Eavesdropping (3/4)



# Wireshark ile Eavesdropping (4/4)

The screenshot displays the 'Wireshark: RTP Player' window. It features two audio waveform visualizations on a green background. The top waveform is muted, indicated by a small speaker icon with a slash. The bottom waveform is active. Below each waveform is a playback control bar with a progress slider. The top bar shows a range from 173:12786 to 192.168.1.102:45200 with a duration of 3.34 seconds. The bottom bar shows a range from 192.168.1.102:45200 to 173:12786 with a duration of 3.90 seconds. At the bottom of the window, there is a 'Jitter buffer [ms]' field set to 50, and buttons for 'Decode', 'Play', 'Pause', 'Stop', and 'Close'. A tooltip 'Play the RTP channel(s)' is visible over the 'Play' button.

Wireshark: RTP Player

From 173:12786 to 192.168.1.102:45200 Duration:3.34 Drop by Jitter Buff:0(0.0%) Out of Seq: 0(0.0%)

From 192.168.1.102:45200 to 173:12786 Duration:3.90 Drop by Jitter Buff:0(0.0%) Out of Seq: 0(0.0%)

Jitter buffer [ms] 50

Decode Play Pause Stop Close

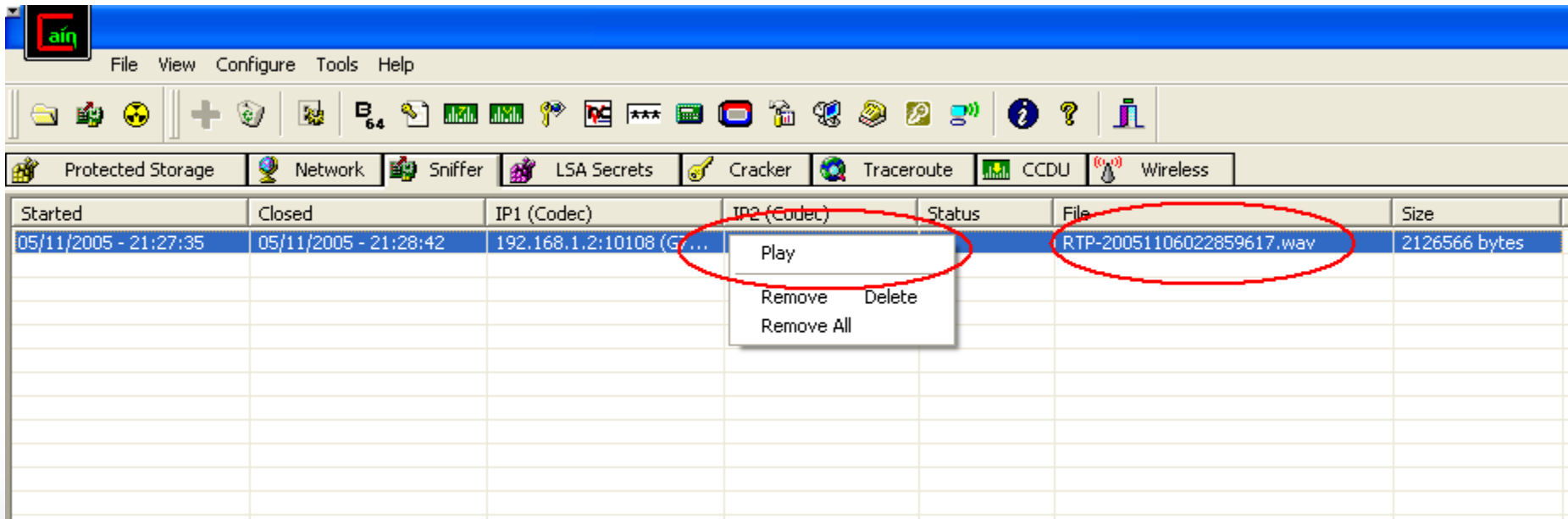
Play the RTP channel(s)

# Sonuç



# Cain & Abel ile Eavesdropping

- Network sniffer'i aktif et
- MITM saldırısı yapmak için ARP spoofing kullan ve SIP/RTP trafiği capture et.



## VoIP Güvenlik Araçları – Eavesdropping (1/3)

- Wireshark – Formerly Ethereal, the premier multi-platform network traffic analyzer. <http://www.wireshark.org>
- Authtool – Tool that attempts to determine the password of a user by analyzing SIP traffic. [http://hackingvoip.com/sec\\_tools.html](http://hackingvoip.com/sec_tools.html)
- Cain & Abel – Multi purpose tool with the capability to reconstruct RTP media calls. <http://www.oxid.it/cain.html>
- Etherpeek-VX – VoIP Sniffer.  
<http://www.wildpackets.com/products/erherpeek/overview>
- <http://www.voipsa.org/Resources/tools.php>

## VoIP Güvenlik Araçları – Eavesdropping (2/3)

- Oreka – Oreka is a modular and cross-platform system for recording and retrieval of audio streams. <http://oreka.sourceforge.net>
- PSIPDump – psipdump is a tool for dumping SIP sessions (+RTP traffic, if available) from pcap to disk in a fashion similar to “tcpdump -w”.  
<http://sourceforge.net/projects/psipdump>
- SIPomatic – SIP listener that's part of LinPhone.  
<http://www.linphone.org/?lang=us&rubrique=1>
- VoiPong – VoiPong is a utility which detects all VoIP calls on a pipeline, and for those which are G711 encoded, dumps actual conversation to separate wave files. It supports SIP, H.323, Cisco's Skinny Client Protocol, RTP and RTCP.  
<http://www.enderunix.org/voipong/index.php>

## VoIP Güvenlik Araçları – Eavesdropping (3/3)

- VoiPong ISO Bootable – Bootable “Live CD” disc version of VoiPong.  
<http://www.enderunix.org/voipong/manual/usage-livecd.html>
- VOMIT – The VOMIT utility converts a Cisco IP Phone conversation into a wave file that can be played with ordinary sound players. <http://vomit.xtdnet.nl>
- NetDude – A framework for inspection, analysis and manipulation of tcpdump trace files. <http://netdude.sourceforge.net>

## VoIP Güvenlik Araçları – Scanning ve Enumeration (1/3)

- EnumIAX- An IAX2 (Asterisk) login enumerator using REGREQ messages.  
<http://sourceforge.net/projects/enumiax/>
- iWar- IAX2 protocol Wardialer. <http://www.softwink.com/iwar/>
- SIP Forum Test Framework (SFTF)- The SIP Forum Test Framework (SFTF) was created to allow SIP device vendors to test their devices for common errors.  
<https://www.sipfoundry.org/sftf>

## VoIP Güvenlik Araçları – Scanning ve Enumeration (2/3)

- SIP-Scan- A fast SIP network scanner. <http://skora.net/voip/voip.html>
- SIPcrack- SIPcrack is a SIP protocol login cracker. It contains 2 programs, SIPdumpto sniff SIP logins over the network and SIPcrack to bruteforce the passwords of the sniffed login. <http://remote-exploit.org/index.php/Sipcrack>
- SIPSCAN- SIPSCAN is a SIP username enumerator that uses INVITE, REGISTER, and OPTIONS methods. [http://www.hackingvoip.com/sec\\_tools.html](http://www.hackingvoip.com/sec_tools.html)
- SiVuS- A SIP Vulnerability Scanner. <http://www.vopsecurity.org/html/tools.html>

## VoIP Güvenlik Araçları – Scanning ve Enumeration (3/3)

- SMAP- SIP Stack Fingerprinting Scanner.  
<http://www.wormulon.net/index.php?/archives/1159-smap-0.4.1-released.html>
- VLANping- VLANPingis a network pinging utility that can work with a VLAN tag.  
[http://www.hackingvoip.com/sec\\_tools.html](http://www.hackingvoip.com/sec_tools.html)
- VoIPAudit- VoIP specific scanning and vulnerability scanner.  
<http://www.voipshield.com>

## Packet Generation / Flooding (1/2)

- SiVuS – [www.vopsecurity.org](http://www.vopsecurity.org)
- IAXFlooder- A packet flooder that creates IAX packets.  
[http://www.hackingvoip.com/sec\\_tools.html](http://www.hackingvoip.com/sec_tools.html)
- INVITE Flooder- Send a flurry of SIP INVITE messages to a phone or proxy.
- Kphone- DDOS-Using KPhonefor flooding attacks with spoofed SIP packets.  
<http://skora.net/voip/voip.html>
- RTP Flooder - Creates "well formed" RTP Packets that can flood a phone or proxy. [http://www.hackingvoip.com/sec\\_tools.html](http://www.hackingvoip.com/sec_tools.html)
- Scapy - Scapy is a powerful interactive packet manipulation program. It can easily handle most classical tasks like scanning, tracerouting, probing, unit tests, attacks or network discovery. [http://www.hackingvoip.com/sec\\_tools.html](http://www.hackingvoip.com/sec_tools.html)

## Packet Generation / Flooding (2/2)

- Seagull - A multi-protocol traffic generator especially targeted towards IMS.  
<http://gull.sourceforge.net/doc/sip.html>
- SIPBomber - SIPBomber is sip-protocol testing tool for Linux.  
<http://www.metalinkltd.com/downloads.php>
- SIPNess - SIPnessMessenger is a SIP testing tool which is used for testing SIP applications. <http://www.ortena.com/files/Messenger.zip>
- SIPp - SIPp is a free Open Source test tool / traffic generator for the SIP protocol.  
<http://sipp.sourceforge.net>
- SIPsak - SIP swissarmy knife. <http://sipsak.org>

## Fuzzing Araçları (1/3)

- SiVuS – [www.vopsecurity.org](http://www.vopsecurity.org)
- Asteroid - This is a set of malformed SIP methods (INVITE, CANCEL, BYE, etc.) that can be crafted to send to any phone or proxy.  
<http://www.infiltrated.net/asteroid/>
- Codenomicon VoIP Fuzzers - Commercial versions of the free PROTOS toolset.  
<http://www.codenomicon.com/products/telecommunications/>
- Spirent ThreatEx - A commercial protocol fuzzer and robustness tester.  
<http://www.spirentcom.com/general/docview.cfm?D=4663>

## Fuzzing Araçları (2/3)

- Fuzzy Packet - Fuzzy packet is a tool to manipulate messages through the injection, capturing, receiving or sending of packets generated over a network. Can fuzz RTP and includes built-in ARP poisoner.  
[http://libresource.inria.fr/projects/VoIP\\_Security/fuzzypacket](http://libresource.inria.fr/projects/VoIP_Security/fuzzypacket)
- Mu Security VoIP FuzzingPlatform - Fuzzingplatform handling SIP, H.323 and MGCP protocols.  
[http://www.musecurity.com/products/protocol\\_usecase.html#voip](http://www.musecurity.com/products/protocol_usecase.html#voip)
- SIP-Proxy - Acts as a proxy between a VoIP UserAgent and a VoIP PBX. Exchanged SIP messages pass through the application and can be recorded, manipulated, or fuzzed. <http://sourceforge.net/projects/sipproxy>

## Fuzzing Araçları (3/3)

- Ohrwurm - Ohrwurm is a small and simple RTP fuzzer.  
<http://mazzoo.de/blog/2006/08/25#ohrwurm>
- PROTOS H.323 Fuzzer - A java tool that sends a set of malformed H.323 messages designed by the University of OULU in Finland.  
<http://www.ee.oulu.fi/research/ouspg/protos/testing/c07/h2250v4/index.html#download>
- PROTOS SIP Fuzzer - A java tool that sends a set of malformed SIP messages designed by the University of OULU in Finland.  
<http://www.ee.oulu.fi/research/ouspg/protos/testing/c07/sip/>

## Signaling Manipulation Araçları (1/3)

- SiVuS – [www.vopsecurity.org](http://www.vopsecurity.org)
- BYE Teardown - This tool attempts to disconnect an active VoIP conversation by spoofing the SIP BYE message from the receiving party.  
[http://www.hackingvoip.com/sec\\_tools.html](http://www.hackingvoip.com/sec_tools.html)
- Check Sync Phone Rebooter - Transmits a special NOTIFY SIP message which will reboot certain phones. [http://www.hackingvoip.com/sec\\_tools.html](http://www.hackingvoip.com/sec_tools.html)
- RedirectPoison - This tool works in a SIP signaling environment, to monitor for an INVITE request and respond with a SIP redirectresponse, causing the issuing system to direct a new INVITE to another location.  
[http://www.hackingvoip.com/sec\\_tools.html](http://www.hackingvoip.com/sec_tools.html)

## Signaling Manipulation Araçları (2/3)

- Registration Eraser - This tool will effectively cause a denial of service by sending a spoofed SIP REGISTER message to convince the proxy that a phone/user is unavailable. [http://www.hackingvoip.com/sec\\_tools.html](http://www.hackingvoip.com/sec_tools.html)
- Registration Hijacker - This tool tries to spoof SIP REGISTER messages in order to cause all incoming calls to be rerouted to the attacker. [http://www.hackingvoip.com/sec\\_tools.html](http://www.hackingvoip.com/sec_tools.html)
- SIP-Kill - Sniff for SIP-INVITEs and tear down the call. <http://skora.net/voip/voip.html>

## Signaling Manipulation Araçları (3/3)

- SIP-Proxy-Kill - Tears down a SIP-Session at the last proxy before the opposite endpoint in the signaling path. <http://skora.net/voip/voip.html>
- SIP-RedirectRTP - Manipulate SDP headers so that RTP packets are redirected to an RTP-proxy. <http://skora.net/voip/voip.html>
- SipRogue - A multifunctional SIP proxy that can be inserted between two talking parties. [http://www.hackingvoip.com/sec\\_tools.html](http://www.hackingvoip.com/sec_tools.html)
- Registration Adder - This tool attempts to bind another SIP address to the target, effectively making a phone call ring in two places (the legitimate user's desk and the attacker's). [http://www.hackingvoip.com/sec\\_tools.html](http://www.hackingvoip.com/sec_tools.html)

## Media Manipulation Araçları

- RTP InsertSound - This tool takes the contents of a .wav or tcpdumpformat file and inserts the sound into an active conversation.  
[http://www.hackingvoip.com/sec\\_tools.html](http://www.hackingvoip.com/sec_tools.html)
- RTP MixSound - This tool takes the contents of a .wav or tcpdumpformat file and mixes the sound into an active conversation.  
[http://www.hackingvoip.com/sec\\_tools.html](http://www.hackingvoip.com/sec_tools.html)
- RTPProxy - Wait for incoming RTP packets and send them to wanted (signaled by a tiny protocol) destination. <http://skora.net/voip/voip.html>
- RAT (Robust Audio Tool) <http://www.mice.cs.ucl.ac.uk/multimedia/software/rat/>

# Referanslar

- VoIPSA–VoIP Security Alliance, [www.voipsa.org](http://www.voipsa.org)
- The VoPSecurity Forum, [www.vopsecurity.org](http://www.vopsecurity.org)
- NIST –
  - Security Considerations for VoIP Systems
  - Voice over Internet Protocol (VoIP), Security Technical Implementation Guide (DISA)
- <http://www.ietf.org/html.charters/iptel-charter.html>
- IP Telephony Tutorial, <http://www.pt.com/tutorials/iptelephony/>
- Signaling System 7 (SS7), <http://www.iec.org/online/tutorials/ss7/topic14.html>
- SIP - <http://www.cs.columbia.edu/sip/>
- IP Telephonywith SIP - [www.iptel.org/sip/](http://www.iptel.org/sip/)
- SIP Tutorials
  - The Session Initiation Protocol (SIP)
  - [http://www.cs.columbia.edu/~hgs/teaching/ais/slides/sip\\_long.pdf](http://www.cs.columbia.edu/~hgs/teaching/ais/slides/sip_long.pdf)
  - SIP and the new network communications model  
<http://www.webtorials.com/main/resource/papers/nortel/paper19.htm>
- H.323 ITU Standards, <http://www.imtc.org/h323.htm>
- Third Generation Partnership Project (3gpp), <http://www.3gpp.org/>

# Standardlar

- ITU
  - Focus Group on Next Generation Networks (FGNGN ) - <http://www.itu.int/ITU-T/ngn/fgngn/>
  - Open Communications Architecture Forum (OCAF) Focus Group <http://www.itu.int/ITU-T/ocaf/index.html>
- IETF
  - Transport area - <http://www.ietf.org/html.charters/wg-dir.html#Transport%20Area>
  - Security Area - <http://www.ietf.org/html.charters/wg-dir.html#Security%20Area>
- ATIS - <http://www.atis.org/0191/index.asp>
  - T1S1.1--Lawfully Authorized Electronic Surveillance
  - T1S1.2--Security
- Lawful Intercept
  - 3GPP -TS 33.106and TS 33.107
  - ETSI DTS 102 v4.0.4



**Teşekkürler**