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 Saldırgan 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 gerekmiyor
- İstemci saldırıları, istihbarat toplama, kalıcı erişim
- Kolay parolalar, eski sistemler, güncelleme sorunları

Viproy VoIP Sızma Aracı

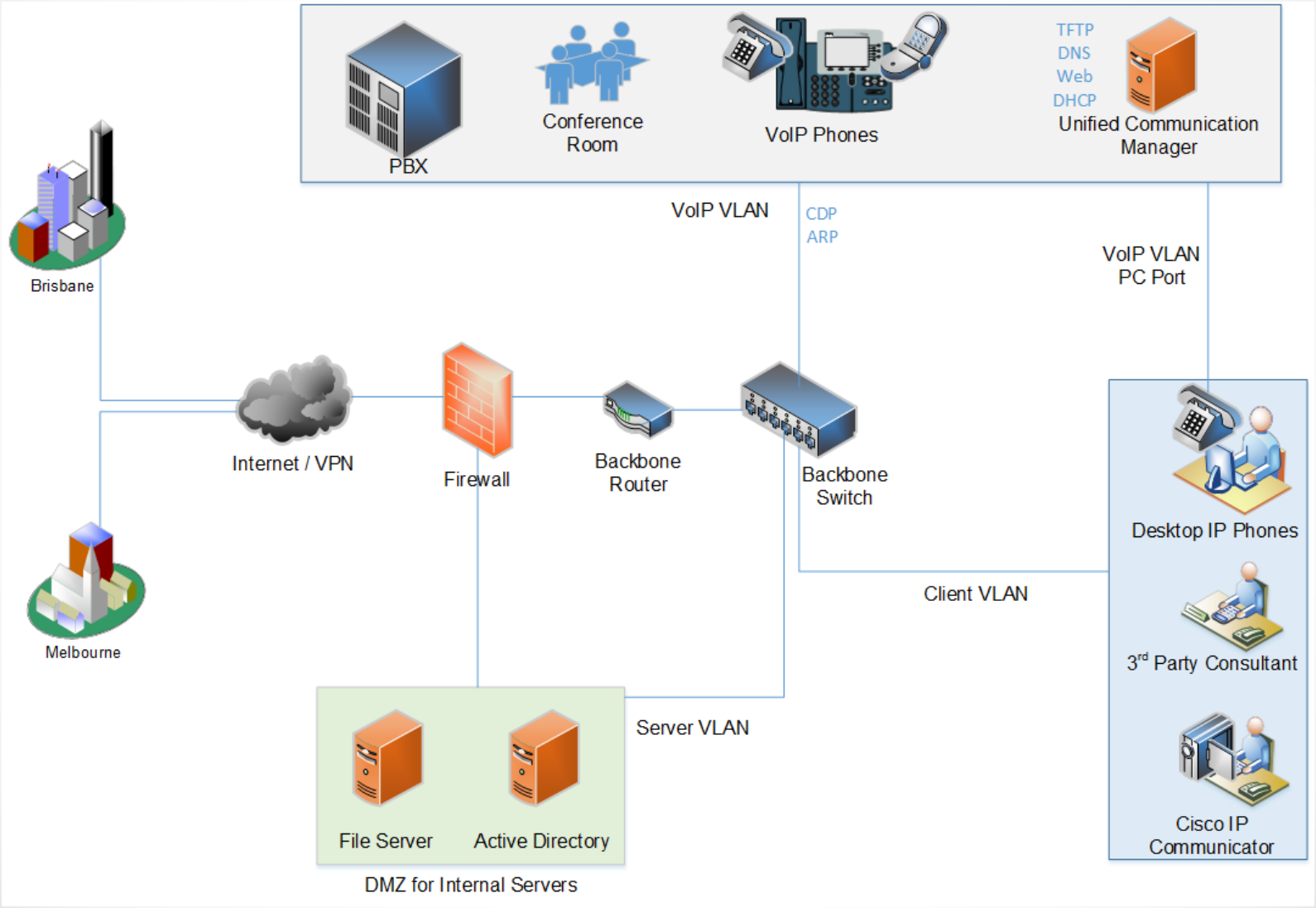
- Viproy, Vulcan'ca "Çağrı/Karar" anlamına gelmektedir

- Viproy VoIP sızma aracı
  - Metasploit Framework test modülleri paketi
  - Hızlı test geliştirme için SIP & Skinny kütüphaneleri
  - Özel SIP başlıkları 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

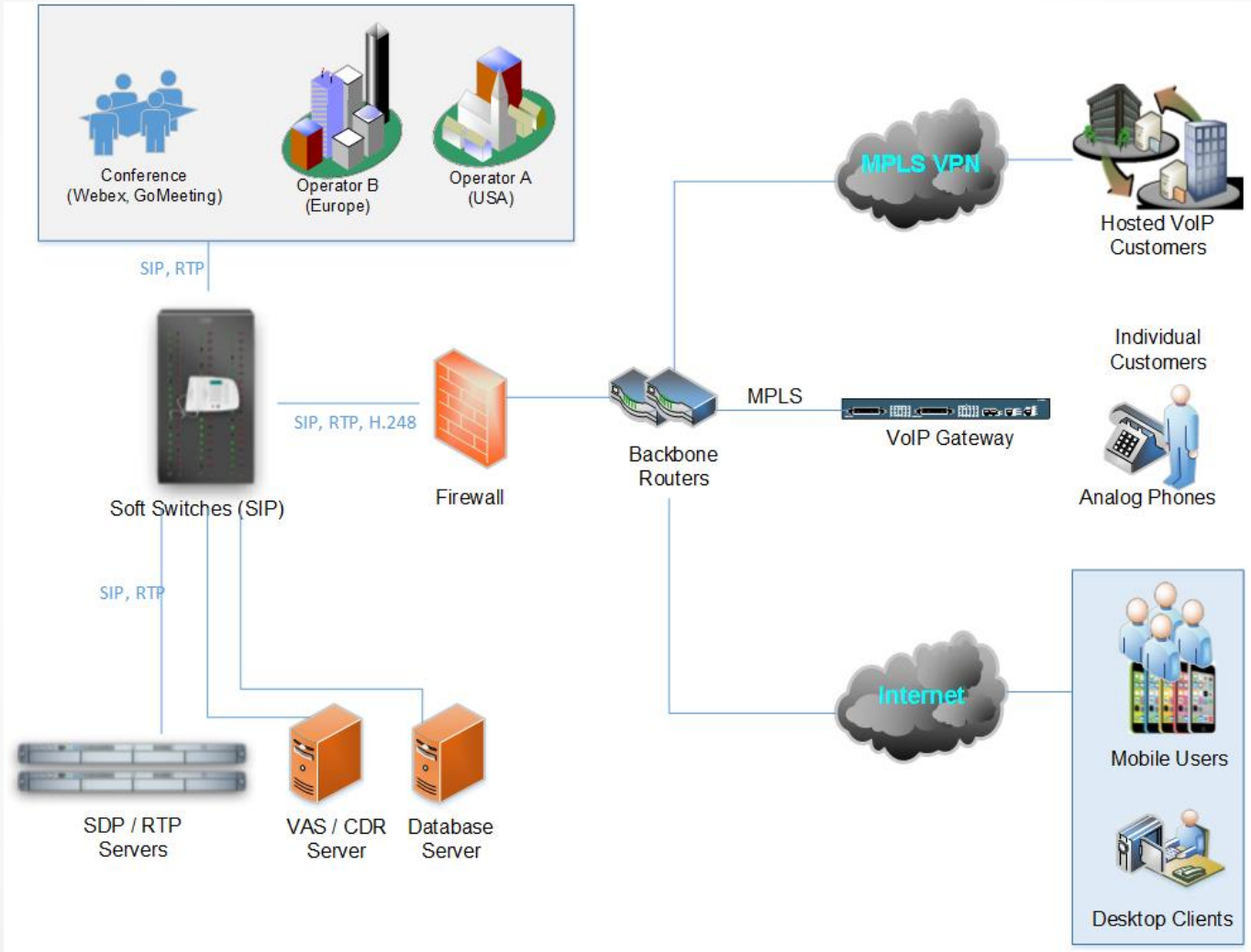
Güvenlik Denetimi ve Özgür Yazılımlar

- 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

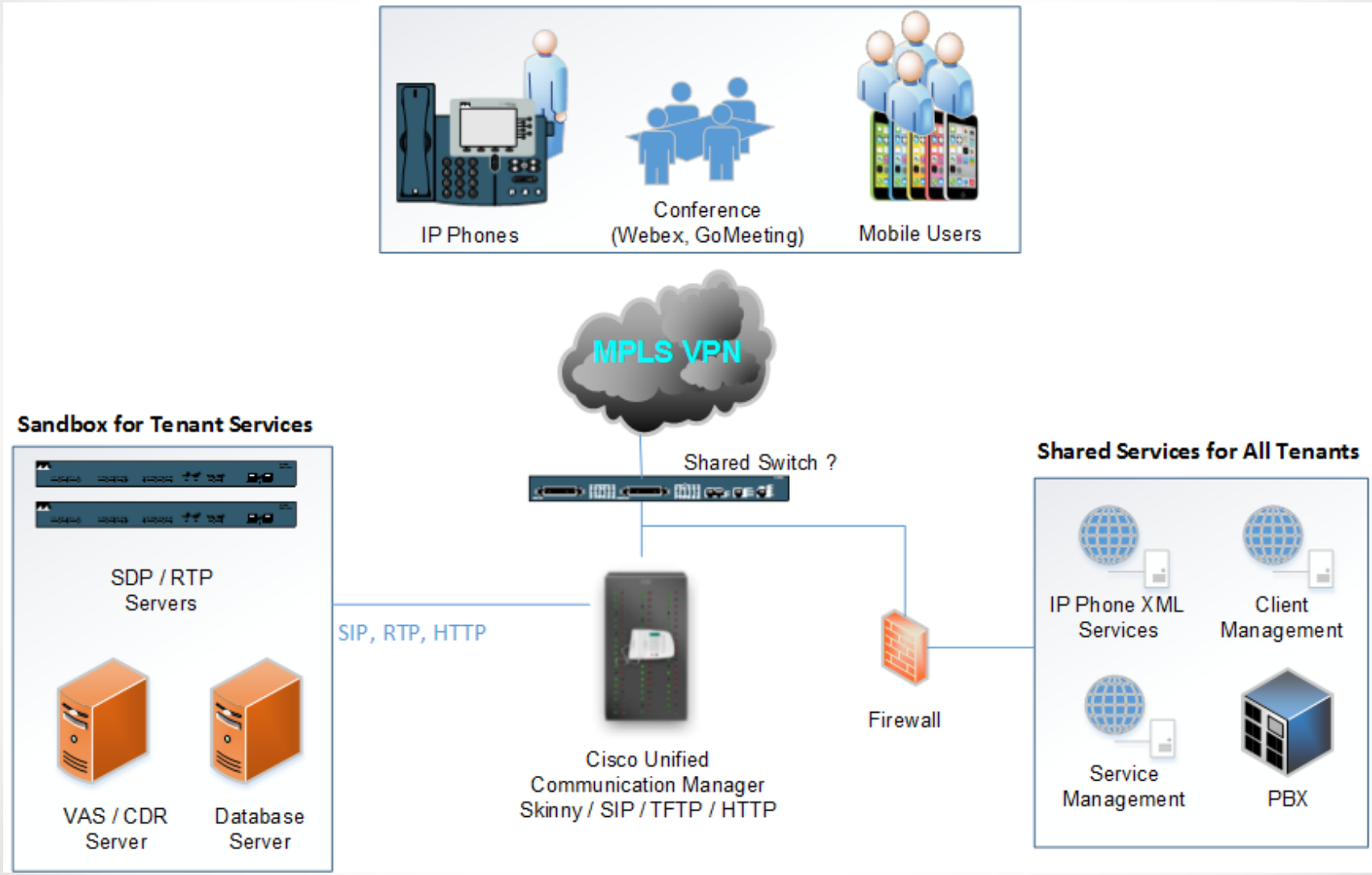
Kurumsal VoIP Ağı



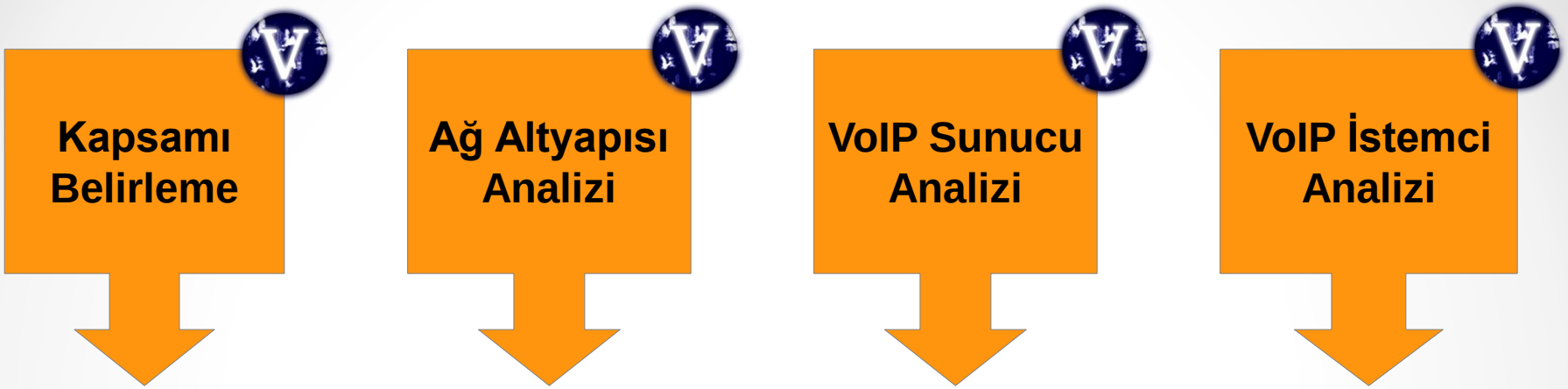
Bütünleşik İletişim (UC)



Bulut VoIP Hizmetleri



Örnek Denetim Rotası



- Sunucuları Saptama
- İstemcileri Saptama
- Ağı Kavrama
- Bilgi Toplama

- Altyapı Keşfi
- SSL/TLS Analizi
- Paket Yakalama
- Çağrı Çözümleme
- Servis Engelleme

- Kimlik Deneme
- Yetki Analizi
- Özel Çağrılar
- Yazılım Sorunları
- Yönetim Sorunları
- Özel Testler

- Doğrudan Çağrı
- Yazılım Sorunları
- Yönetim Sorunları
- Özel Testler

Denetim Kapsamının Belirlenmesi

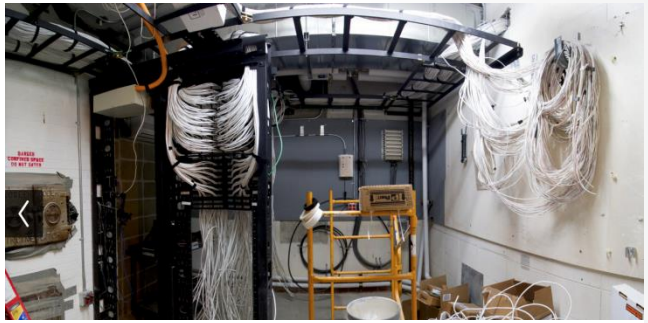
- Denetim bilgilerinde verilenler her zaman yeterli değildir
  - Sunucular (SIP, SIP Proxy, RTP Proxy)
  - İstemciler (Yazılım, Özel Donanım)
  - Ağ Altyapısının Yerleşimi
- Denetim öncesi gerekli bilgiler
  - Donanım ve Yazılımların Türü, Sürümü
  - Seçilen Protokoller ve Seçenekler
  - Yönetim veya 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 alterntifler)
  - Ticari VoIP servisleri (mobil ve bulut çözümleri)
  - Kurumsal kullanım (VLAN, toplantı odaları)
- VoIP protokolleri (SIP, Skinny, RTP, IAX, Diameter)

Fiziksel Erişim Analizi

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



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

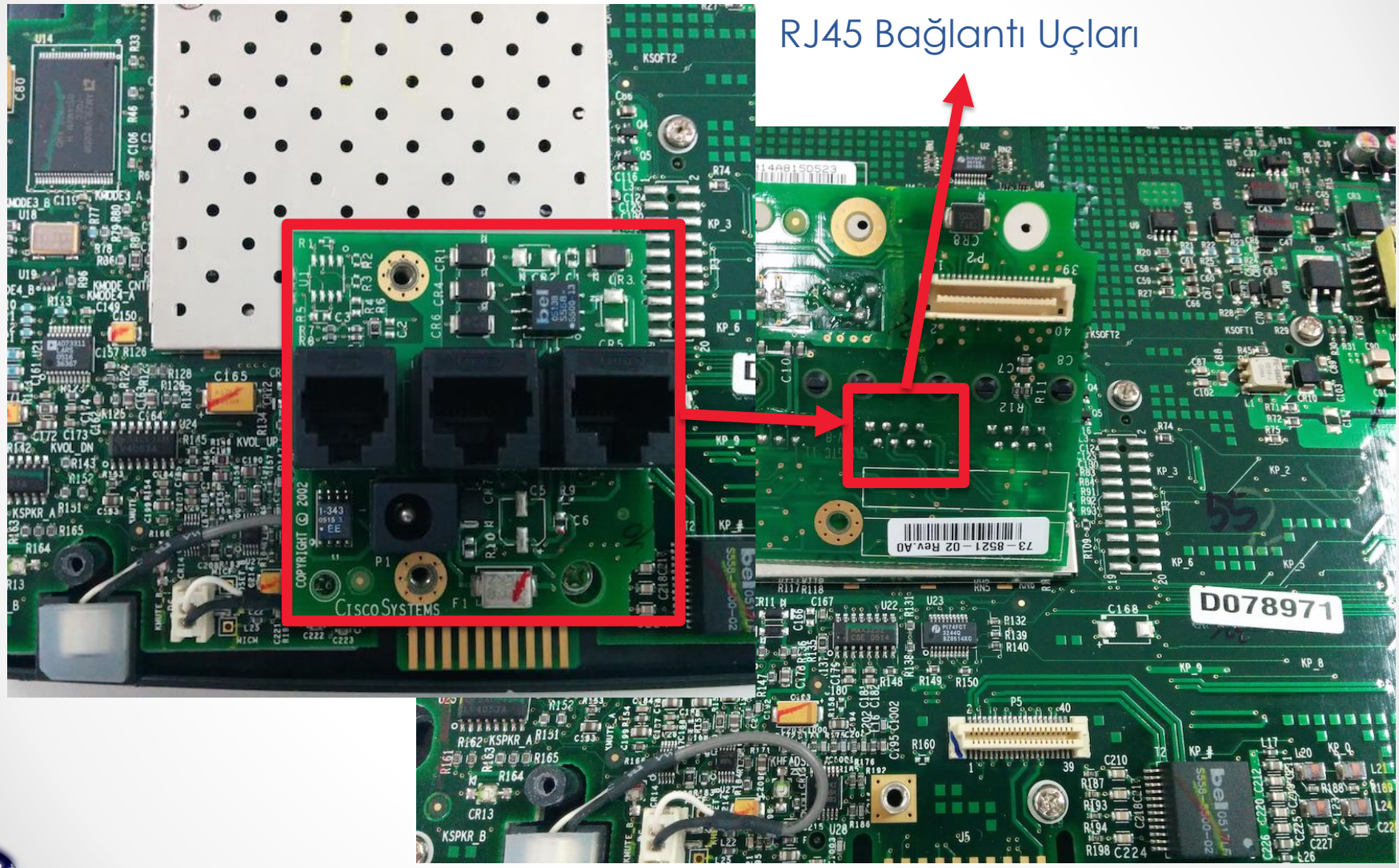
There is considerable evidence to suggest that Australia's copper network is in a worse state than those of other nations. How bad is it and can it be fixed?

CREDIT: MAGILLA (CANOFWORMS.ORG)

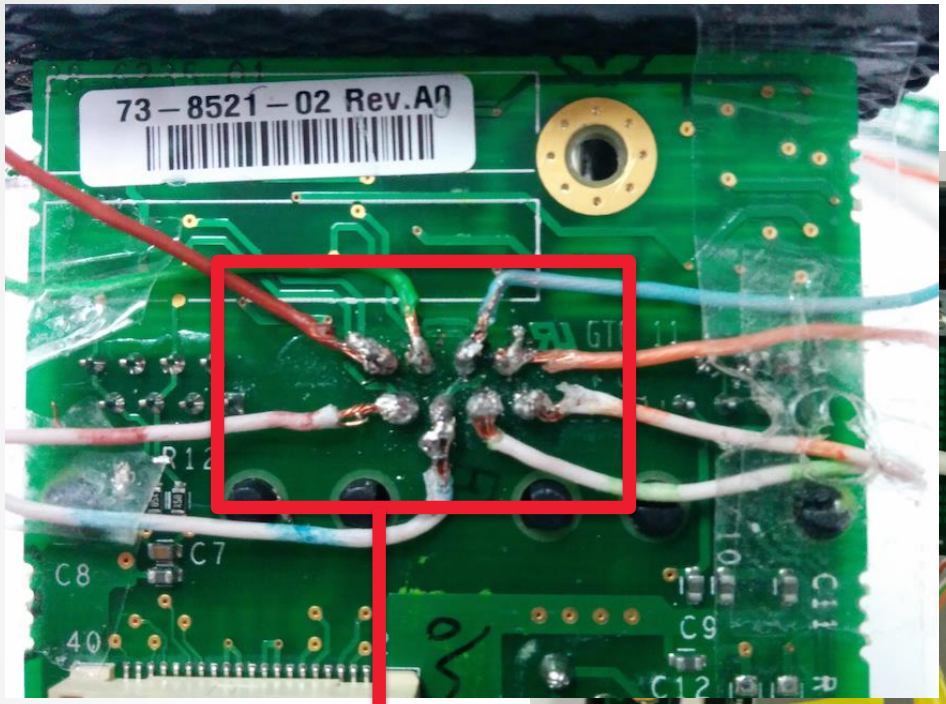
VoIP Ağına Fiziksel Erişim

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

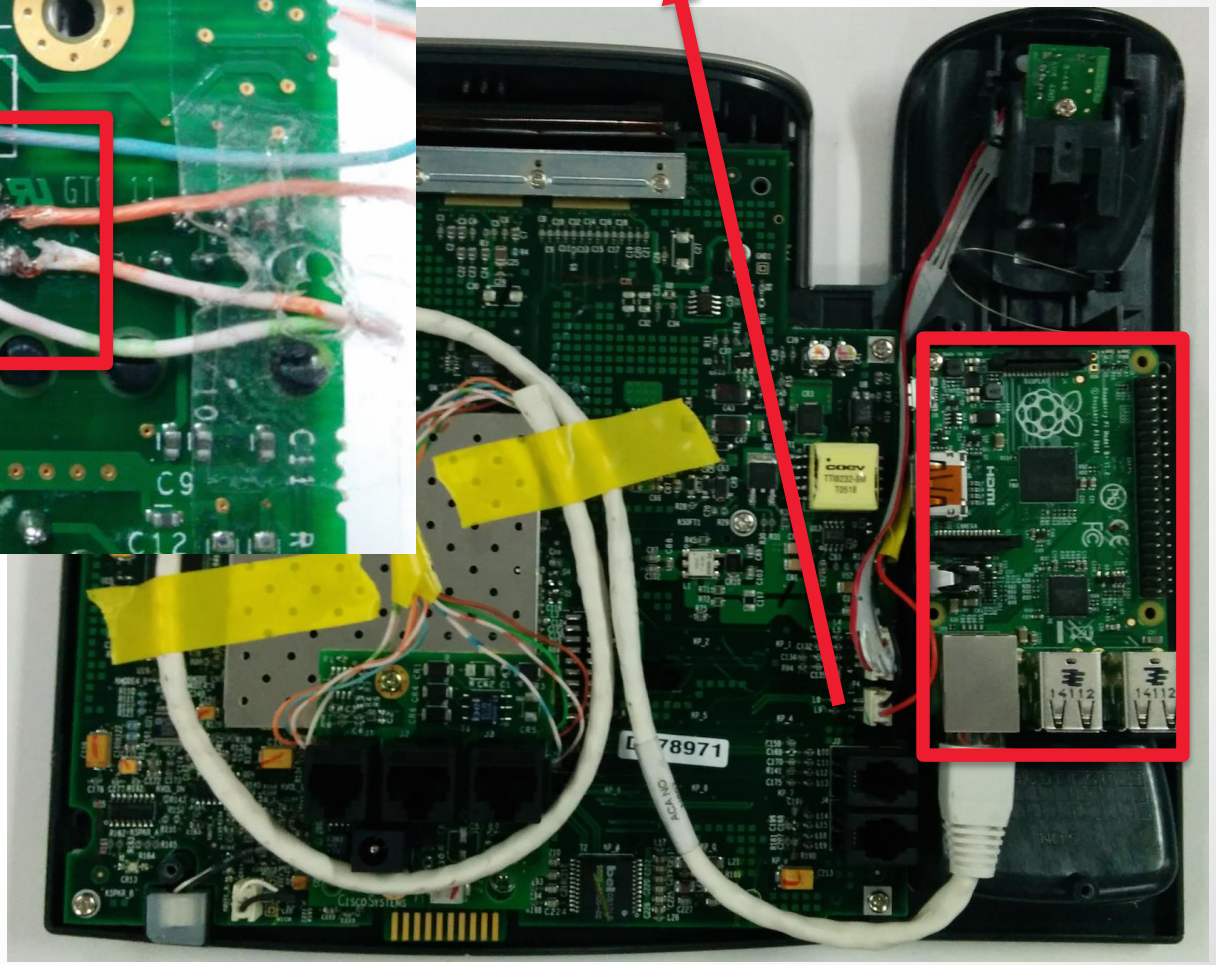
Kalıcı Erişim için Tapberry Pi



Kalıcı Erişim için Tapberry Pi



Hoparlör Bağlantısı



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 davranmak 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 = Sinyaleşme + 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 İletişim (UC)

Temel SIP Akışı

Phone A

1- REGISTER

1- 200 OK

2- INVITE

3- 183 Trying

4- 200 OK

4- ACK

SIP Server

3- INVITE

3- 200 OK

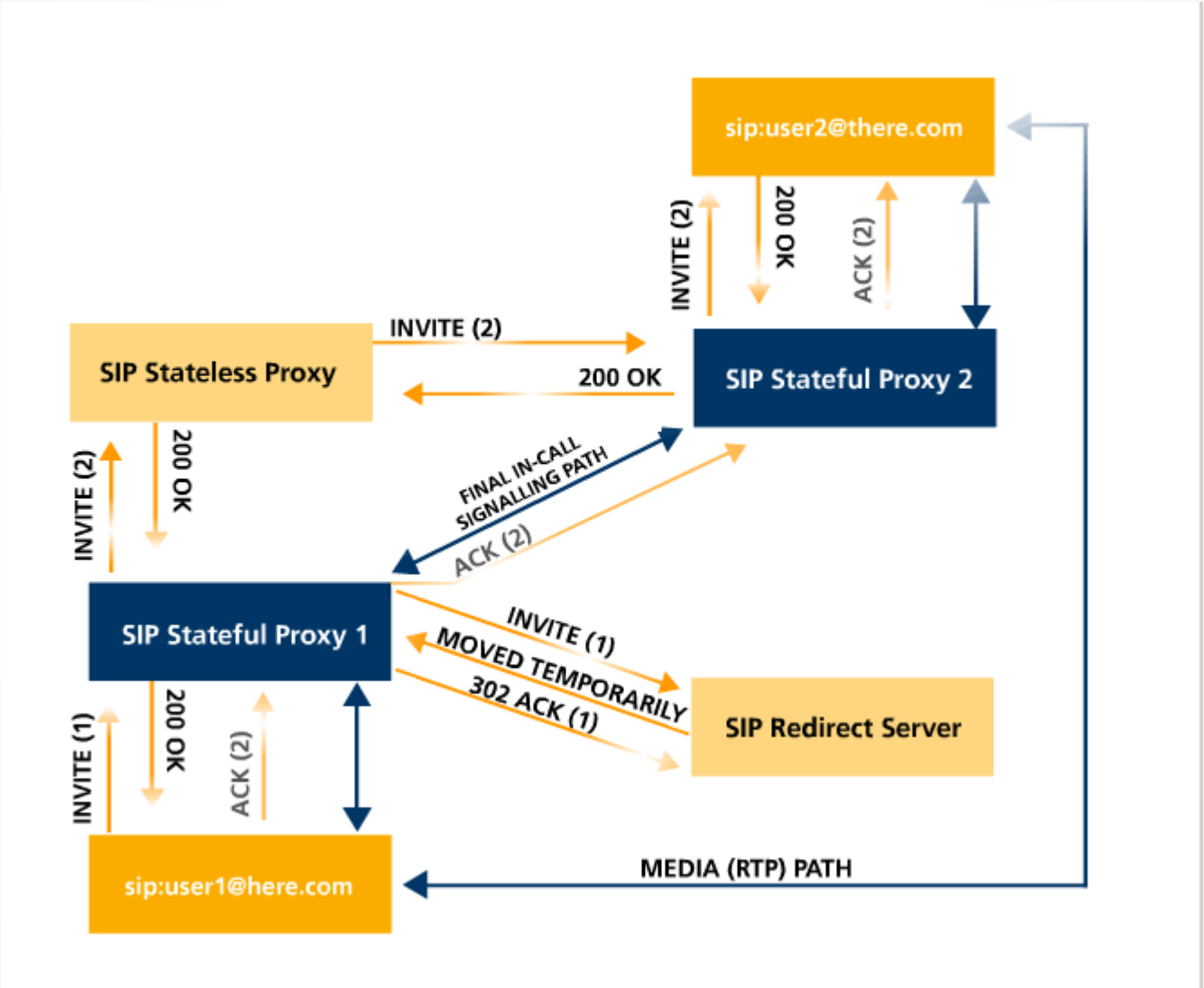
RTP

RTP Proxy

RTP

Phone B

Kısmen Karmaşık SIP Akışı

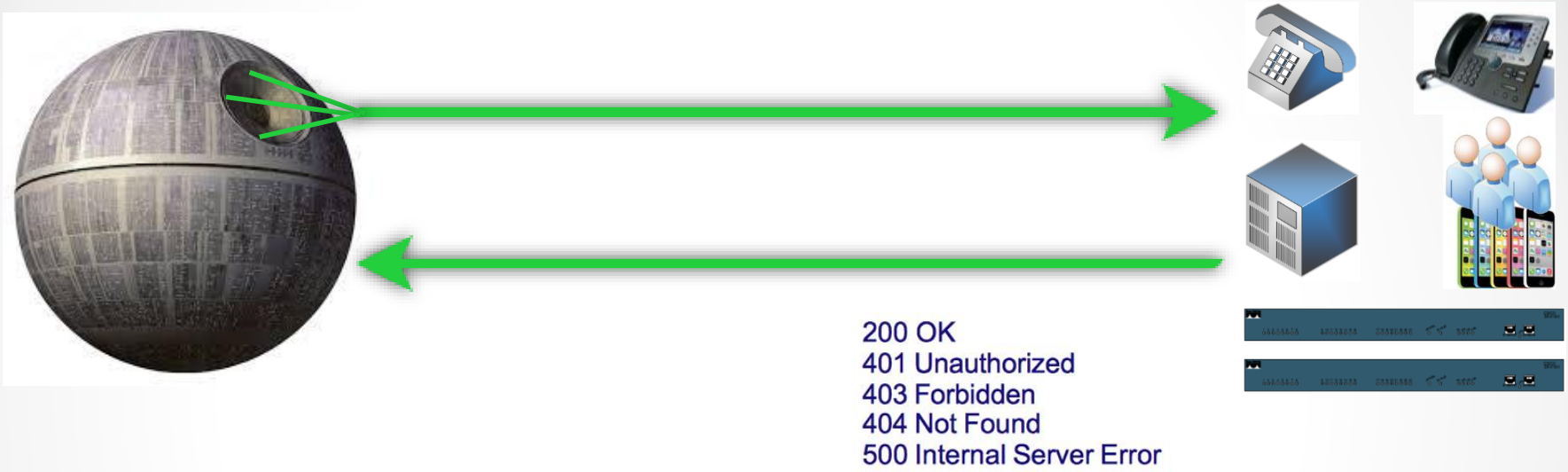


Temel Saldırılar

- 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)



200 OK
401 Unauthorized
403 Forbidden
404 Not Found
500 Internal Server Error

RESPONSE Depends on Information in REQUEST

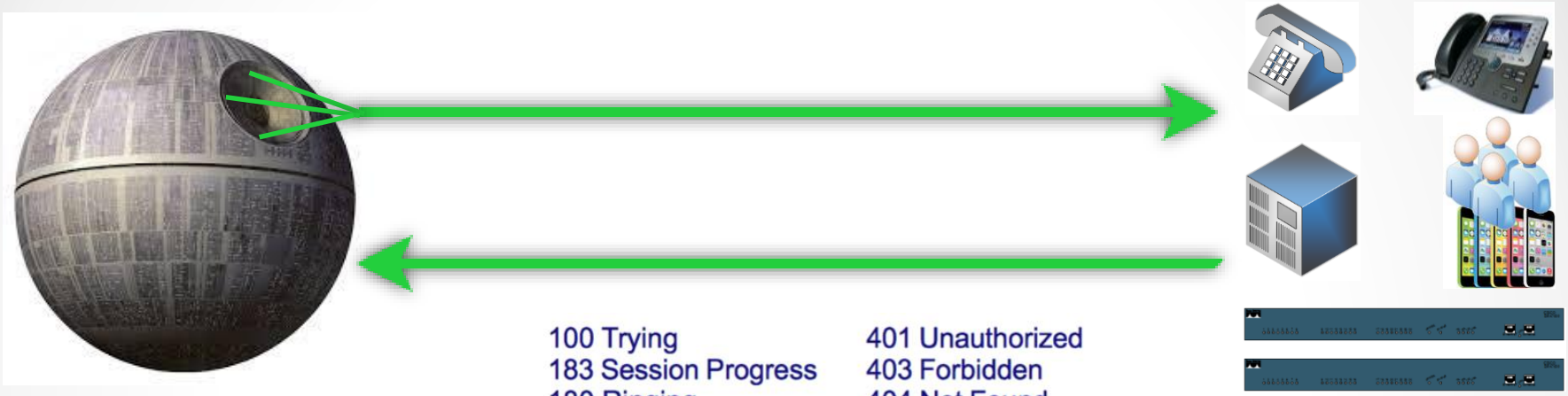
- Type of Request (REGISTER, SUBSCRIBE)
- FROM, TO, Credentials with Realm
- Via

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)



100 Trying
183 Session Progress
180 Ringing
200 OK

401 Unauthorized
403 Forbidden
404 Not Found
500 Internal Server Error

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

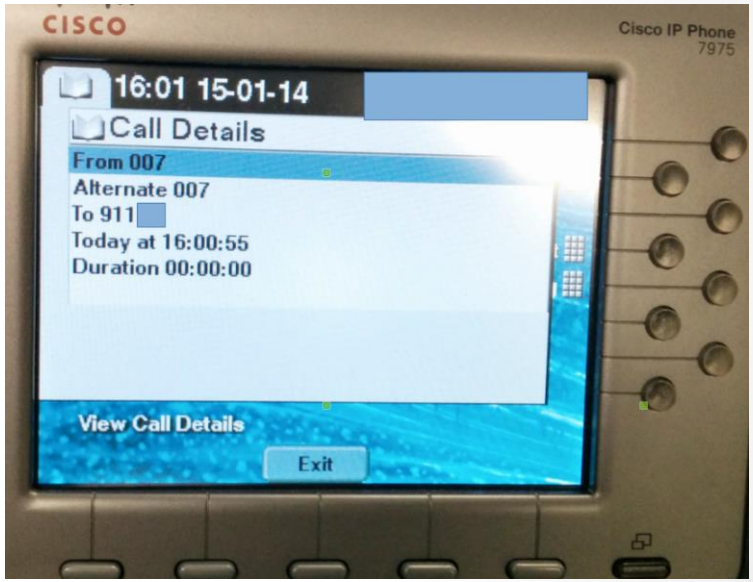
- Brute Force (FROM&TO) for VAS and Gateways
- Testing Call Limits, Unauthenticated Calls, CDR Management
- INVITE Spoofing for Restriction Bypass, Spying, Invoice
- ....

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

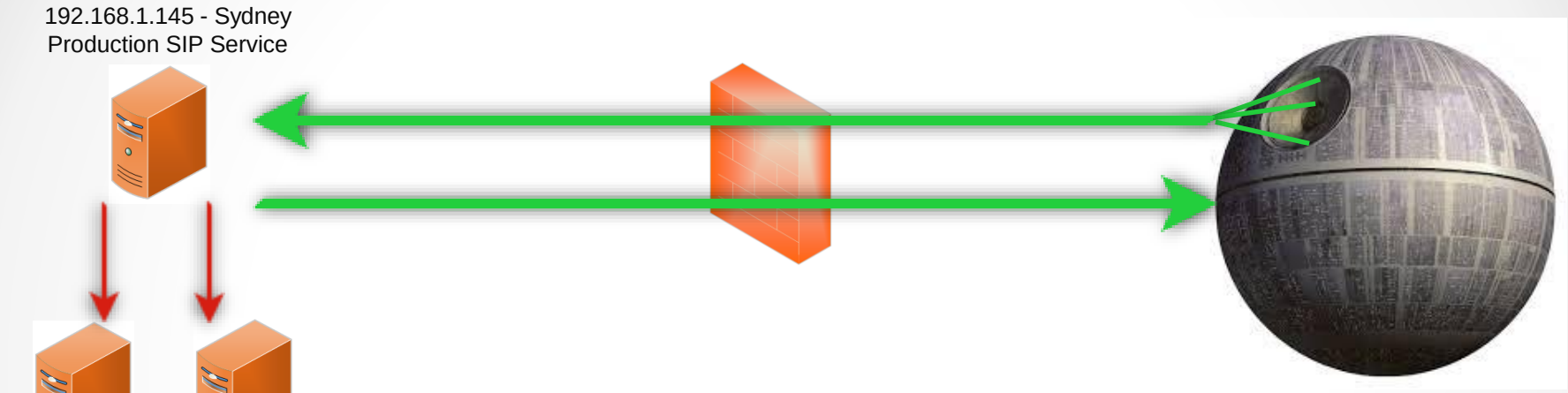
- Tüm operatörler arayan kimliğine güvenirler
- Bir tane etkilenen operatör ile herkes aldatılabilir

İleri Düzey SIP Saldıları

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

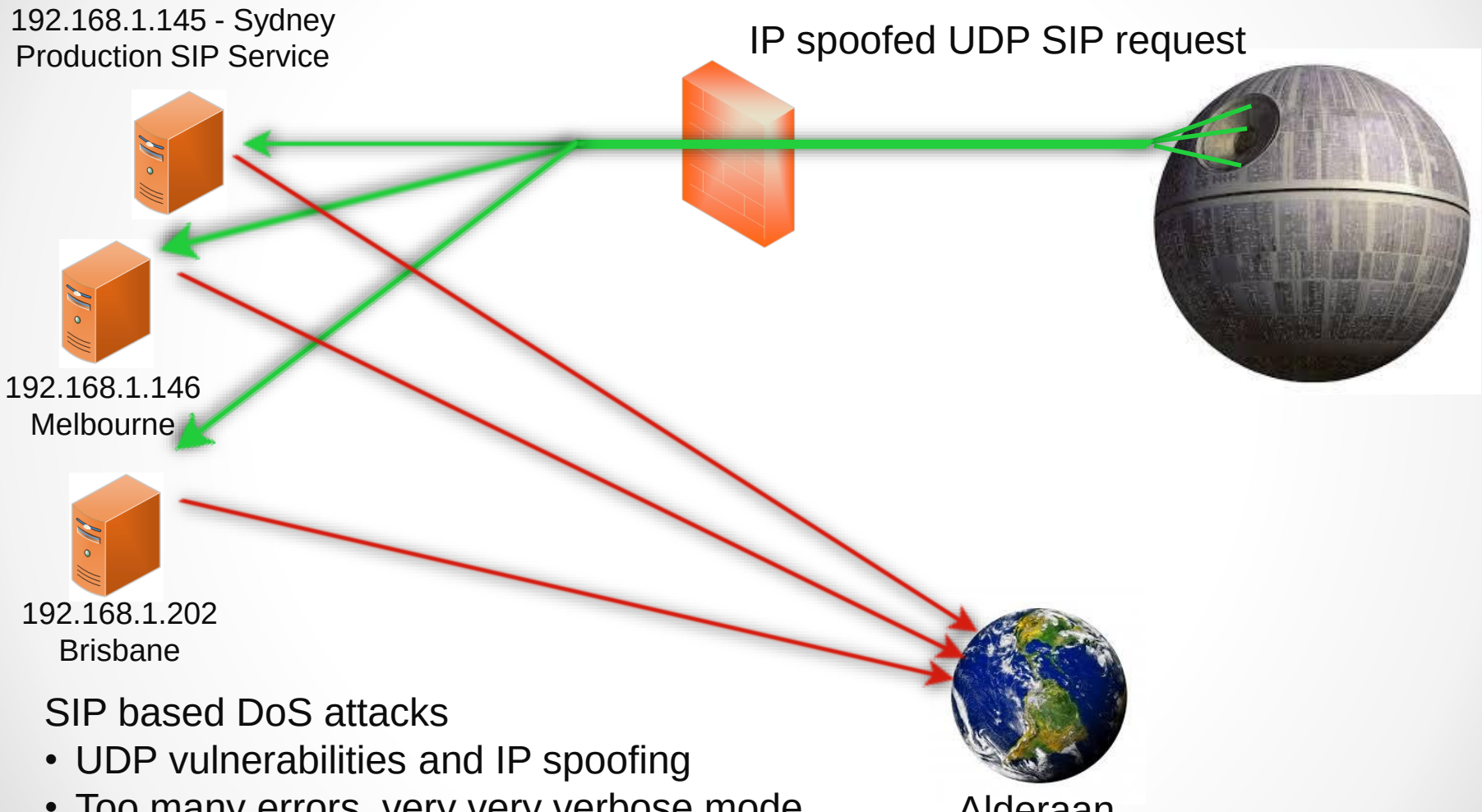
- SIP Proxy atlatma saldırısı
- SIP güven ilişkileri analizi
- Servis engelleme analizi

SIP Proxy Atlatma Saldırısı




```
msf auxiliary(vsipportscan-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)
```

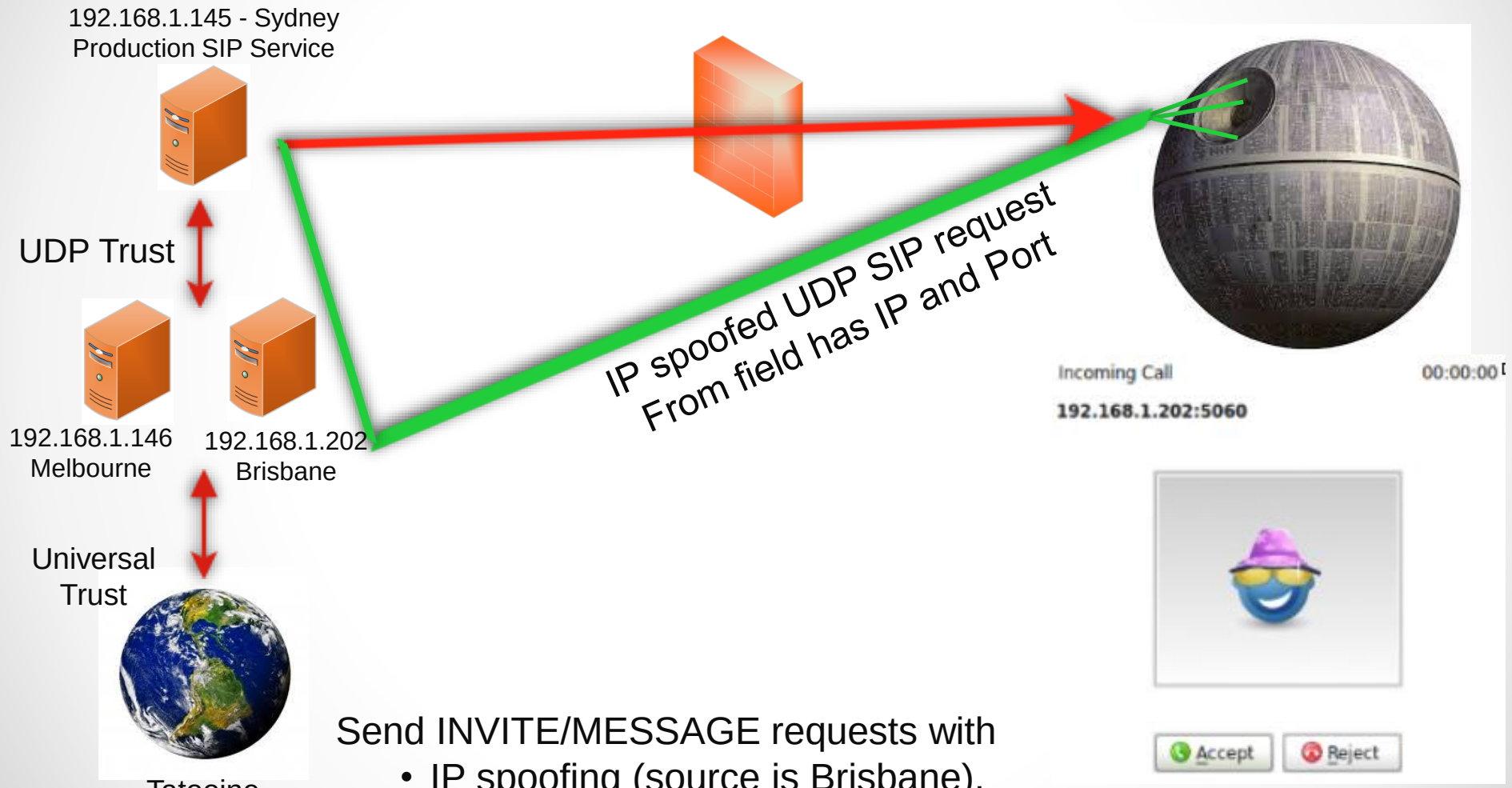
Dağıtık Servis Engelleme Saldırısı



SIP based DoS attacks

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

SIP Güven İlişkileri Analizi

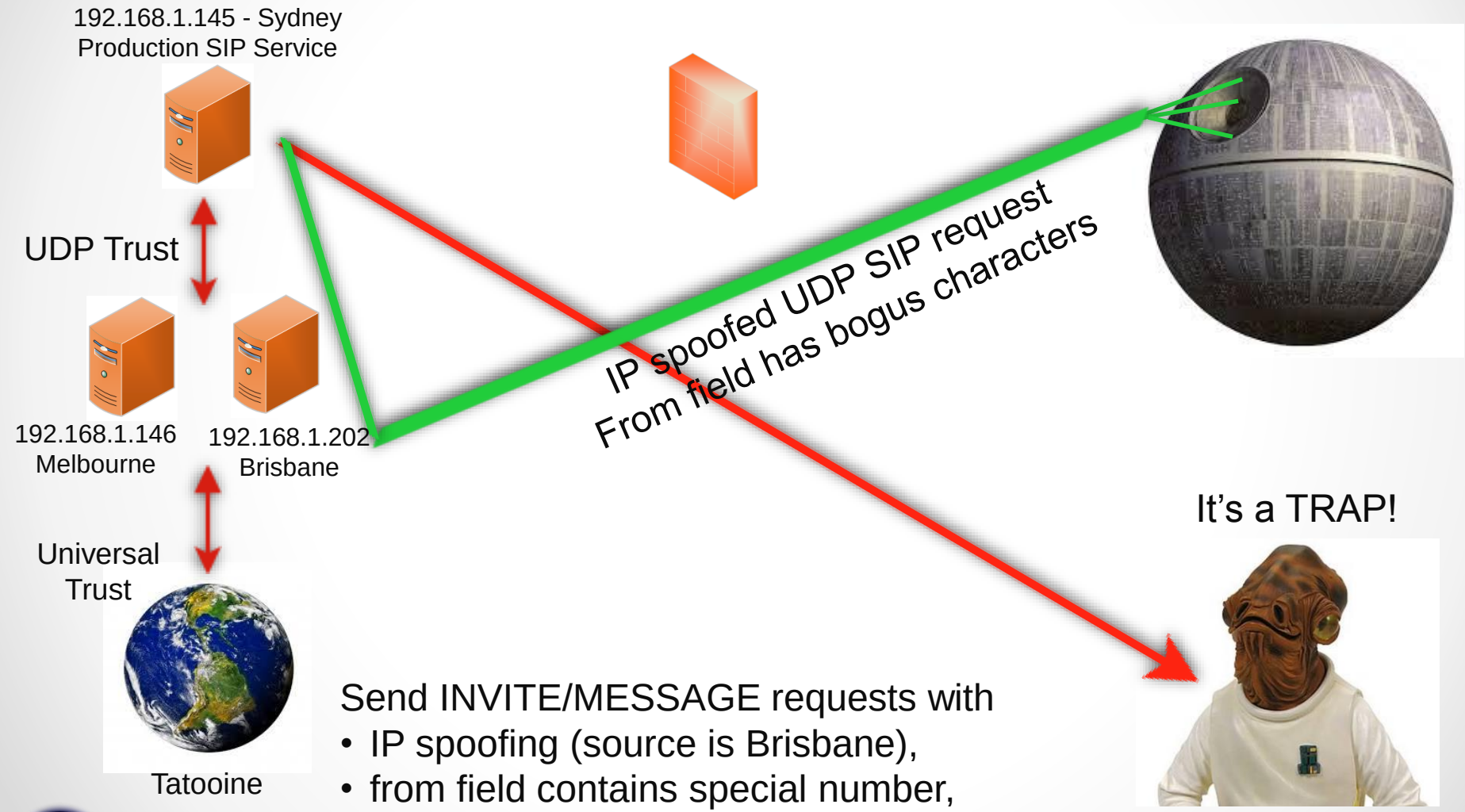


Send INVITE/MESSAGE requests with

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

the caller ID will be your trusted host.

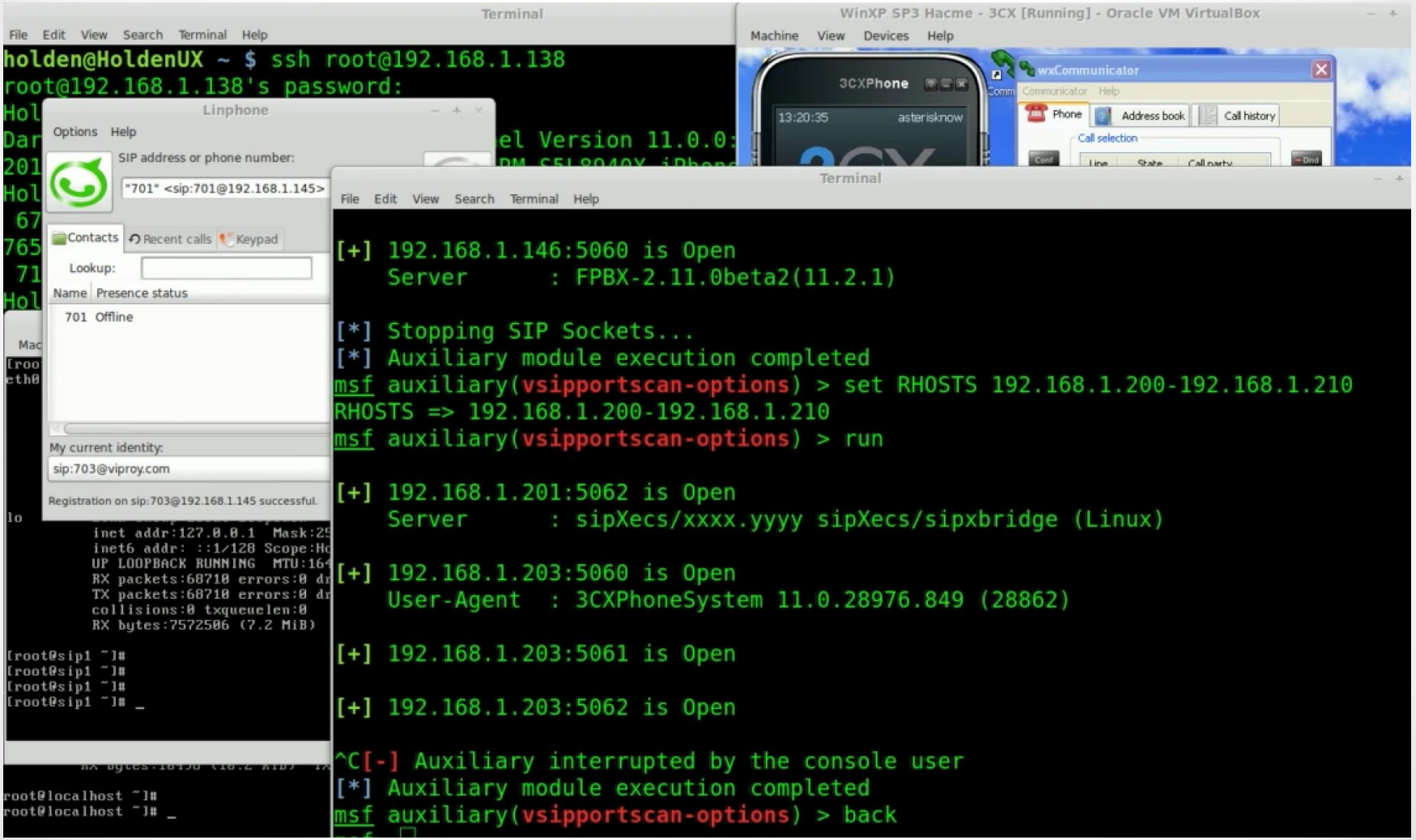
SIP Güven İlişkileri Analizi



Send INVITE/MESSAGE requests with
- IP spoofing (source is Brisbane),
- from field contains special number,

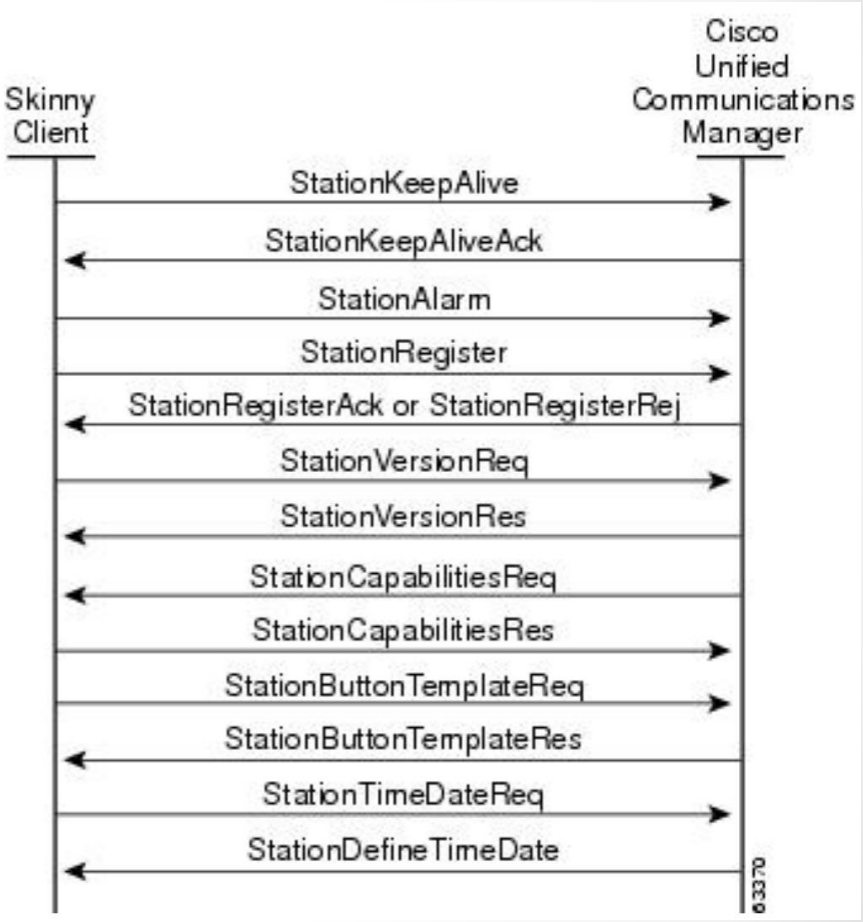
you will have fun or voicemail access.

Viproy ile SIP Analizi



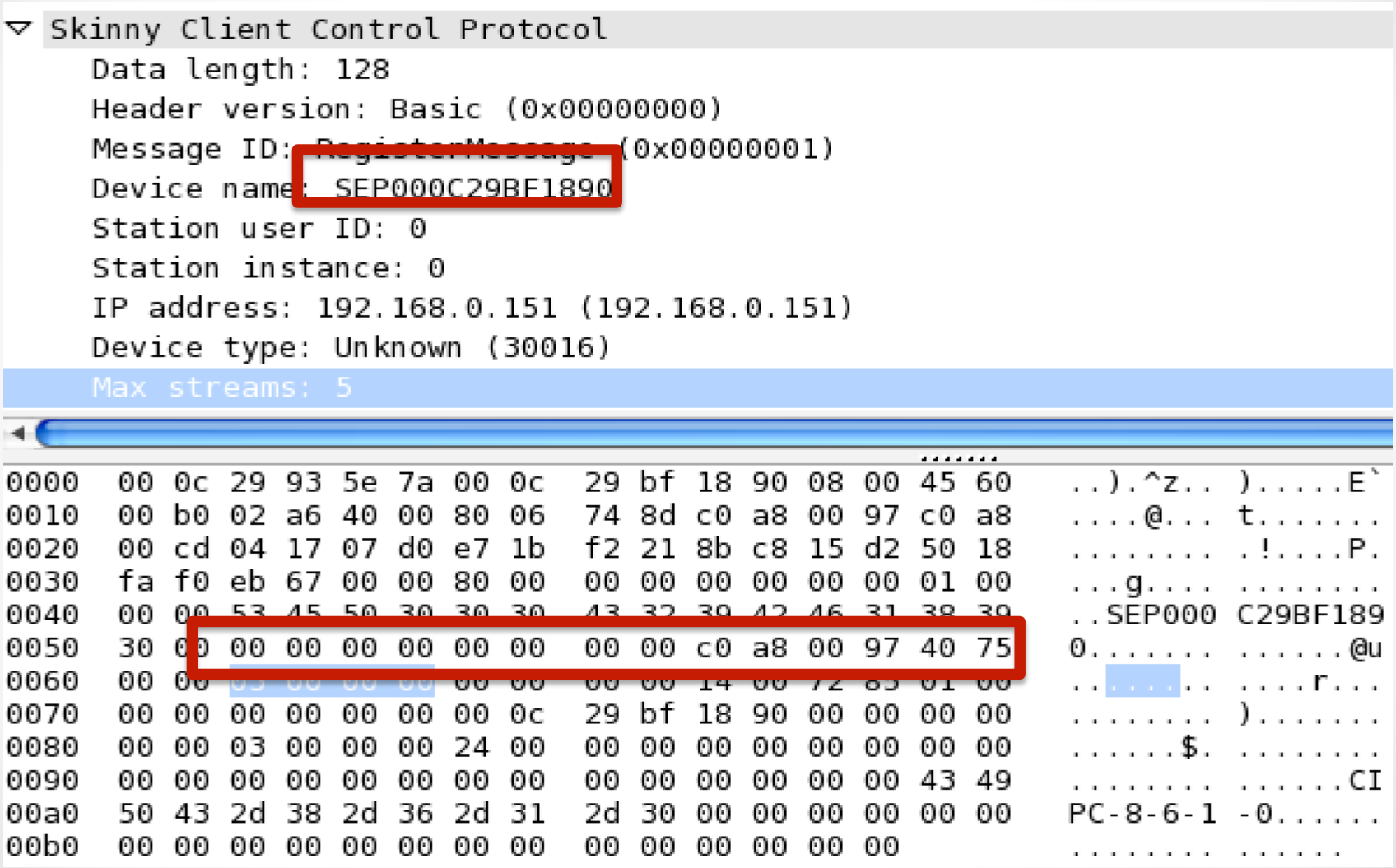
Cisco Skinny

- 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



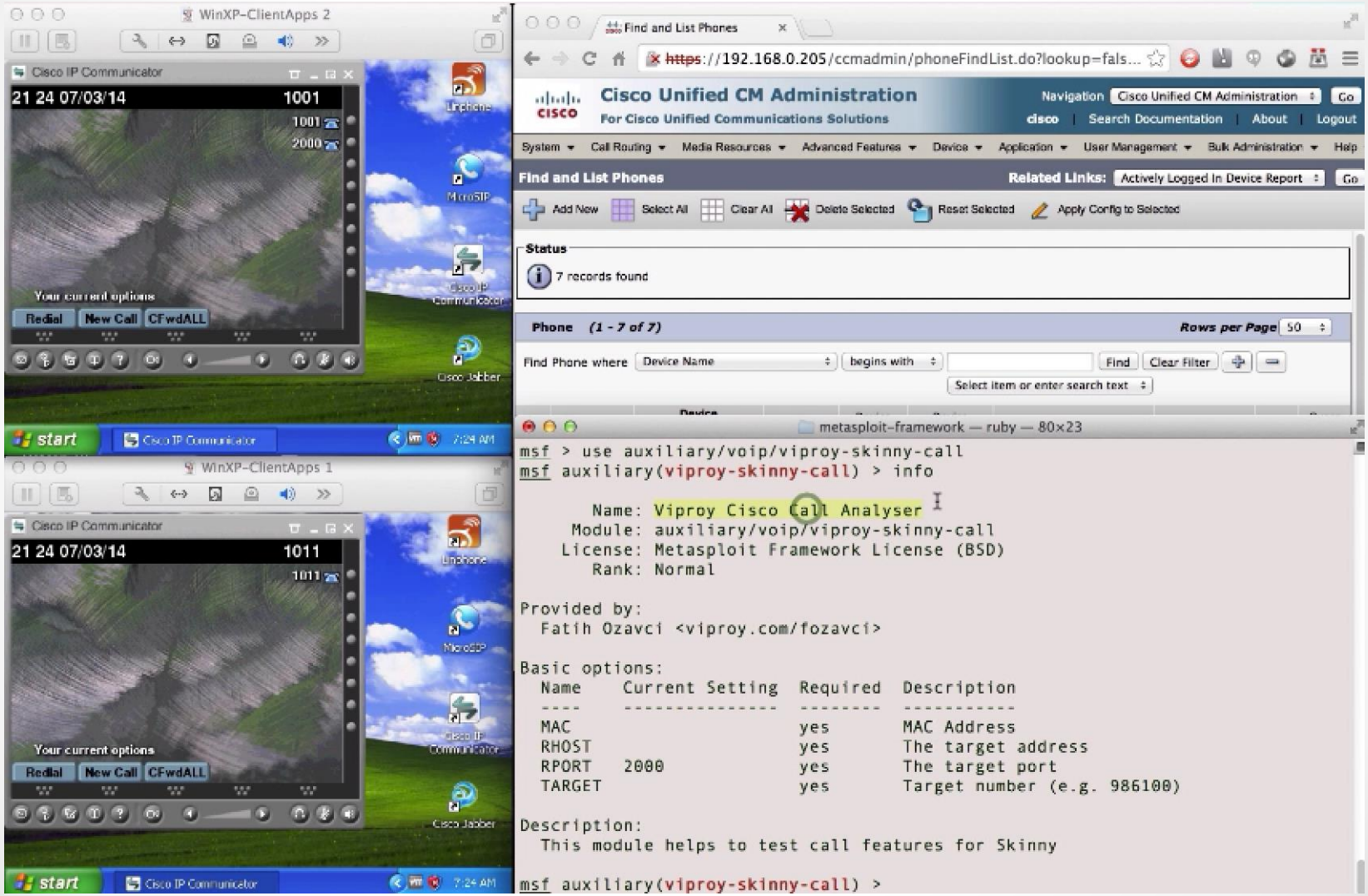
Cisco Skinny Analizi

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

```
def prep_register(device,device_ip)
  p = "\x01\x00\x00\x00" #register message
  p << "#{device}\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00" #device
  p << ip_to_bytes(device_ip) #"\xC0\xA8\n6" #ip address
  p << "5\x01\x00\x00" #device type
  p << "\x03\x00\x00\x00\x00\x00\x00\x00\x06\x00\x00\x84\x01\x
  b=length_to_bytes(p.length,4) #length
  return b+"\x00\x00\x00\x00"+p
end
```

```
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[75,40]
      lines = bytes_to_length(p[116,4])
      speeddials = bytes_to_length(p[120,4])
      m = "Device: #{devicename}\tUser ID: #{use
    when "9b000000"
      r = "CapabilitiesReqMessage"
      m = nil
    when "97000000"
      r = "ButtonTemplateMessage"
      m = nil
    when "21010000"
      r = "ClearPriNotifyMessage"
      m = nil
    when "15010000"
      r = "ClearNotifyMessage"
```

Viproy ile Cisco Skinny Analizi



Viproy için Kaynaklar

- Viproy VoIP Penetration and Exploitation Kit

Author : http://viproy.com/fozavci
Homepage : http://viproy.com
Github: http://www.github.com/fozavci/viproy-voipkit

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

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

- Hacking Trust Relationships Between SIP Gateways

http://viproy.com/files/siptrust.pdf

- VulnVoIP: Örnek zafiyet içeren VoIP sistemi

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

Sorular?

Teşekkürler!