



**VoIP:
Attacks & Countermeasures
in the Corporate World**

Agenda

- Introduction
- Typical VoIP Network Architecture
- Anatomy of VoIP Attacks
- Demo of a few VoIP Attacks
- Countermeasures

Introduction

- Historically trends and advances in IT outpace security requirements. e.g. 802.11 Wireless. VoIP is the same.
- Tools are becoming more readily available.
- Many of the threats against VoIP are the same threats inherited from the data networking world.
e.g. eavesdropping, mitm, replay etc.

Key Threats

- Denial of Service
 - attacks against availability
- Eavesdropping
 - unauthorised interception of voice packets
- Impersonation
 - masquerading as a handset or a piece of VoIP infrastructure

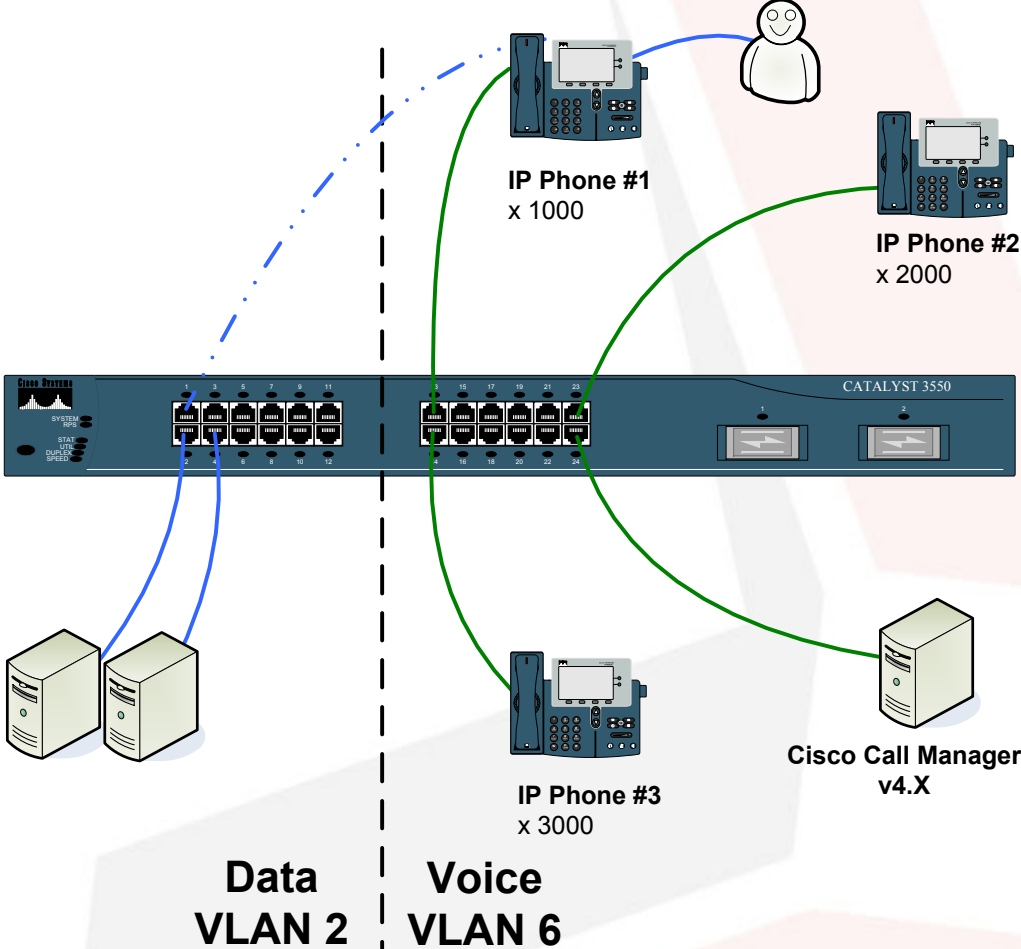
Disclaimer

The techniques demonstrated are not vendor specific.

Our attacks are against an “out of the box” or “default” implementation of VoIP.

We are not responsible for what you do with the tools and techniques demonstrated!

Typical Cisco VoIP Implementation



Anatomy of Attack - Impersonation

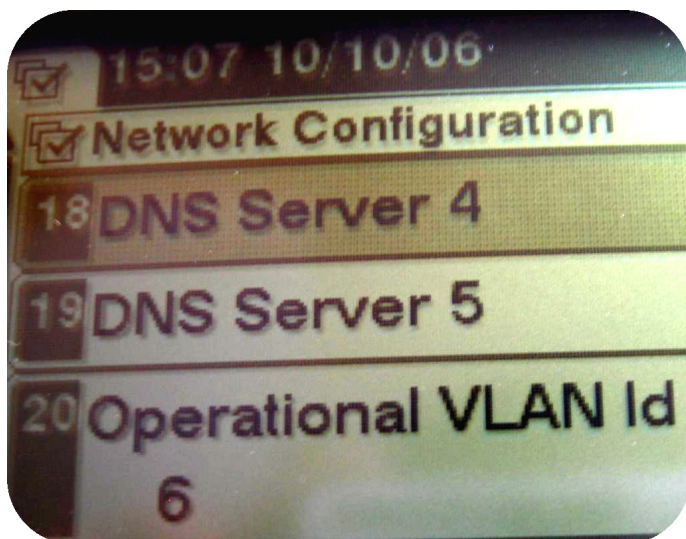
- Step 1: Determine MAC address of handset
- Step 2: Change MAC address on PC
- Step 3: Use Softphone to make a call as that extension

Anatomy of Attack - Eavesdropping

- Step 1: Gather initial information
- Step 2: Get access to voice VLAN
- Step 3: Locate phone targets
- Step 4: Execute ARP poisoning attack and record voice call

Information Gathering

- Cisco phone information disclosure



- IP addresses: DHCP, Call Manager, TFTP, DNS Servers

VoIP Security

- Plug into the PC port and sniff!

The image shows a Wireshark capture of a CDP packet. The packet list pane shows a CDP packet from source 'Cisco_64:97:1e' to destination 'Cisco_e6:d1:cd'. The packet details pane shows the following information:

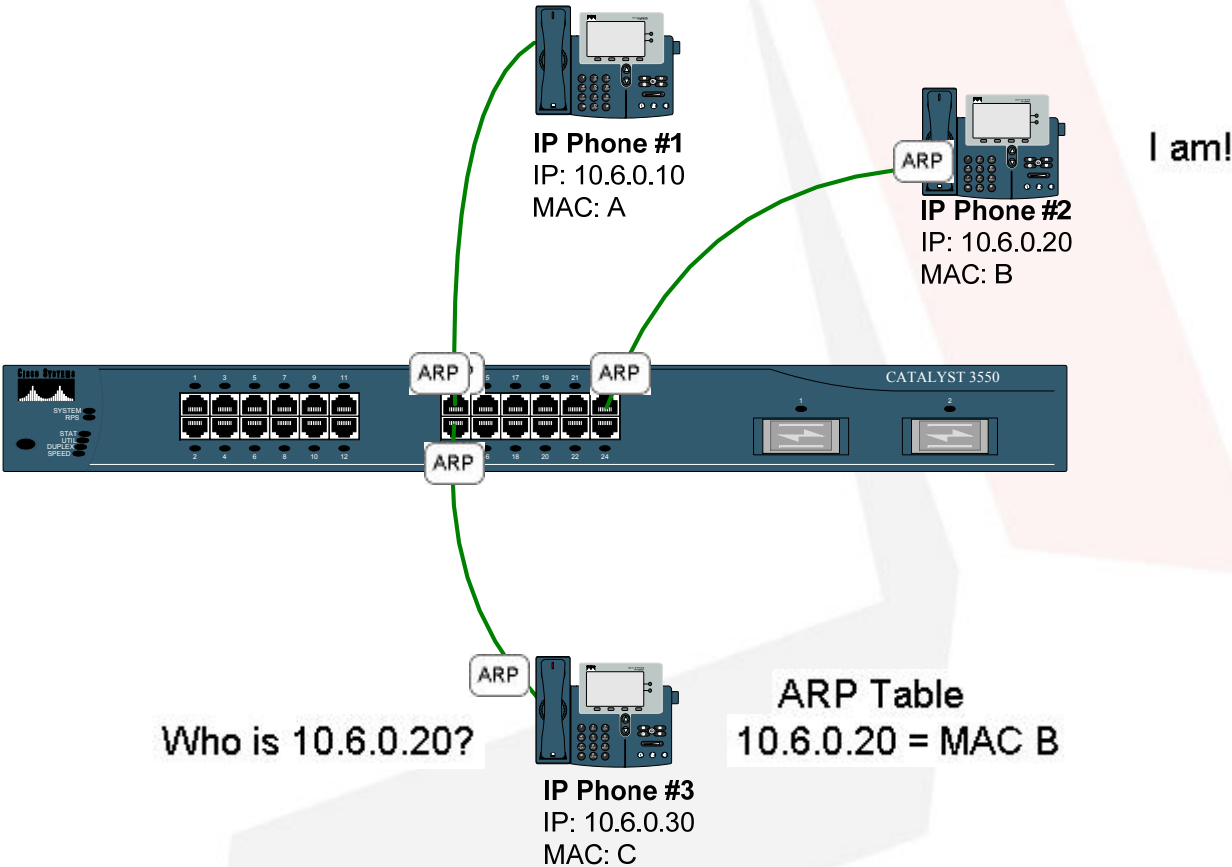
- TTL: 180 seconds
- Checksum: 0x5950
- Device ID: SEP0017E064971E
- Addresses
 - Port ID: Port 2
- Capabilities
- Software Version
- Platform: Cisco IP Phone 7941
- Type: Unknown (0x0019), length: 12
- VoIP VLAN Query: 512
- Native VLAN: 2
 - Type: Native VLAN (0x000a)
 - Length: 6
 - Native VLAN: 2
- Duplex: Full
- VoIP VLAN Reply: 6
 - Type: VoIP VLAN Reply (0x000e)
 - Length: 7
- Data
 - Voice VLAN: 6

The packet bytes pane shows the raw data of the packet, with the 'Voice VLAN: 6' field highlighted in blue and circled in red.

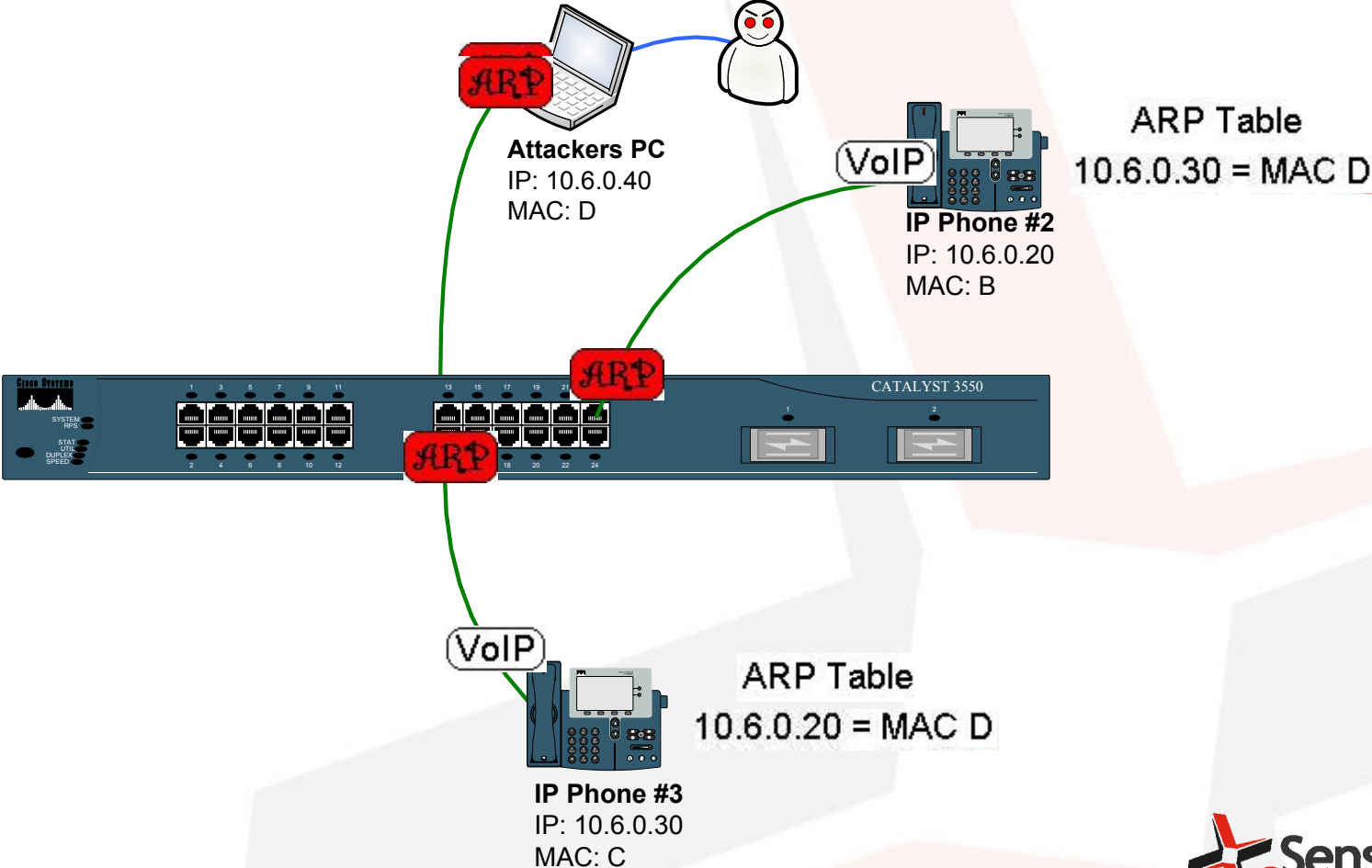
Get on the Voice Network

- Use the info we have gathered to get on the Voice VLAN.
- Configure the network adapter to tag all ethernet frames with the voice VLAN.
- Voila! We are on the voice VLAN.
- Now we can attack any system on the voice network.

MITM Attack - ARP Theory



MITM Attack - ARP Poisoning Theory



MITM Attack - Execution

- Start *Cain & Abel* and configure ARP poisoning.
- *Cain & Abel* also has the capability to record a call.
- Sit back and wait!



VoIP Security

Game Over!



Some Attack Possibilities..

- Telephone banking / Voicemail PIN disclosure
- Insertion of audio into conversation
- Real-time voicemail capture

Compromising the PIN

- Telephone banking requires a user to enter a customer number and PIN using the touchpad.
- Each number pressed sends a unique tone which is interpreted by the end system.



VoIP Security

The image shows a Wireshark network traffic capture window. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, and Help. Below the menu is a toolbar with various icons for file operations, navigation, and analysis. A filter field is present with the text "Expression... Clear Apply".

The main display area shows a list of captured packets. Three packets are highlighted in blue:

- 121 7.685756 SKINNY [TCP out-of-order] SetLampMessage
- 122 7.686051 SKINNY CallInfoMessage
- 123 7.686199 SKINNY [TCP out-of-order] CallInfoMessage

The selected packet (122) is expanded to show the "Skinny Client Control Protocol" details. The data length is 388 bytes. The message ID is "CallInfoMessage (0x0000008f)". The calling party name is "Nathan Besh" and the calling party number is "4443". Other fields include "Called Party Name", "Line Instance: 1", "Call Identifier: 1166", "Call Type: outBoundCall (2)", "Original Called Party Name", "Original Called Party: 8500", "LastRedirectingPartyName", "LastRedirectingParty", "OriginalCdpnRedirectReason: 0", "LastRedirectingReason: 0", "CgpnVoiceMailbox: 4443", "CdpnVoiceMailbox", "OriginalCdpnVoiceMailbox", "LastRedirectingVoiceMailbox", "CallInstance: 1", "CallSecurityStatus: callSecurityStatusNotAuthenticated (1)", and "partyPIRestrictionBits".

At the bottom, a hex dump shows the raw data of the packet, with a corresponding ASCII representation of the calling party name and number.



- But which buttons were pressed?

The image shows a Wireshark network traffic capture. The packet list pane shows three packets:

No.	Time	Source	Destination	Protocol	Info
744	11.433418			RTP	Payload type=ITU-T G.711 PCMU, SSRC=809859382, Seq=329
745	11.452063			SKINNY	KeypadButtonMessage
746	11.452085			RTP	Payload type=ITU-T G.711 PCMU, SSRC=1204256856, Seq=17

The packet details pane for packet 745 (SKINNY KeypadButtonMessage) is expanded, showing:

- Frame 745 (78 bytes on wire, 78 bytes captured)
- Ethernet II, Src: Cisco_1c:9a:91 (00:17:e0:1c:9a:91), Dst: Foxconn_29:d2:d3 (00:15:58:29:d2:d3)
- Internet Protocol, Src: (), Dst: ()
- Transmission Control Protocol, Src Port: 49935 (49935), Dst Port: 2000 (2000), Seq: 164, Ack: 2376, Len: 24
- skinny Client Control Protocol
 - Data Length: 16
 - Reserved: 0x00000000
 - Message ID: KeypadButtonMessage (0x00000003)
 - KeypadButton: Four (0x00000004)

The packet bytes pane shows the raw data in hexadecimal and ASCII:

```
0000 00 15 58 29 d2 d3 00 17 e0 1c 9a 91 08 00 45 68 ..X).... ..Eh
0010 00 40 8b 0e 00 00 20 06 fa f2 0a 05 00 3c 0a 05 .@.... ..<..
0020 00 0a c3 0f 07 d0 4c aa 70 f1 d7 31 d0 07 50 18 .....L. p.1..P.
0030 20 00 a5 ab 00 00 10 00 00 00 00 00 00 00 03 00 .....
0040 00 00 04 00 00 00 01 00 00 00 8e 04 00 00 .....

```



Countermeasures

Cisco Switch:

- Enable DHCP Snooping
- Enable Dynamic ARP Inspection
- Enable IP Sourceguard
- Enable Port Security
- Implement VLAN ACLs
- Implement 802.1x

Countermeasures (cont.d)

Cisco Call Manager: (Not without some side effects!)

- Disable Settings button on phone
- Disable Span to PC port
- Disable Gratuitous ARP
- Disable PC Voice VLAN Access
- Configure Signaling & Media Encryption!

How Real is the Threat in Australia?

- One Australian organisation suffers a major telephone hack each and every day.
- AusCERT Computer Crime and Security Survey 2006 shows average value of loss of over \$60,000.
- The largest phone hack on record is \$1.7M.
- 97% not reported due to risk of adverse publicity.
- Threat to phone service - how would your business cope without phones for an entire day?
- Telstra, Optus and Macquarie Telecom have written to clients warning of the dangers and confirming the customer is liable.

Conclusion

- Most current implementations of VoIP are insecure.
- VoIP can be secured with the right know how.
- The only way to know if your implementation is secure is to have it audited by independent experts.

Questions?

Contact:

Jason Edelstein

T: +61 2 9290 4441

E: jason@senseofsecurity.com.au

www.senseofsecurity.com.au