

Viproy ile VoIP Denetimi

• • •

Fatih Özavcı
Güvenlik Danışmanı



Konuşmacı

- Fatih Özavcı, Güvenlik Danışmanı
- İlgi alanları
 - VoIP & Phreaking
 - Mobil teknolojiler
 - Ağ altyapıları
 - Gömülü sistemler
 - Donanım ve IoT Hacking
- Viproy VoIP sızma aracı geliştiricisi
- Uluslararası konuşmacı ve eğitmen
 - Blackhat, Defcon, Troopers, AusCert, Ruxcon



Tehditler ve Saldırırgan Yetenekleri

Varsayımlar:

- VoIP ağlarına fiziksel olarak erişim zordur
- VoIP saldırıları üst düzey yetenekler gerektirir
- Saldırılar mahremiyet ve çağrı sahteciliği odaklıdır
- VoIP servisleri çok güvenli yapılandırılmıştır

Gerçek Hayat:

- Fiziksel güvenlik yetersizliği, zayıf erişim denetimi
- Viproy sonrası, saldırı için VoIP deneyimi gerekmıyor
- İstemci saldırıları, istihbarat toplama, kalıcı erişim
- Kolay parolalar, eski sistemler, güncelleme sorunları



Viproy VoIP Sızma Aracı

- Viproy, Vulcan'ca “Çağrı/Karar” anlamına gelmektedir
- Viproy VoIP sızma aracı
 - Metasploit Framework test modülleri paketi
 - Hızlı test geliştirme için SIP & Skinny kütüphaneleri
 - Özel SIP başlıklarları ve kimlik doğrulama desteği
 - Güven ilişkisi analizi, SIP Proxy analizi, MITM modülleri
- Modüller
 - Basit ve karmaşık SIP testleri kapasitesi (mesaj, çağrı)
 - SIP kimlik doğrulama, kullanıcı ve alan adı saptama
 - SIP güven ilişkisi analizi, SIP proxy kullanımı, sahte servis
 - Cisco Skinny analizi ve Cisco CUCM/CUCDM exploitleri
 - Polycom yapılandırma ayıklayıcı

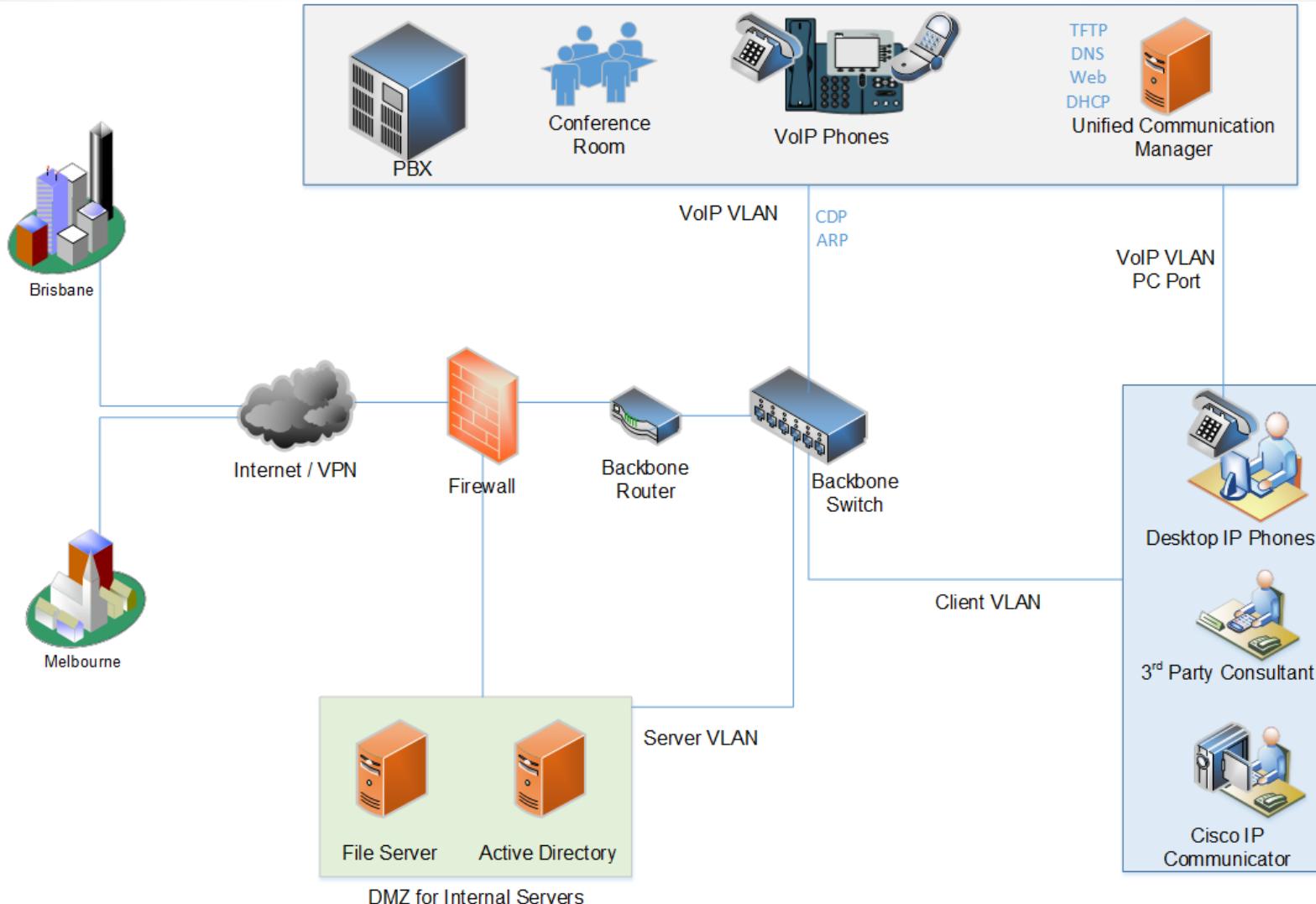


Güvenlik Denetimi ve Özgür Yazılımlar

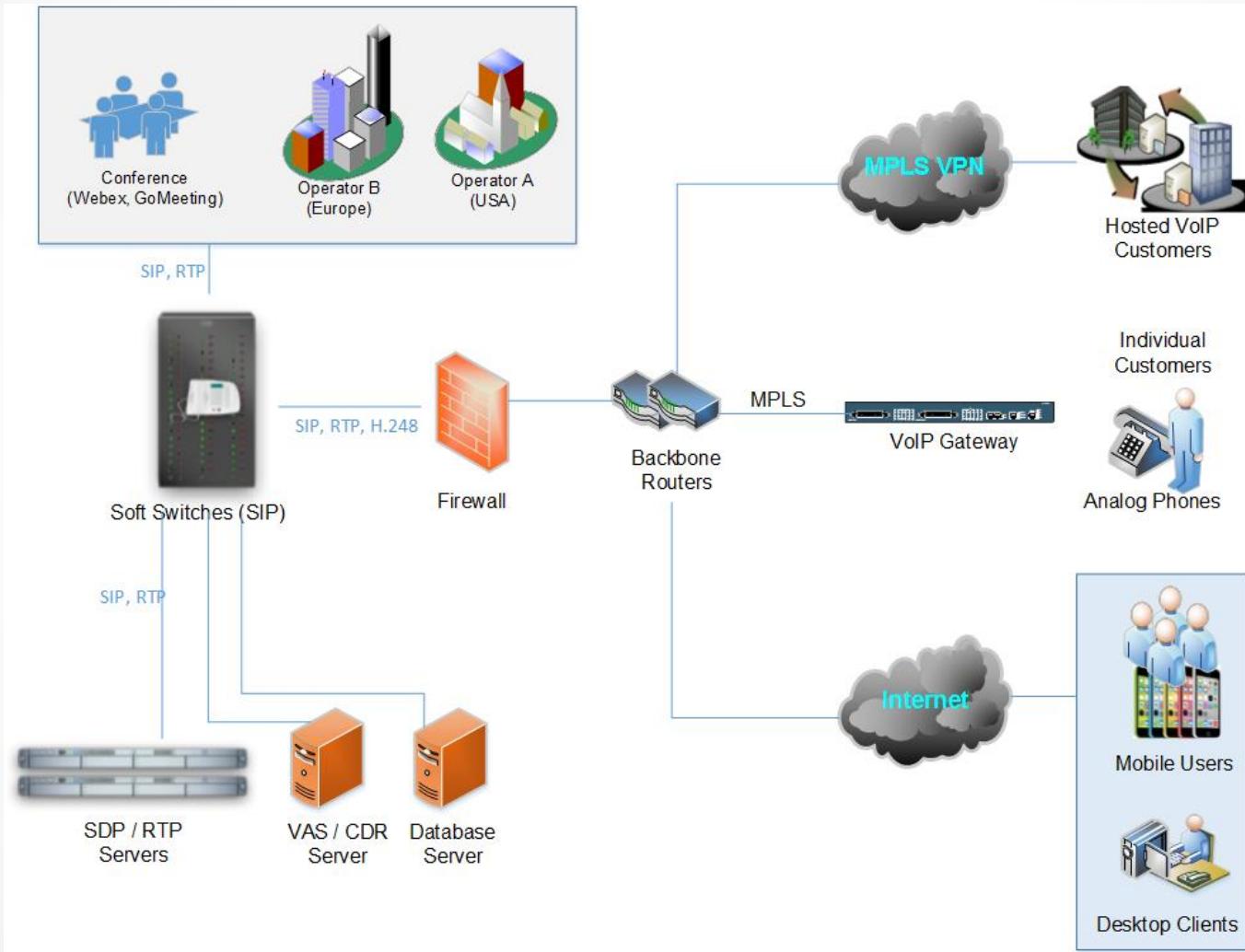
- Denetim kuruma/sisteme/yazılıma özel olmalıdır ve her testin özelleştirilmesi gerekmektedir
- Özel testlerin tanımlanabilmesi, kullanılabilecek test şekillerinin döngülere sokulmasını gerektirmektedir
- Çeşitli denetim adımlarında alınan çıktıların birleştirilmesi ve beraber değerlendirilmesi gerekmektedir
- Basit, hızlı ve amaca hizmet eden yazılımlar denetim sürecinin verimini arttırmaktadır
- Kaynak kodu açık, yapılan işlemin net olarak görünebileceği araçlar tercih edilmelidir



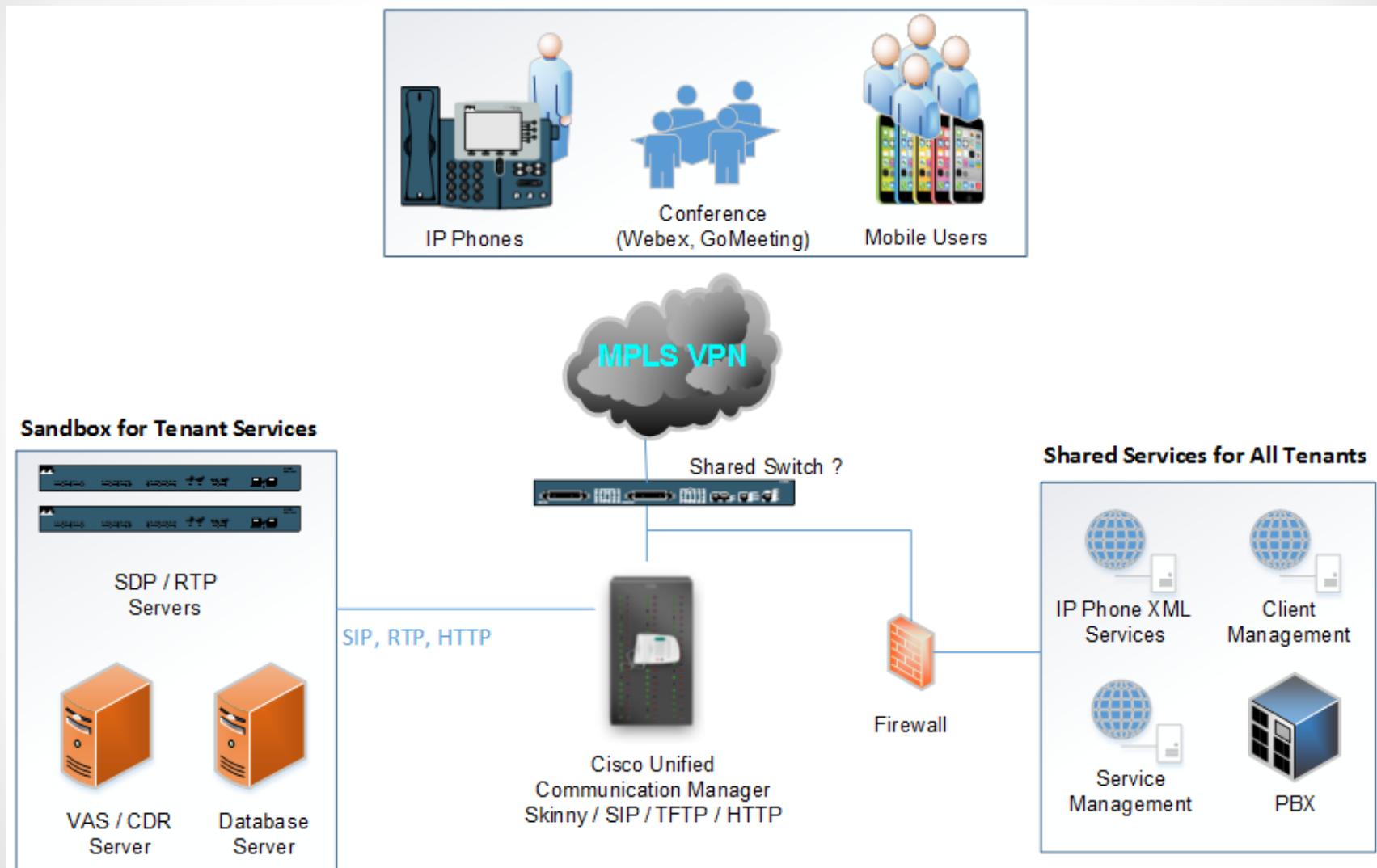
Kurumsal VoIP Ağları



Bütünleşik İletişim (UC)



Bulut VoIP Hizmetleri



Örnek Denetim Rotası



Denetim Kapsamının Belirlenmesi

- Denetim bilgilerinde verilenler her zaman yeterli değildir
 - Sunucular (SIP, SIP Proxy, RTP Proxy)
 - İstemciler (Yazılım, Özel Donanım)
 - Ağ Altyapısının Yerleşimi
- Denetim öncesi gerekli bilgiler
 - Donanım ve Yazılımların Türü, Sürümü
 - Seçilen Protokoller ve Seçenekler
 - Yönetim veya Destek Amaçlı Servisler
 - TLS ve SRTP Kullanımı



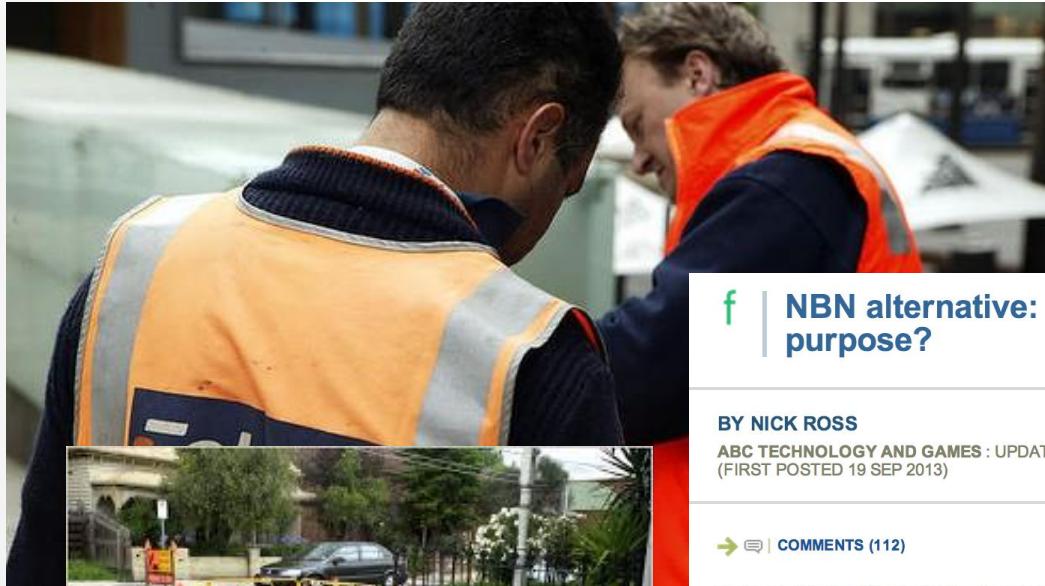
VoIP Servisinin Anlaşılması

- İstemci Türleri
 - Yazılım (IP Communicator, Android/iOS Apps)
 - IP telefonlar (Cisco 7945, Yealink)
 - Video konferans cihazları (Cisco Presence)
 - Harici konferans çözümleri (Webex, GoMeeting)
- Servis Amacı
 - Uluslararası/Ulusal/Mobil şebeke bağlantıları
 - Çağrı merkezi (ticari ürün ve özgür alternatifler)
 - Ticari VoIP servisleri (mobil ve bulut çözümleri)
 - Kurumsal kullanım (VLAN, toplantı odaları)
- VoIP protokoller (SIP, Skinny, RTP, IAX, Diameter)



Fiziksel Erişim Analizi

- Yerel dağıtım şebekeleri ve odaları
- Ağ ve müşteri hizmeti sonlandırma cihazları



f | NBN alternative: Is Australia's copper network fit for purpose?

BY NICK ROSS

ABC TECHNOLOGY AND GAMES : UPDATED 20 SEP 2013
(FIRST POSTED 19 SEP 2013)

→ | COMMENTS (112)

In the world of political and media misinformation that is the NBN, an important issue, that hasn't been fully addressed, is "How fit for purpose is Australia's copper network?" This seemingly mundane and tedious question directly affects tens of billions of dollars in government spending. How?

The bulk of the Coalition's NBN alternative policy uses the existing copper network to get the internet to your home or



There is considerable evidence to suggest that Australia's copper network is in a worse state than those of other nations. How bad is it and can it be fixed?
CREDIT: MAGILLA (CANOFWORMS.ORG)



VoIP Ağına Fiziksel Erişim

- Toplantı odaları, lobi, misafir telefonları, acil durum telefonları
 - PC portları, PoE
 - Raspberry Pi
 - 3G/4G ile kalıcı erişim



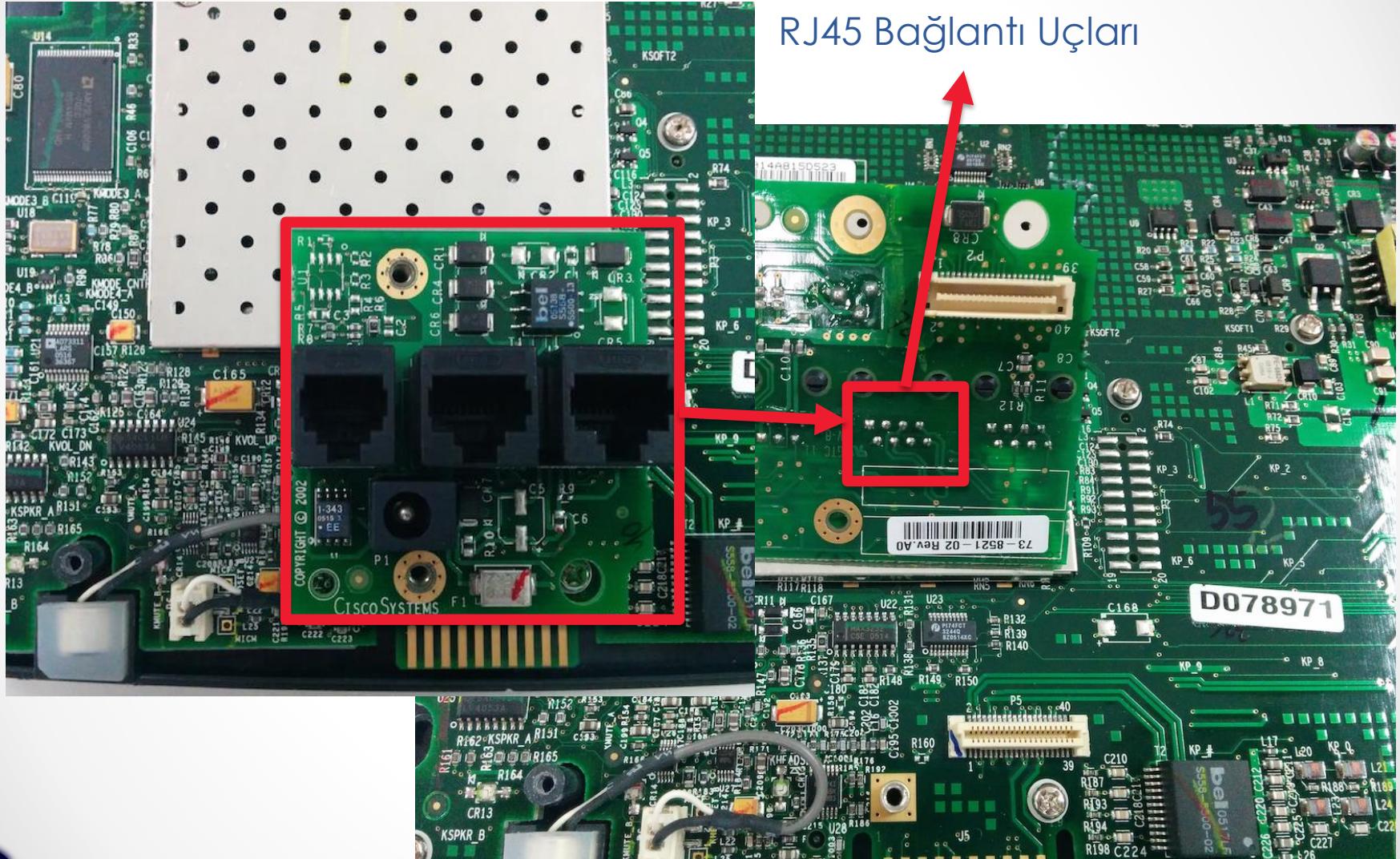
Product Name (产品名称): UC Phone (UC电话)
Model (型号): CP-7945G
Manufacturer (制造商): Cisco Systems, Inc.
Power input (输入): 48V=0.38A(0.38A)

声明: 此为A级UC系统产品附件 (中国大陆), 在生活环境 中, 该产品可能会造成无线电干扰, 在这种情况下, 可能需要用户对其干扰采取切实可行的措施。
This Class B digital apparatus complies with Canadian ICES-003.
Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

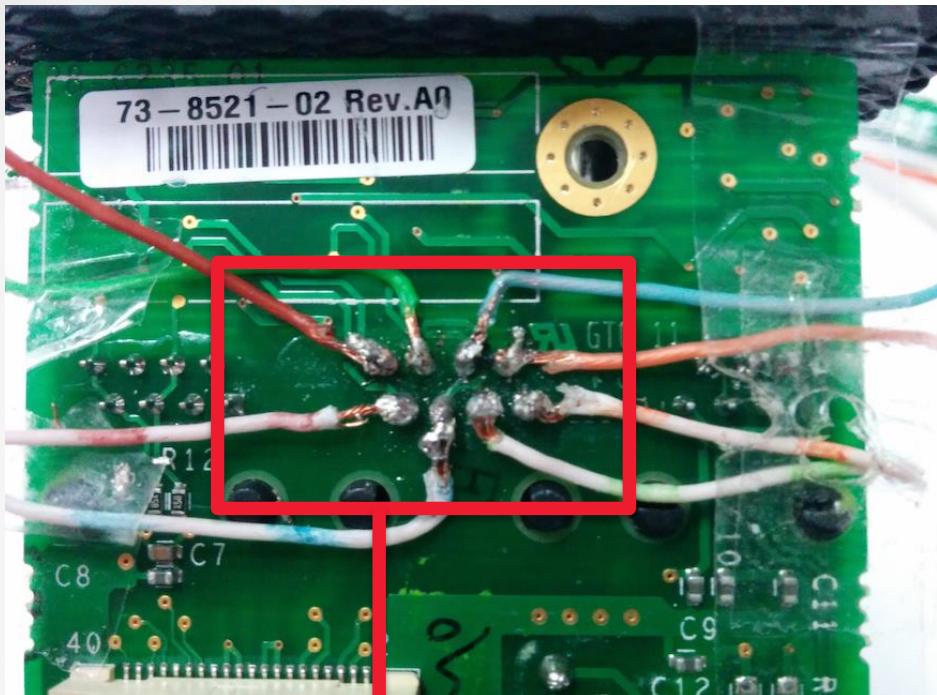
This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Certifications:
ANATEL: N906
CE: 20
FCC: TMY-CP-7945G
VCCI: PG
HAC: VCI
TELEPERMIT: TELEPERMIT
SRI: SN: FCH1444ANHC
LR82435
PTC 220 / 07 / 088
http://cisco-returns.com
MAC: ECC882B12CF9
PID VID:CP-7945G V08
Made in China 中国制造
www.cisco.com

Kalıcı Erişim için Tapberry Pi



Kalıcı Erişim için Tapberry Pi



Cat 5 kablo bağlantısı



CDP Sahteciliği

- Cisco cihazlarının keşfi
- Voice VLAN bilgisi alınması
- Araçlar
 - Viproy CDP modülü
 - Wireshark
- Paket yakalayarak ağ altyapısının öğrenilmesi
- Sahte CDP paketi gönderilerek bir telefon gibi davranışmak ve Voice VLAN'ına erişim istemek
- Voice VLAN bağlantısı (802.1x, EAP-MD5)



Cisco Discovery Protocol (CDP)

No.	Time	Source	Destination	Protocol	Length	Info
5024	915.241597	Cisco_db:b...	CDP/VTP/DT...	CDP	125	Device ID: SEP001B0CDBB14C Port ID: Port 2
5034	916.241534	Cisco_db:b...	CDP/VTP/DT...	CDP	125	Device ID: SEP001B0CDBB14C Port ID: Port 2
5041	917.241045	Cisco_db:b...	CDP/VTP/DT...	CDP	125	Device ID: SEP001B0CDBB14C Port ID: Port 2
5407	977.246836	Cisco_db:b...	CDP/VTP/DT...	CDP	125	Device ID: SEP001B0CDBB14C Port ID: Port 2
5501	995.652824	Cisco_8b:0...	CDP/VTP/DT...	CDP	463	Device ID: MON2

► Frame 5501: 463 bytes on wire (3704 bits), 463 bytes captured (3704 bits) on interface 0

► IEEE 802.3 Ethernet

► Logical-Link Control

► Cisco Discovery Protocol

 Version: 2

 TTL: 180 seconds

► Checksum: 0xbd59 [correct]

► Device ID: MON2

► Software Version

► Platform: cisco WS-C6509-E

► Addresses

► Port ID: GigabitEthernet7/11

► Capabilities

► VTP Management Domain: ON2

► Native VLAN: 2142

► Duplex: Full

► VoIP VLAN Reply: 2181

► Trust Bitmap: 0x00

► Untrusted port CoS: 0x00

► Management Addresses

► Power Available:



Sinyalleşme

VoIP = Sinyalleşme + Medya

- Sinyalleşme servisleri çağrı başlatma, takip, aktarım ve kayıt gibi işlemlerden sorumludur.
- Medya aktarımı ise sinyalleşmeden ayrı bir kanaldan/servisten yapılır. (örn. RTP, H.323)
- Önemli sinyalleşme protokolleri
 - SIP servisleri (Üretici uzantıları ve özelleştirmeler)
 - Üreticiye özel sinyalleşme servisleri (SCCP / Skinny)

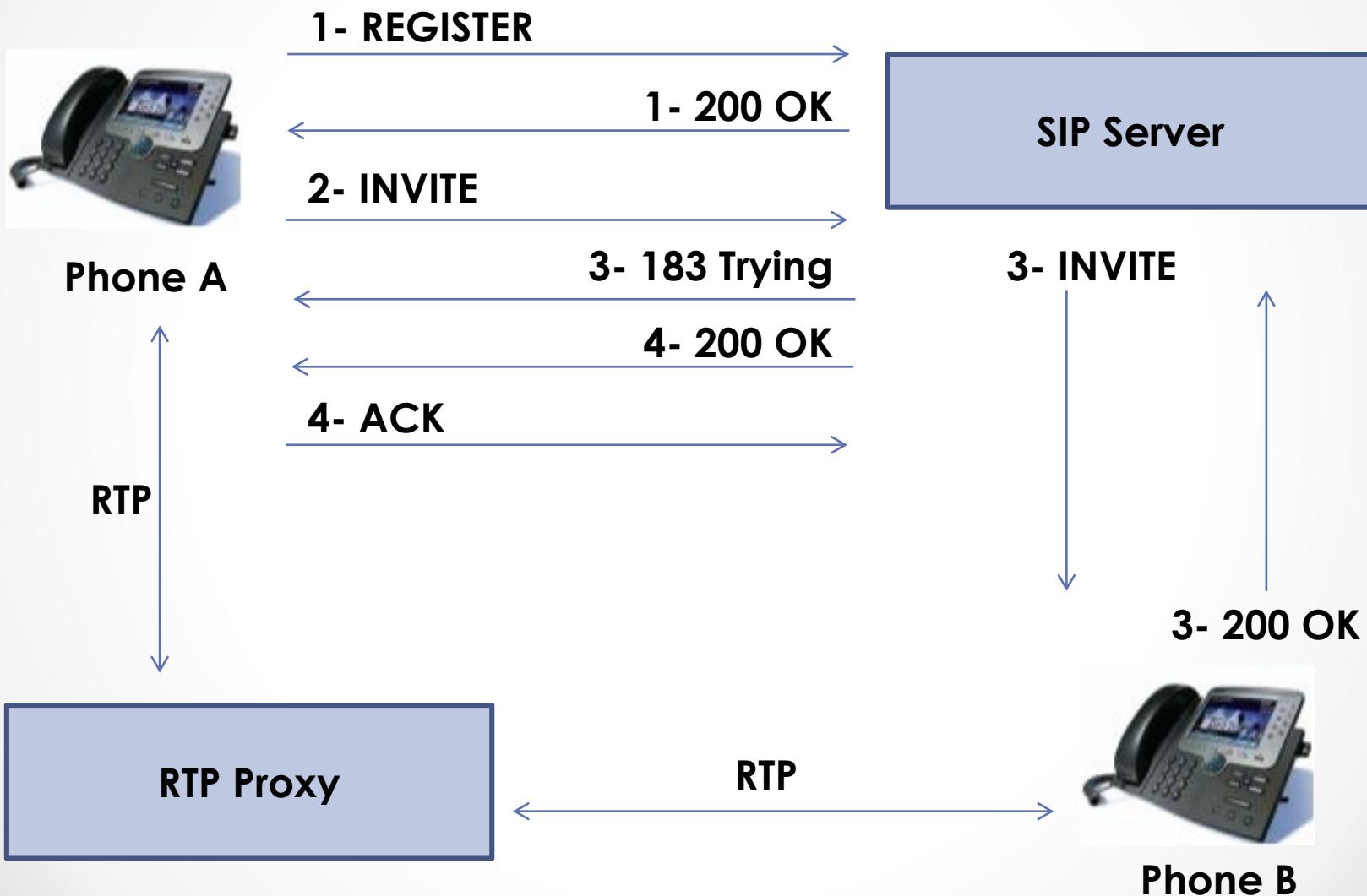


Session Initiation Protocol

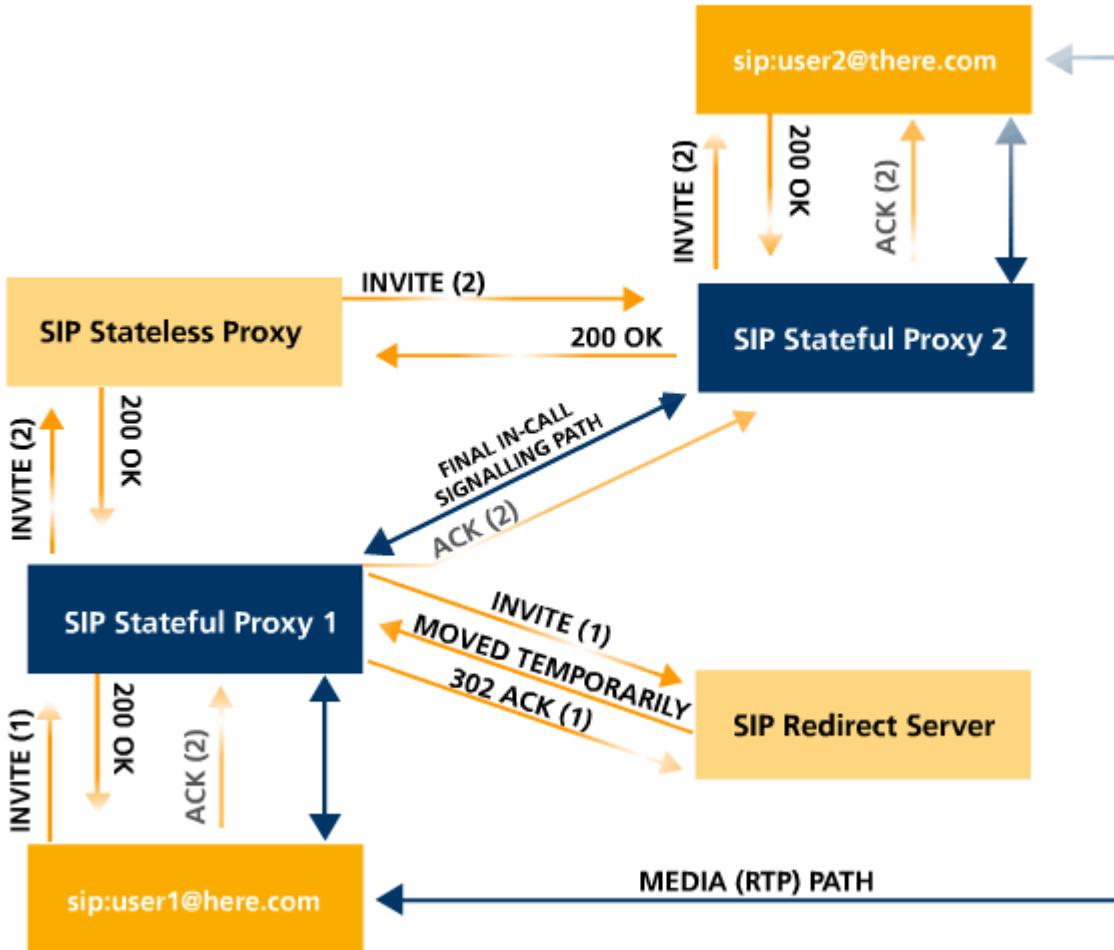
- 1996'da geliştirildi, 2002 yılında standartlaştı
- Sinyalleşme yöntemleri
 - Register
 - Invite
 - Subscribe
 - Message
- RTP iletişiminin, mesajlaşma içeriğinin ve kullanıcı kimliklerinin korunması için şifreleme gerekmektedir
- Kimlik doğrulama (Digest, Sertifika, NTLM)
- Bütünleşik iletişim (UC)



Temel SIP Akışı



Kısmen Karmaşık SIP Akışı



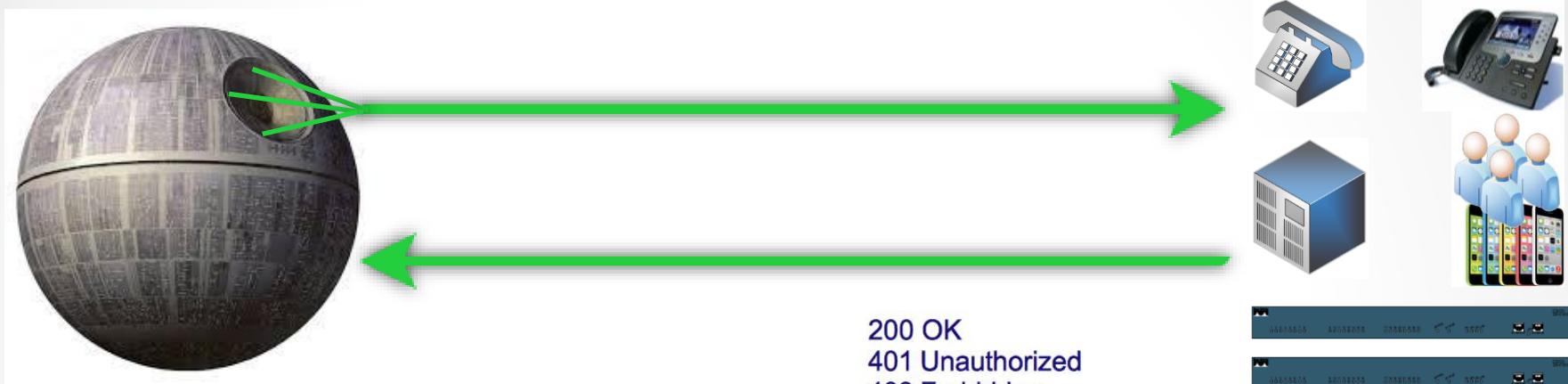
Temel Saldırılar

- SIP servislerinin ve görevlerinin bulunması
- Kullanılabilir metod ve özelliklerin keşfi
- SIP yazılımı ve açıklarının analizi
- Hedef dahili, kullanıcı ve alan adlarının saptanması
- Kimlik doğrulama olmaksızın SIP kaydı (trunk, VAS)
- Saptanan kullanıcı hesaplarına sözlük saldırısı
- Kimlik doğrulama ve kayıt olmaksızın çağrı analizi
- IP temelli doğrudan çağrı analizi
- Çağrı ve kimlik sahteciliği



Kayıt Analizi

Register (FROM, TO, Credentials)



RESPONSE Depends on Information in REQUEST

- Type of Request (REGISTER, SUBSCRIBE)
- FROM, TO, Credentials with Realm
- Via

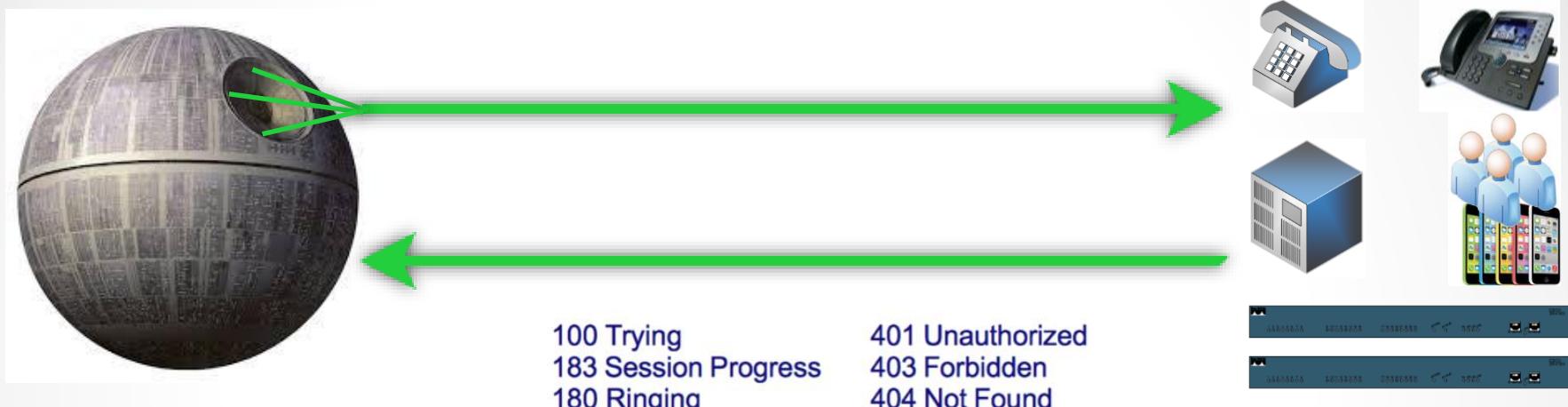
Actions/Tests Depends on RESPONSE

- Brute Force (FROM, TO, Credentials)
- Detecting/Enumerating Special TOs, FROMs or Trunks
- Detecting/Enumerating Accounts With Weak or Null Passwords
-



Çağrı ve Faturalandırma Analizi

Invite / Ack / Re-Invite / Update (FROM, TO, VIA, Credentials)



RESPONSE Depends on Information in INVITE REQUEST

- FROM, TO, Credentials with Realm, FROM <>, TO <>
- Via, Record-Route
- Direct INVITE from Specific IP:PORT (IP Based Trunks)

Actions/Tests Depends on RESPONSE

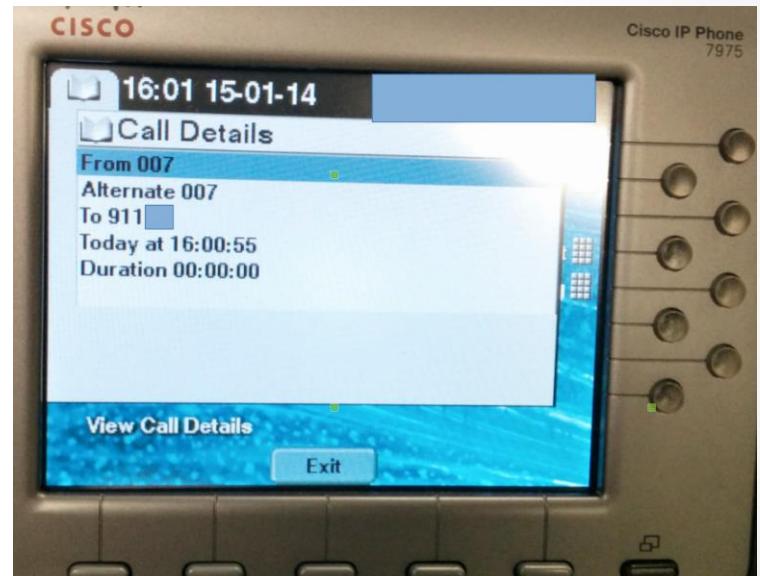
- Brute Force (FROM&TO) for VAS and Gateways
- Testing Call Limits, Unauthenticated Calls, CDR Management
- INVITE Spoofing for Restriction Bypass, Spying, Invoice
-

Çağrı Sahteciliği

Remote-Party-ID başlığı

Remote-Party-ID: <sip:007@1.2.3.4>;party=called;screen=yes;privacy=off

- Çağrı sahteciliği
- Faturalandırma atlatma
- Voicemail erişimi
- Harici operatörler



Tüm Operatörler için Çağrı Sahteciliği

- Tüm operatörler arayan kimliğine güvenirler
- Bir tane etkilenen operatör ile herkes aldatılabilir

Forbes ▾ Your Secret Weapon in Business: Culture Active on LinkedIn 

TECH 7/25/2011 @ 12:32PM | 9,228 views



Marc Weber Tobias
Contributor

the guardian

News | World | Sport | Comment | Culture | Business | Environment
News > UK news

Phone hacking may have led to Milly Dowler voicemail deletions, says judge
Voice messages, once hacked, would have been deleted automatically, Mr Justice Saunders tells Old Bailey jury

Share

Lisa O'Carroll
theguardian.com, Friday 6 June 2014 00:12 AEST



Stuart Kullner sounded like a headteacher, according to a member of staff from Monday's Recruitment Agency, the court heard. Photograph: Mark Thomas/Rex Features

Murdered schoolgirl Milly Dowler's voicemails would have been deleted automatically after they were hacked by the News of the World, the Old Bailey heard.

The Register

Data Centre Software Networks Security Policy Business Hardware Science Bootnotes Columns



SHOP SM SHOP NOW

SECURITY

Reg probe bombshell: How we HACKED mobile voicemail without a PIN

messages are still not secure

Two UK mobile networks are wide open to attack. The Register has found that even after Lord Leveson ruled into the practice of phone hacking, it remains at the most basic level of security.

listened to the private voicemail of a fellow Register reporter. In the inbox of a new SIM bought for testing purposes, there was a message from a SIM issued to police doing anti-terrorist work. The login PIN for any of them; I faced no

The newspapers accessing people's voicemail change things about it all is that at no stage have

SpoofCard DESIGN YOUR CALLER ID

HOME BUY CREDITS FEATURES MOBILE APPS MEDIA HELP SIGN UP LOGIN

Disguise your Caller ID

Display a different number to protect yourself or pull a prank on a friend. It's easy to use and works on any phone!

Get Spoofing! They'll never know it was you.

TRY A LIVE DEMO OR GET STARTED NOW

İleri Düzey SIP Saldırıları

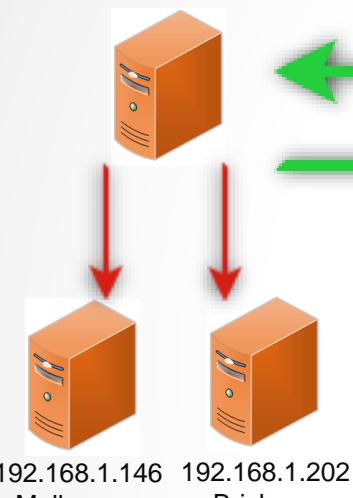
Bütünleşik iletişimimin olduğu ve çok sayıda oturum yönetim geçidinin çalıştığı ağlarda ileri düzey saldırılar da uygulanabilir.

- SIP Proxy atlatma saldırısı
- SIP güven ilişkileri analizi
- Servis engelleme analizi



SIP Proxy Atlatma Saldırısı

192.168.1.145 - Sydney
Production SIP Service



```
msf auxiliary(vsupportscan-options) > run
[+] 192.168.1.146:5060 is Open
    Server      : FPBX-2.11.0beta2(11.2.1)

[+] 192.168.1.145:5070 is Open
    User-Agent   : sipXecs/4.7.0 sipXecs/registry (Linux)

[+] 192.168.1.201:5061 is Open
    Server      : sipXecs/xxxx.yyyy sipXecs/sipxbridge (Linux)

[+] 192.168.1.203:5060 is Open
    User-Agent   : 3CXPhoneSystem 11.0.28976.849 (28862)
```



Dağıtık Servis Engellemeye Saldırısı

192.168.1.145 - Sydney
Production SIP Service

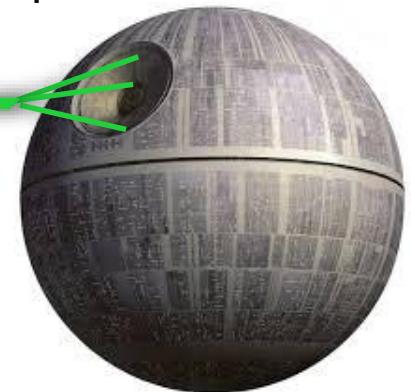


192.168.1.146
Melbourne



192.168.1.202
Brisbane

IP spoofed UDP SIP request



Alderaan

SIP based DoS attacks

- UDP vulnerabilities and IP spoofing
- Too many errors, very very verbose mode
- ICMP errors

SIP Güven İlişkileri Analizi

192.168.1.145 - Sydney
Production SIP Service



UDP Trust



192.168.1.146
Melbourne

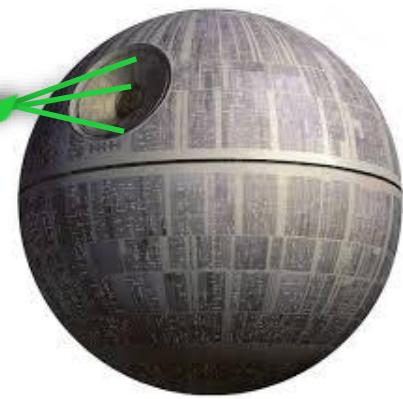
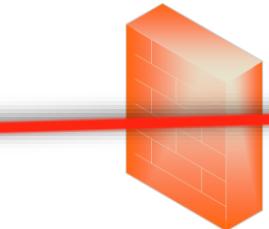


192.168.1.202
Brisbane

Universal
Trust



Tatooine



IP spoofed UDP SIP request
From field has IP and Port

Incoming Call

192.168.1.202:5060

00:00:00



Accept

Reject

Send INVITE/MESSAGE requests with

- IP spoofing (source is Brisbane),
- from field contains Spoofed IP and Port,

the caller ID will be your trusted host.



SIP Güven İlişkileri Analizi

192.168.1.145 - Sydney
Production SIP Service



UDP Trust



192.168.1.146
Melbourne

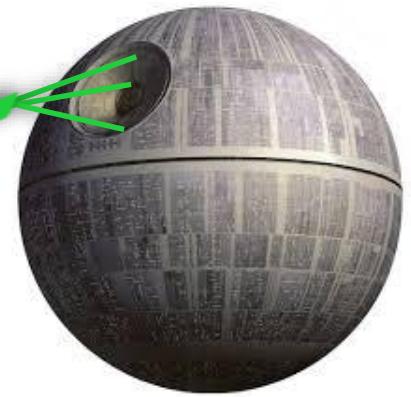
192.168.1.202
Brisbane

Universal
Trust



Tatooine

IP spoofed UDP SIP request
From field has bogus characters



It's a TRAP!



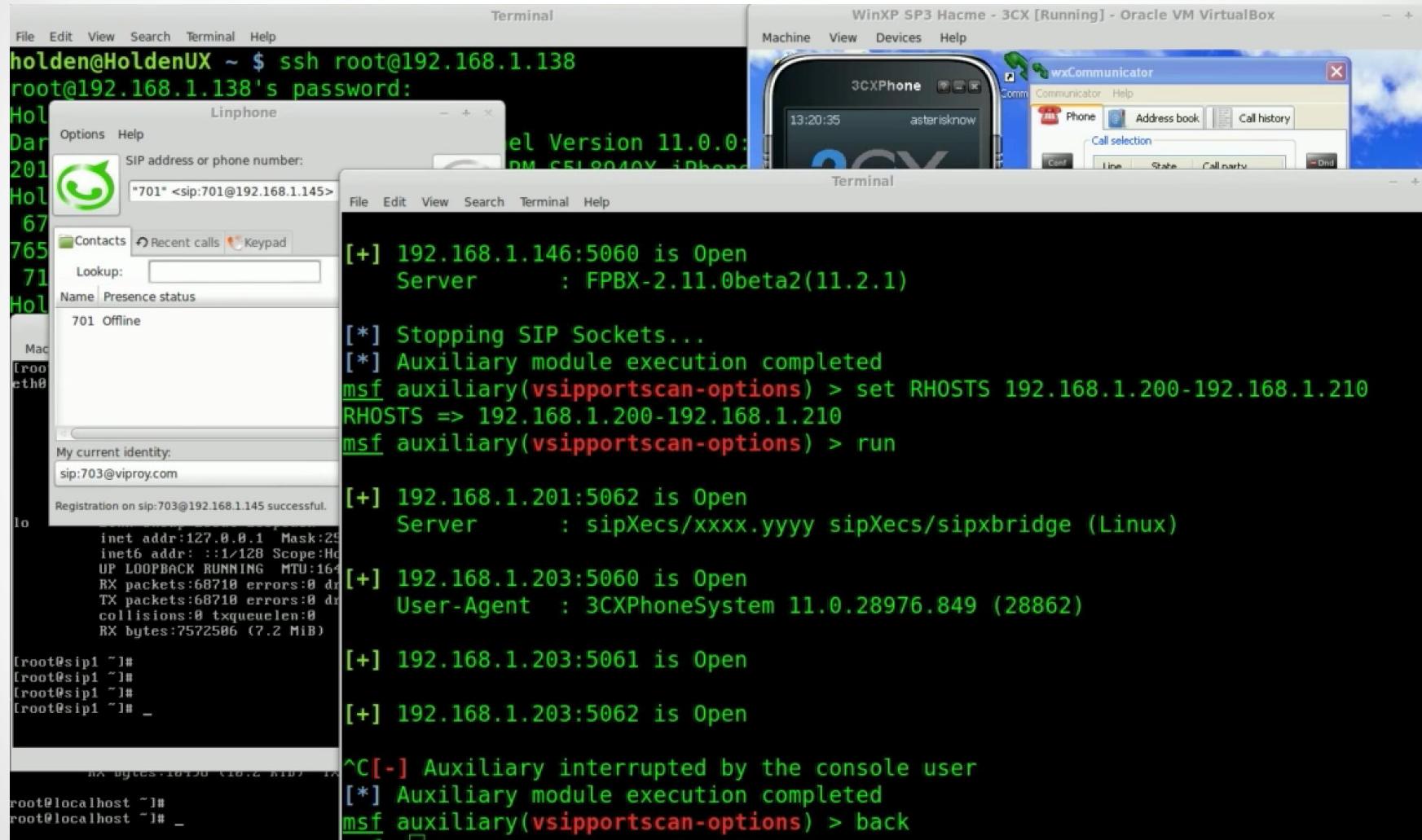
Send INVITE/MESSAGE requests with

- IP spoofing (source is Brisbane),
- from field contains special number,

you will have fun or voicemail access.

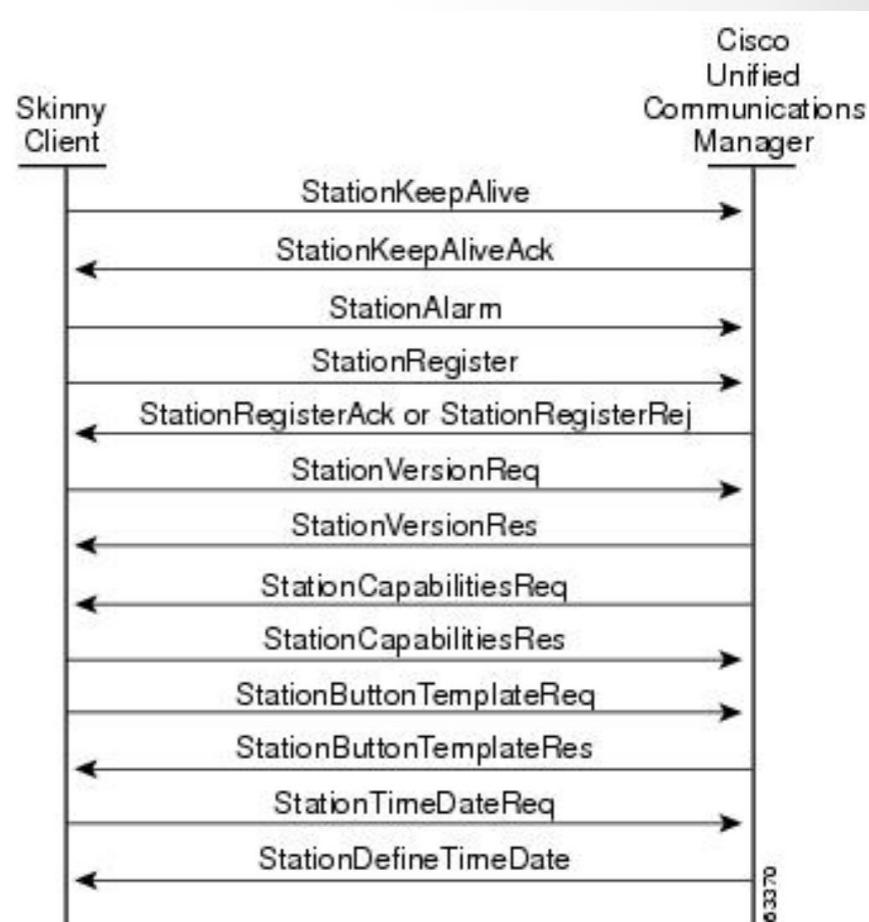


Viproj ile SIP Analizi



Cisco Skinny

- Cisco Skinny (SCCP)
 - İkilik, düz metin değil
 - Çeşitli sürümler
 - Kimlik doğrulama desteği bulunmuyor
 - Kimliklendirmede MAC adresi kullanılıyor
- Temel saldırılar
 - İzinsiz telefon kaydı
 - İzinsiz çağrı açma
 - Çağrı sahteciliği
 - Telefon yönlendirme



Source: Cisco



Cisco Skinny Analizi

▼ Skinny Client Control Protocol

Data length: 128

Header version: Basic (0x00000000)

Message ID: RegisterMessage (0x00000001)

Device name: SEP000C29BF1890

Station user ID: 0

Station instance: 0

IP address: 192.168.0.151 (192.168.0.151)

Device type: Unknown (30016)

Max streams: 5

0000	00	0c	29	93	5e	7a	00	0c	29	bf	18	90	08	00	45	60	E`	
0010	00	b0	02	a6	40	00	80	06	74	8d	c0	a8	00	97	c0	a8	@...	t.....		
0020	00	cd	04	17	07	d0	e7	1b	f2	21	8b	c8	15	d2	50	18	!....	P.	
0030	fa	f0	eb	67	00	00	80	00	00	00	00	00	00	00	01	00	g.....		
0040	00	00	53	45	50	30	30	30	43	32	30	42	46	31	39	30	SEP000	C29BF189		
0050	30	00	00	00	00	00	00	00	00	00	c0	a8	00	97	40	75	0.....	@u		
0060	00	00	00	00	00	00	00	00	00	00	00	14	00	72	03	01	00	r...	
0070	00	00	00	00	00	00	00	00	0c	29	bf	18	90	00	00	00	00).....	
0080	00	00	03	00	00	00	24	00	00	00	00	00	00	00	00	00	00	\$..	
0090	00	00	00	00	00	00	00	00	00	00	00	00	00	00	43	49	CI	
00a0	50	43	2d	38	2d	36	2d	31	2d	30	00	00	00	00	00	00	00	PC-8-6-1	-0.....	
00b0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	



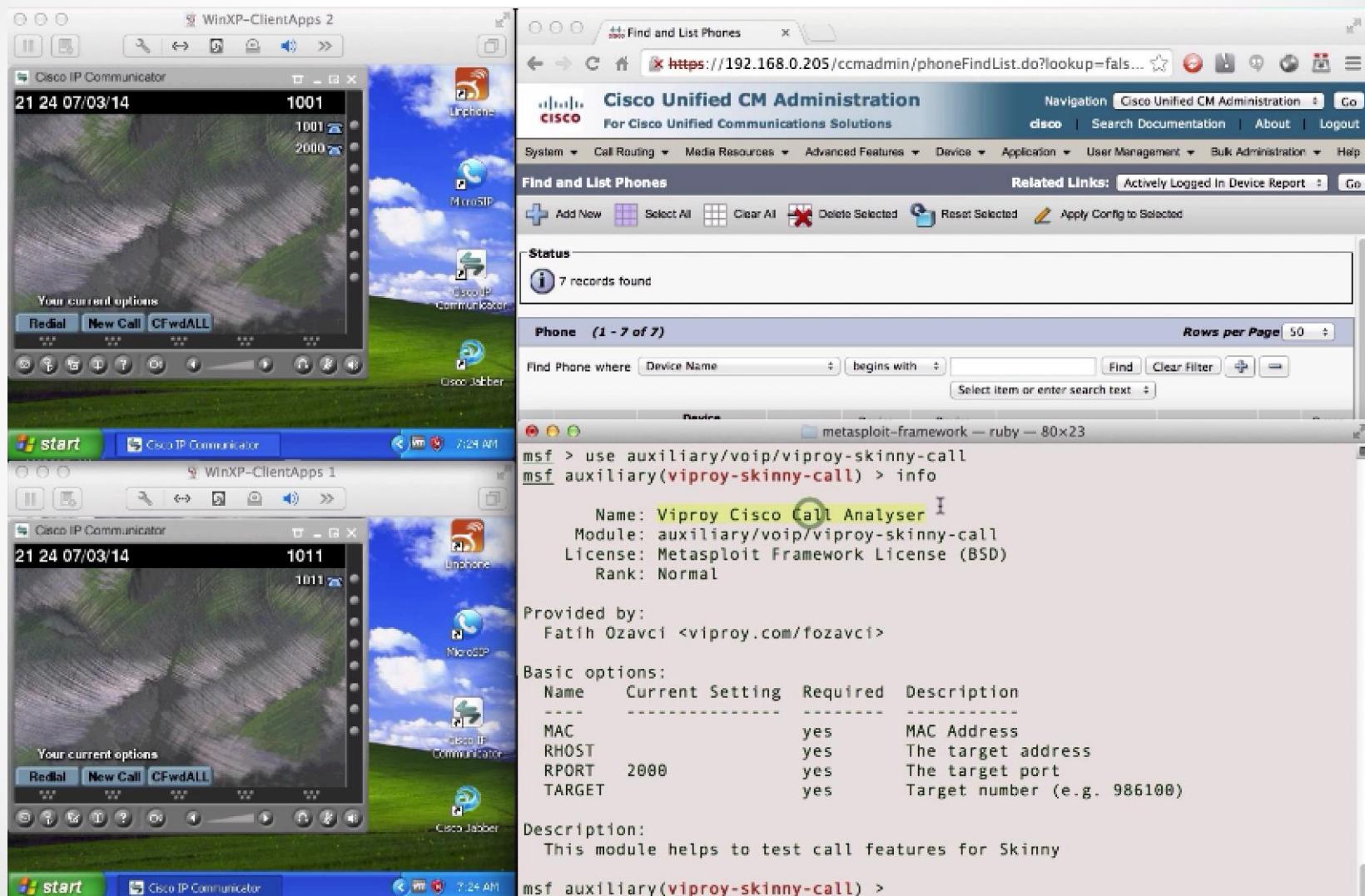
Cisco Skinny Analizi

- Viproxy, Skinny kütüphanesi ve 3 test modülü ile güçlü bir Skinny test ortamı sunmaktadır
 - İzinsiz kayıt
 - İzinsiz çağrı açma
 - İzinsiz çağrı yönlendirme

```
def skinny_parser(p)
  l = bytes_to_length(p[0..3])
  r = p[8..4].unpack('H*')[0]
  lines = nil
  case r
    when "9d000000"
      r = "RegisterRejectMessage"
      m = p[12..l-4]
    when "81000000"
      r = "RegisterAckMessage"
      m = "Registration successful."
    when "93000000"
      r = "ConfigStatMessage"
      devicename = p[12..15]
      userid = bytes_to_length(p[27..4])
      station = bytes_to_length(p[31..4])
      username = p[35..40]
      domain = p[45..48]
      lines = bytes_to_length(p[116..4])
      speeddials = bytes_to_length(p[120..4])
      m = "Device: #{devicename}\tUser ID: #{userid}\t#{username}\t#{domain}\t#{lines}\t#{speeddials}"
    when "9b000000"
      r = "CapabilitiesReqMessage"
      m = nil
    when "97000000"
      r = "ButtonTemplateMessage"
      m = nil
    when "21010000"
      r = "ClearPriNotifyMessage"
      m = nil
    when "15010000"
      r = "ClearNotifyMessage"
      m = nil
  end
end
```



Viproj ile Cisco Skinny Analizi



Viproj için Kaynaklar

- Viproj VoIP Penetration and Exploitation Kit

Author : <http://viproj.com/fozavci>

Homepage : <http://viproj.com>

Github: <http://www.github.com/fozavci/viproj-voipkit>

- Attacking SIP Servers Using Viproj VoIP Kit (50 mins)

https://www.youtube.com/watch?v=AbXh_L0-Y5A

- Hacking Trust Relationships Between SIP Gateways

<http://viproj.com/files/siptrust.pdf>

- VulnVoIP: Örnek zayıflık içeren VoIP sistemi

<http://www.rebootuser.com/?cat=371>



Sorular?



Teşekkürler!

