Cisco IP Telephony 보안 솔루션

2004.10.20

Bang, Hang Mo (banha@cisco.com)

목차

- **IP Telephony**의 보안 위협
- **IP Telephony** 보안 전개 모델
- **IP Telephony** 보안 기술
  - **Infrastructure Security**
  - **IP Phone** 자체 보안 기능
  - **Cisco Call Manager** 시스템 보안
- **Summary**

IP Telephony의 보안 위협

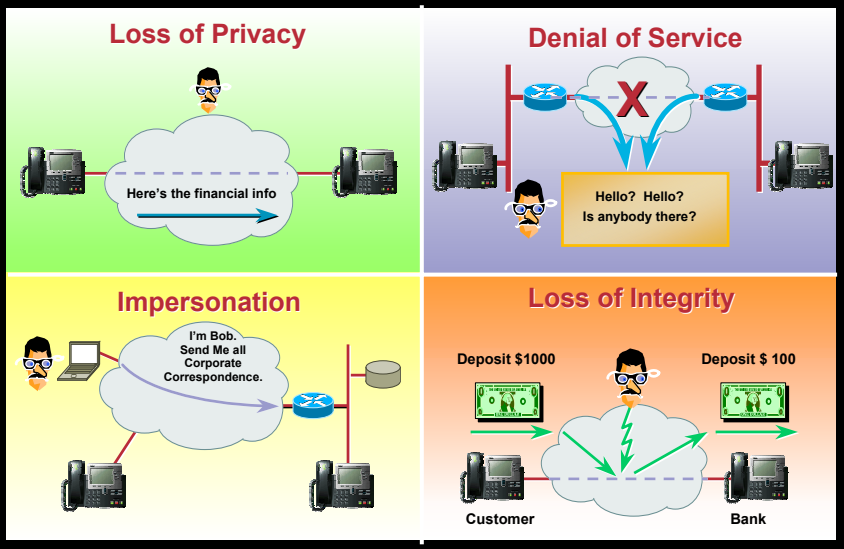
IP Telephony에 대한 보안 요구의 증가

Cisco.com

- Growing technical knowledge and skills
- Increasing leverage through Automation
- Exploiting network access and moving easily through the infrastructure
- Becoming more skilled at masking their behavior

IP Telephony에 대한 보안 위협

Cisco.com



Voice 와 Data의 보안위협

Cisco.com

- IP Telephony **inherits IP Data Network threat** models:
  - **Reconnaissance, DoS, Host Vulnerability Exploit, Surveillance, Hijacking, Identity, Theft, Misuse, etc.**
- QoS requirements of IP Telephony **increase exposure to DoS attacks** that affect:
  - **Delay, Jitter, Packet Loss, Bandwidth**
- **PC endpoints** typically require **user authentication**, **phones** typically allow **any user**
  (exceptions: access/billing codes, Class of Service)
- **User Identity Theft** in traditional PBX phones carries over to IP Telephony… leads to:
  - **Unauthorized Access and Privileges, Service Theft**
- **Device Identity Theft** – malicious devices on the IP network acting like IP phones… leads to:
  - **Reduced Service Availability, Eavesdropping, Inserting/Deleting/Modifying Audio Streams**

IP Telephony Security Axioms

Cisco.com

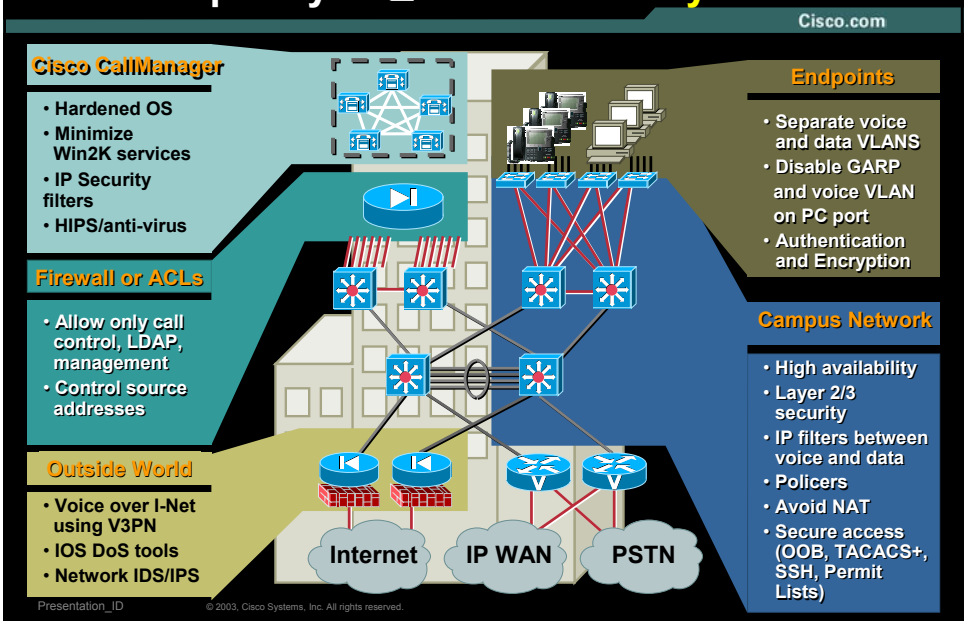
- **Build it in layers** so that the compromise of any one system or feature does not result in the compromise of the entire network.
- **A sound IP Telephony security strategy** is dependent **on a sound data security strategy.**
- Security is a balance between risk avoidance and cost.
- Filter, Filter, Filter

Voice Security =

Physical Protection + Device Hardening + Firewalls & ACLs + IDS/IPS + V3PNs + Availability + Identity + Integrity + Privacy + Monitoring + Remediation

IP Telephony Best Practice

IP Telephony 보안: Build It in Layers



IP Telephony Infrastructure Security

Infrastructure 보안 고려 사항

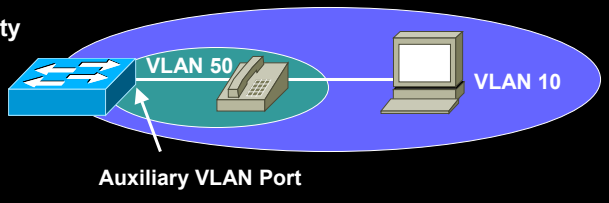
Cisco.com

- Manage switches & routers with SSH, HTTPS, OOB, Permit Lists, etc.
- Separate voice and data VLANs
  - –Use private addresses, avoid NAT
  - –Dedicated VLAN ID for trunks
  - –Never use VLAN 1
  - –Disable unused ports, put them in unused VLAN
- Actively use ACLs
  - –Group assets along bit-wise boundaries
  - –ARP, GARP, ICMP Redirect, TCP Intercept, etc.
  - –Only allow sources from your known addresses
  - –Protect QoS
- STP attack mitigation (BPDU Guard, Root Guard)

Data And Voice Segmentation

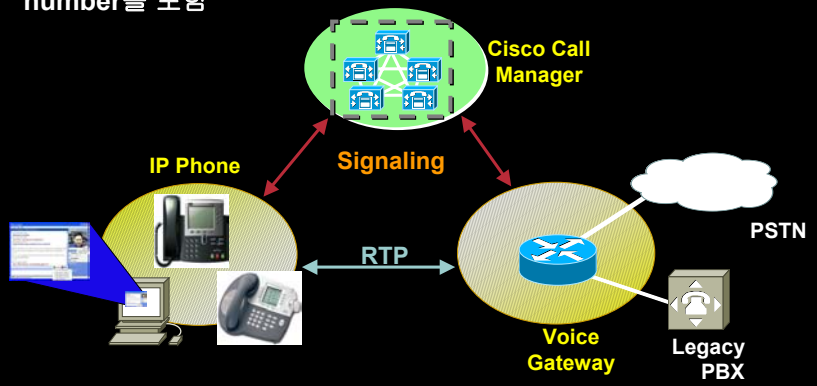
Cisco.com

- IP phones typically provide access to both segments
  - –IP phones support a “data port” for the local PC so that only a single cable is necessary
  - –Don’t rely solely on VLANs for separation – in the interest of layered security, also provide Layer 3 filtering at the access layer
- Segmentation also provides opportunities for
  - – Unique QoS policies
  - – Preservation of existing IP address strategy
  - – Scalability
  - – Manageability



Infrastructure Security: Voice Protocol의 기본 구조

- **Signaling protocols** 은 well-known ports를 사용하며, Firewall을 통과 하도록 구성
- Voice는 Undefined UDP ports를 사용하여 **RTP** 로 전달됨
- Signaling packets 은 RTP에서 사용 될 IP address 와 Port number를 포함



Infrastructure Security: Firewall / NAT Voice ALGateways

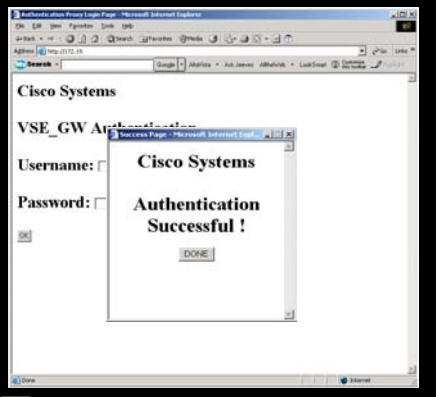
ALG = Application Layer Gateway = Inspection Engines

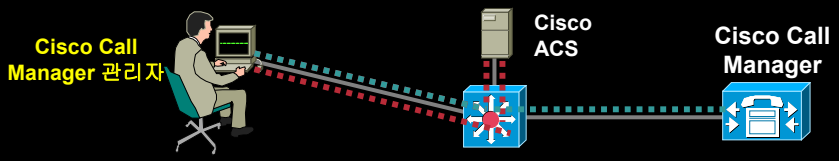
- Voice signaling protocols의 Stateful inspection 지원
- PIX and IOS Firewalls에서 SIP, SCCP, H.323, MGCP 지원
- **Firewall ALG**
  - RTP가 사용할 UDP Port를 알기 위하여 Signaling packet 을 조사함.
  - 사용될 UDP Port를 Dynamical하게 허용
  - 사용이 끝난 UDP Port를 닫기 위하여 End-of-Call signaling을 감시
- **NAT ALG**
  - Signal Packet에서 사용된 사설 Source IP address 및 port number 를 공인 IP address 및 Port로 NAT'ing
- Note: Current ALGs not applicable when voice is authenticated or encrypted!!!

Infrastructure Security : Authentication Proxy 이용

- Dynamic ACL in Cisco IOS
- Allows vulnerable ports to be opened after a AAA challenge when a user makes a connection through a router
- HTTP, FTP, NetBIOS, etc.
- Authorization persists for configurable time
- CCM 앞에 위치한 L3 장비에서 제공(admin and users)

http://10.32.1.10/ccmadmin





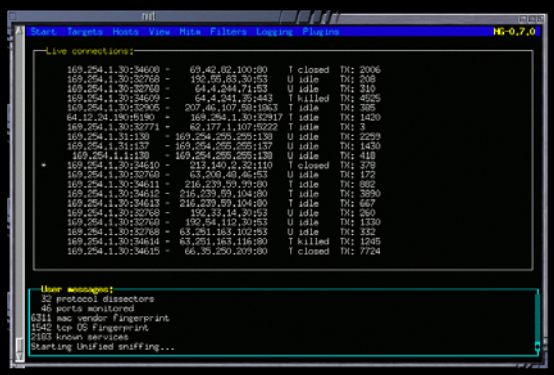
Infrastructure Security: VoIP Hacker Tools

- Ettercap, dsniff—insert themselves as man-in-the-middle by sending gratuitous ARPs to opposing endpoints claiming to be the other end

  Many other manifestations

- VOMIT (Voice over Misconfigured IP Telephony)
  - Converts TCPDump file to WAV file
- Nmap and nessus scan for open ports
- nemesis is a packet creation tool
- macof cam flooding
- Lots of others

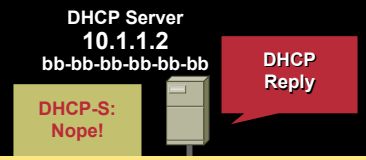
ettercap screenshot



Infrastructure Security: DHCP Spoofing 및 Exhaustion 방지

Cisco.com

- DHCP Snooping creates binding of IP address to MAC address
- Defines ports that can DHCP Reply
- Rate limit DHCP messages
- Resets with loss link



10.1.1.1

```
ip dhcp snooping
ip dhcp snooping vlan <id>

interface FastEthernet1/1
 ip dhcp snooping trust

interface FastEthernet1/2
 ip dhcp snooping limit rate 10
```

10.1.1.1	aa-aa-aa-aa-aa-aa
10.1.1.2	bb-bb-bb-bb-bb-bb
10.1.1.3	cc-cc-cc-cc-cc-cc

Infrastructure Security: Man-in-the-Middle Attacks 방지

Cisco.com

- Built on DHCP Binding Table
- Dynamic ARP Inspection watches ARP/GARP for violations
- IP Source Guard examines every packet
- Will shun packets or disable port

Successfully Stops Ettercap, Dsniff

10.1.1.1	aa-aa-aa-aa-aa-aa	1/0
10.1.1.2	bb-bb-bb-bb-bb-bb	1/1
10.1.1.4	dd-dd-dd-dd-dd-dd	1/3

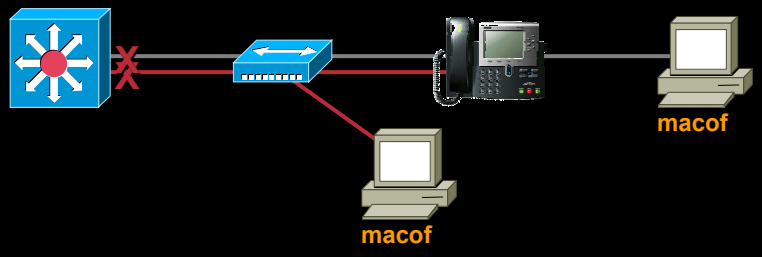
```
ip arp inspection vlan <id>
ip arp inspection validate src-mac ip

Interface FastEthernet1/0
 ip arp inspection trust

interface FastEthernet1/1
 ip arp inspection limit rate 10
 ip verify source vlan dhcp-snooping port-security
```

10.1.1.3
cc-cc-cc-cc-cc-cc

10.1.1.4
dd-dd-dd-dd-dd-dd

Infrastructure Security: MAC Flooding Attacks 방지

Cisco.com



Limit Port to No More than 3 Mac Addresses

```
Interface FastEthernet1/1
 switchport port-security
 switchport port-security maximum 3
 switchport port-security aging time 1
 switchport port-security violation restrict
 switchport port-security aging type inactivity
```

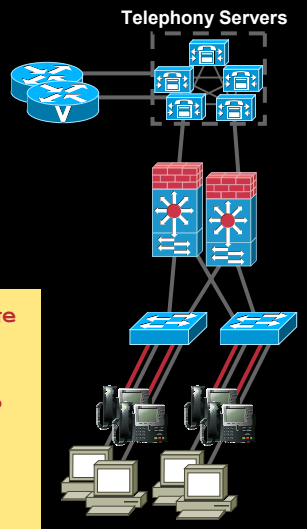
Why 3 macs?

- Phone on data VLAN
- Phone on voice VLAN
- PC on data VLAN

Infrastructure Security: Edge에서의 Attack 방지를 위하여 VACLs 사용

Cisco.com

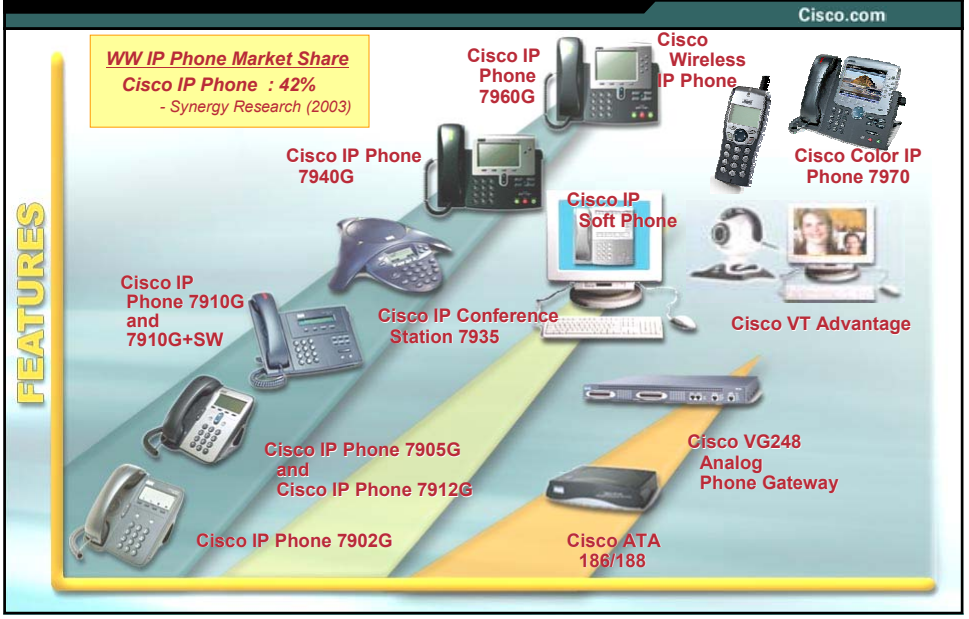
- **Phones** only need to send **RTP to each other** and **TCP to the servers**
- Use a simple VACL to limit traffic to exactly that
- **Stops any and all TCP attacks against the phones!!!**




```
permit udp <voice subnet> <mask> range
16384 32768 any range 16384 32768

permit udp <voice subnet> <mask> tftp
<server subnet> <mask>

permit tcp <voice subnet> <mask>
<server subnet> <mask>
```

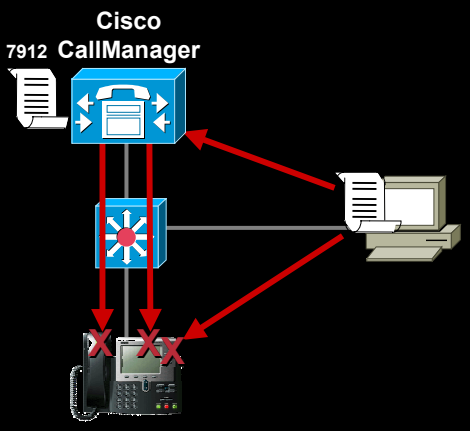
Cisco IP Phone 자체 보안 기능

Cisco IP Phones



IP Phone Hardening:
Rogue Images 설치 방지 기능

- **Signed firmware images**
  - Guaranteed from Cisco
  - Unique signature for each phone model
  - Can't subvert security features!
- **Signed config files**
  - 7940, 7960 and 7970



IP Phone Hardening:
Layer 1 / 2 에서 IP Phone 보안

Configurable Options:

- 다음과 같은 기능을 **Disable** 가능
  - **PC port**
  - **"Settings" button**
  - **Speakerphone**
  - **Web access**
- **Gratuitous ARPs (GARPs)** 무시
- **PC Port** 로부터의 **Voice VLAN** 접근 방지

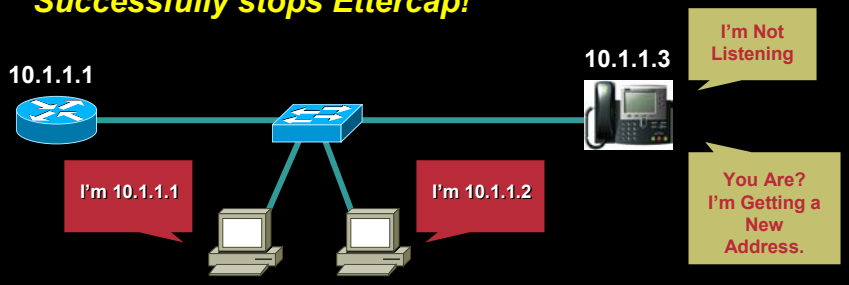
Product Specific Configuration	
Disable Speakerphone	☐
Disable Speakerphone and Headset	☐
Forwarding Delay*	Disabled
PC Port*	Disabled
Settings Access*	Disabled
Gratuitous ARP*	Disabled
PC Voice VLAN Access*	Disabled
Video Capabilities*	Disabled
Auto Line Select*	Disabled
Web Access*	Disabled

These Features Were All Introduced in CCM 3.3(3), Except Signed Config Files and Disable Web Access Which Were Introduced in CCM 4.0

IP Phone Hardening: Gratuitous ARP 무시 기능

- Attack 장비가 Man-in-the-middlle이 되어 도청할 목적으로 라우터의 IP 를 도용하여 Gratuitous ARP(GARP) 보냄
- IP Phone은 GARP 을 무시함 (실제로는 ARP Cache를 Update하지 않음)

Successfully stops Ettercap!

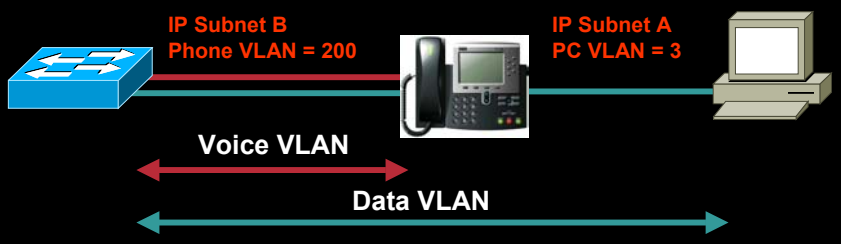


•참고) **Dynamic ARP Inspection and IP Source Guard** are better tools to stop **ARP poisoning and ARP spoofing attacks**

IP Phone Hardening: PC Port를 통한 Voice VLAN 접근 방지 기능

- **Blocks 802.1q tagged with voice VLAN** being sent to or received from the PC port on the phone
- **Blocks the malicious sniffing** of voice streams from the PC port of a phone
- Also blocks intentional sniffing in troubleshooting or monitoring situations
- There are better ways to sniff, such as the SPAN and R-SPAN feature on Catalyst switches

Successfully Stops VOMIT



Cisco Call Manager 시스템 보안

CCM 시스템 Hardening: Hardened Windows Operating System

Cisco.com

- **Hardened Windows-2000 Server OS** shipped by default, and downloadable from www.cisco.com
- Same OS build used for seven applications:
  - Cisco CallManager, Emergency Responder, Conference Connection, Personal Assistant, IPCC Express, IP/IVR, and ISN
- Every version gets incrementally more secure:
  - Registry, IP stack, file system, permissions, middleware apps, disable unused services, etc.
- **US DOD security accreditation**

CCM 시스템 Hardening: Security Patch and Hotfix Policy

Cisco.com

- Cisco monitors several sites such as Microsoft, CERT, and SANS for new vulnerabilities
- Any applicable patch deemed Severity 1 or Critical is tested and posted to www.cisco.com within 24 hours as hotfixes
- All applicable patches are consolidated and posted once per month as incremental service releases
- Email alias tells you when new patches are available
- http://www.cisco.com/warp/public/779/largeent/software_patch.html

Blaster Patch Was Available on www.cisco.com Three Weeks Before It Hit the Internet!

Sasser Patch Was Available on www.cisco.com Two Weeks Before It Hit the Internet!

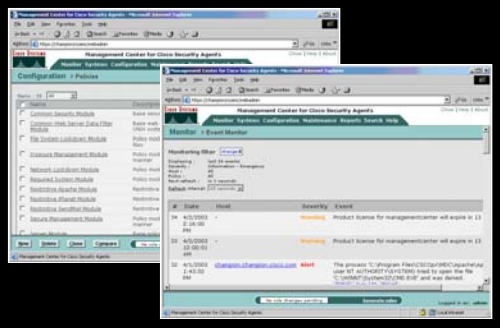
CCM 시스템 Hardening: Anti-Virus Software

Cisco.com

- Cisco doesn't sell it, bundle it, include it or OEM it, but we do recommend you run it!!!
- McAfee VirusScan Enterprise 4.5, 7.0 and 7.1
- Symantec Corporate Edition 7.61, 8.0 and 8.1
- Trend Micro ServerProtect5

CCM 시스템 Hardening: Host-Based IPS (Cisco Security Agent)

- Available for all telephony applications
  - Headless bundled
  - Managed optional
- Policy-based, not signature-based
- Zero updates
- "Day Zero" support
- VMS centrally administers managed agents with distributed, autonomous policy enforcement
- Effective against existing and previously unseen attacks
- Stopped Slammer, Nimda and Code Red sight unseen with out-of-the-box policies



CSA Server Protection:

- Host-based intrusion protection
- Buffer overflow protection
- Network worm protection
- Operating system hardening
- Web server protection
- Security for other applications

CCM 시스템 Hardening: Protect Cisco CallManager from Unwanted Access

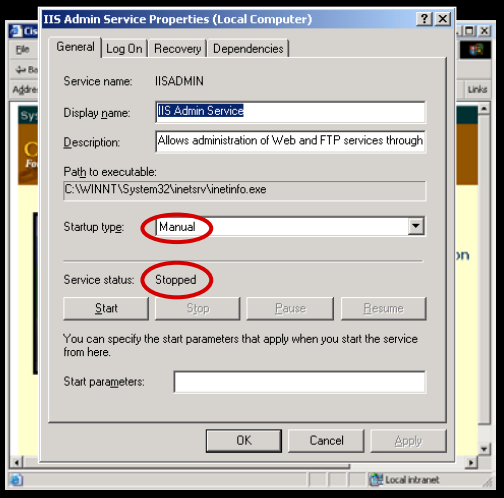
IP Security Filter—Blocks Fixed Windows and SQL Ports

- Extra layer of protection from worms, viruses, and hackers
- Provided script makes it easy—in C:\Utils
- Apply IP addresses, subnets, or local hosts for full access—include servers for third-party apps (billing, management, etc.)
- Packets from any other address blocks SMB, ICMP (in but not out), Netbios, NTP, SNMP, and SQL
- HTTP, Terminal Services and VNC not blocked
- Found in local security policy
- Not to be confused with TCP Filters

CCM 시스템 Hardening: Protect Windows Against Common Exploits

Cisco.com

- **Most XML apps go to the Internet to get data**
  - Offload XML to dedicated server
- **DHCP can be served from the infrastructure**
  - Deploy DHCP close to the endpoints
- **80% of attacks against Windows are targeted at IIS!!!**
  - **Turn off IIS on the Subscribers—Set to Manual for Installer**
  - Change Script Error Message setting to not detailed



CCM 시스템 Hardening: Limit Access to Admin Webpages

Cisco.com

- **Multi-Level Admin (MLA) limits access by user ID**
- **Users are defined in LDAP directory**
- **Users are placed in User Groups**
- **User Groups are placed in Functional Groups**
- **Functional Groups have access to individual webpages**
  - Read/write
  - Read-only
  - No access

CCM 시스템 Hardening: Summary

Cisco.com

- **Hardened OS**
- Patches and hotfixes **kept up to date**
- **Anti-virus**
- Cisco Security Agent **(CSA)**
- Optional security settings
  - Manual settings for your environment
  - Disable unused services
  - Apply IIS and IP security filters

Cisco IP Telephony is Secure !

How Do You Secure Your Voice Network?

Cisco.com

	OPEN	BETTER	BEST
Isolate Servers	Open	ACLs	Firewalls and Rate Limiting
Protect the OS	Open	CSA/AV/Patches Manual Settings	Optional Script/ Managed CSA
Remote Administration	Open	Authentication Proxy	Out-of-Band Management
Phone Hardening	Open	Signed Images and L1/L2 Toggles	Authentication and Encryption
Network Connectivity	Open	VACLs, Ignore GARP	DHCP Snooping, DAI, ISG
Forensic Information	Open	Syslog	NIPS/VMS/CWSIM

It All Depends on Your Situation

NetworkWorldFusion 05/24/04 Declares "Cisco IPT is Secure !!!"

Cisco.com

"Cisco's maximum-security VoIP configuration earned our most Secure rating. Our attack team couldn't disrupt, or even disturb, Cisco's phone operations after three days of trying."

"Security weaknesses earned the basic Avaya configuration a so-so Vulnerable rating, while the hardened package fared better with an overall Resistant rating."

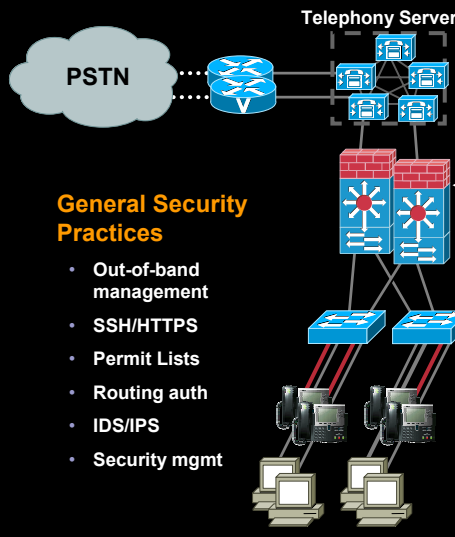
VoIP security rating scale

Overall rating	Maximum impact that assault team could achieve
Secure	No perceptible disruption to voice service.
Resistant	Only minor and/or temporary disturbance(s).
Vulnerable	Phone service affecting many phone users could be disrupted for a protracted period, via a sophisticated or coordinated attack.
Open	Phone service affecting most phone users could be significantly disrupted, indefinitely, via a fairly straight-forward assault.
Unsecure	Phone system or service affecting all users could be readily and indefinitely disabled.

Deployment Models for Secure IP Telephony

Single Site

Cisco.com



Refer to SAFE and SRND for All the Details

Firewall or ACL in Front of Telephony Servers with Rate Limiting

General Security Practices

- Out-of-band management
- SSH/HTTPS
- Permit Lists
- Routing auth
- IDS/IPS
- Security mgmt

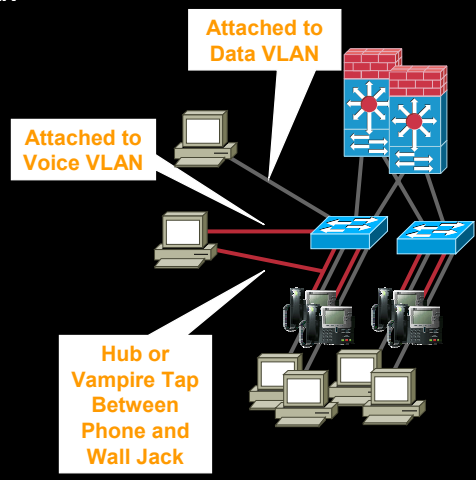
Layer 2 Best Practices

- Separate Voice/Data VLANs
- VACLs
- DHCP Snooping
- Dynamic ARP Inspection
- IP Source Guard
- Port Security
- Conditional QoS Trust

Mitigating Attacks Against Endpoints

Cisco.com

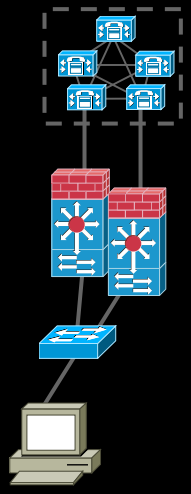
- Blocking PC access to voice VLAN stops eavesdropping attacks (VOMIT)
- DAI and Source Guard prevent man-in-the-middle attacks or traffic interception (ettercap, dsniff)
- VACLs stopped directed TCP attacks
- DHCP Snooping stops DHCP spoofing and starvation attacks
- Signed firmware and config files prevent security features from being subverted
- Certificates disallow rogue CCM and phone insertion
- Encryption prevents media interpretation (if intercepted)



Mitigating Attacks Against Servers

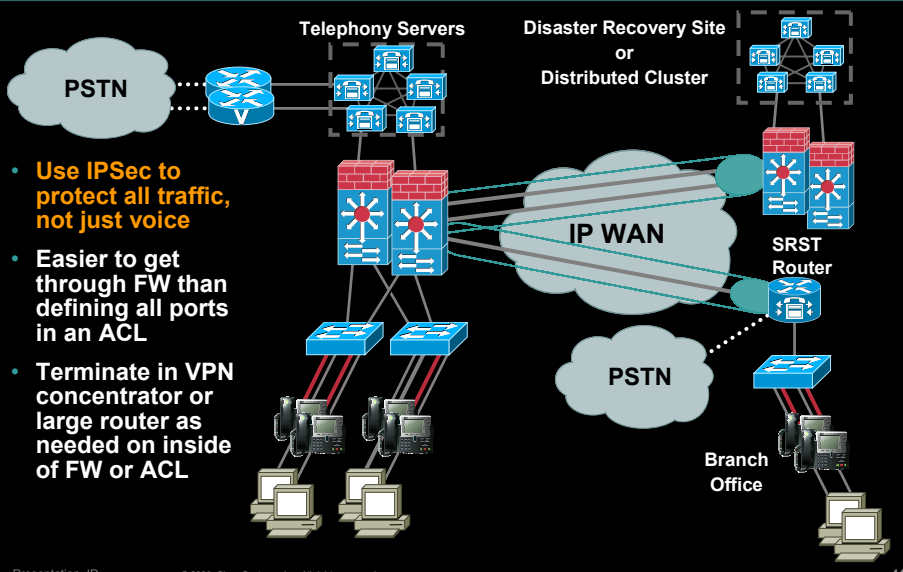
Cisco.com

- **FW, ACL and VACL** prevent targeted TCP and UDP attacks and port scans
- **Authentication proxy** limits access to vulnerable ports at L3
- **Rate limiting prevents DoS and DDoS attacks on signaling ports to servers**
- Common Windows exploits thwarted by **hardened OS**
- Targeted and anonymous illicit behavior stopped by **CSA**



Connecting to a Branch Office or DR Site

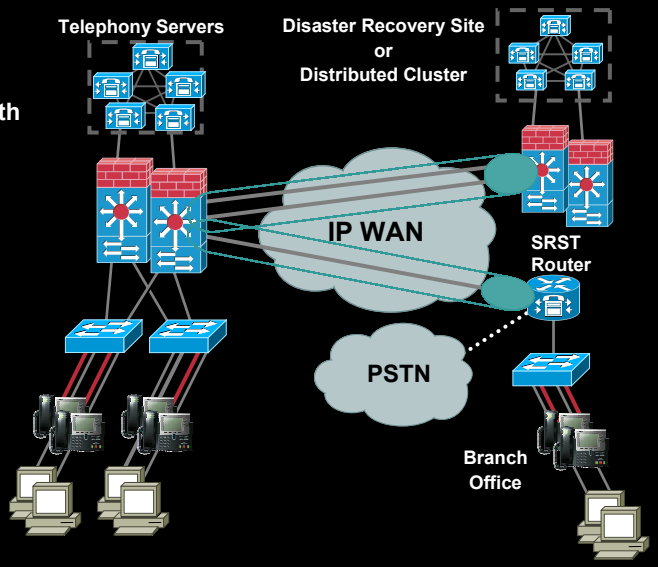
Cisco.com



- **Use IPSec to protect all traffic, not just voice**
- Easier to get through FW than defining all ports in an ACL
- Terminate in VPN concentrator or large router as needed on inside of FW or ACL

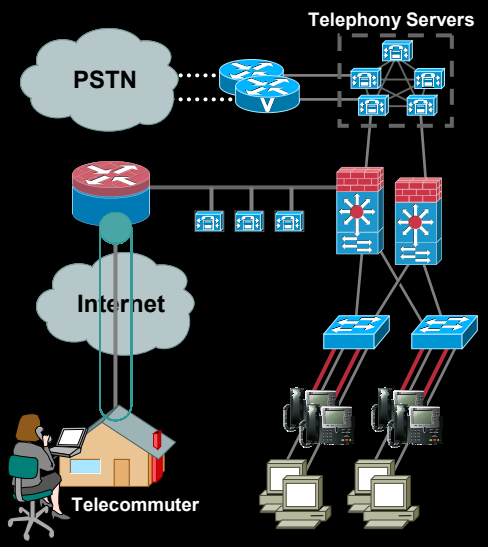
Connecting to a Branch Office or DR Site

- Remember to maintain bandwidth requirements for clustering-over-the-WAN
  - 40ms maximum round-trip delay
  - Allow 900kbps for each 10,000 BHCA
  - Enough additional bandwidth to carry resulting calls in a failure situation

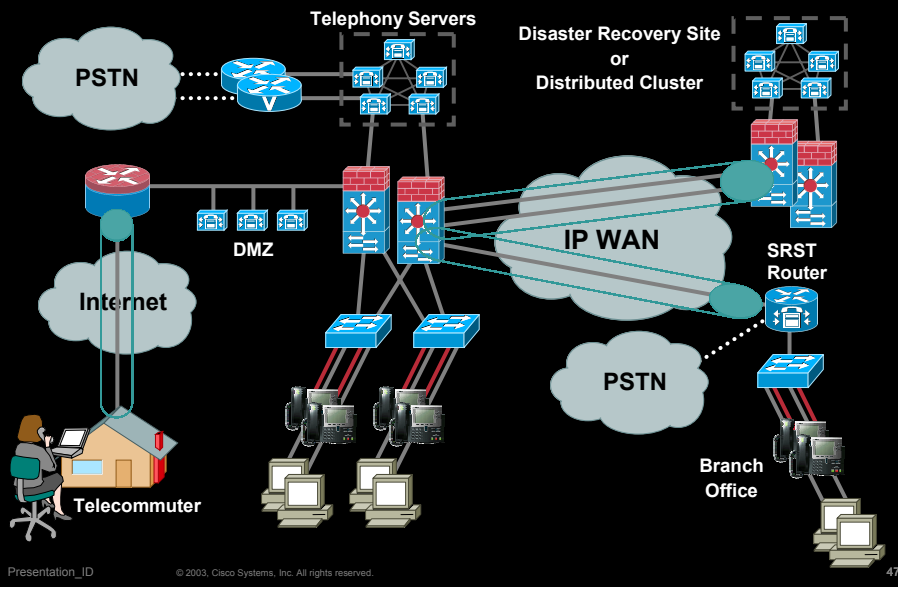


Connecting Telecommuters over the Internet

- Use V3PNs with IPSec to protect all traffic from SOHO location, not just voice
- Terminate at HQ end in VPN concentrator or large router



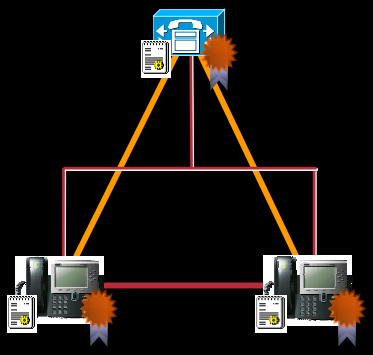
Putting It All Together



Cisco IP Telephony Authentication and Encryption

Certificate-Based Authentication and Encryption

- **Public Key/Private Key Pair**
- **X.509v3 Digital Certificate**
  - Self-Signed (CCM)
  - MIC from Cisco Mnfg (7970)
  - LSC from CAPF (7940/7960)
- **Certificate Trust List**
  - CTL Client
- **Transport Layer Security**
  - RSA Signatures
  - HMAC-SHA-1 Auth Tags
  - AES-128-CBC Encryption
- **Secure RTP**
  - HMAC-SHA-1 Auth Tags
  - AES-128-CM Encryption

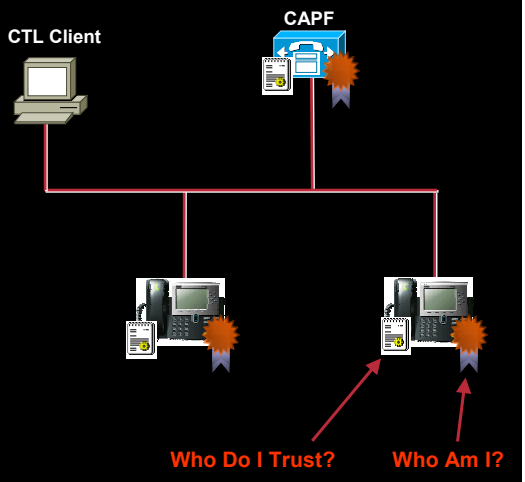


In Cisco CallManager 4.0,

- 7970 supports MIC certs with auth and encr TLS and SRTP
- 7940/7960 support LSC certs with auth TLS

Certificate Trust List

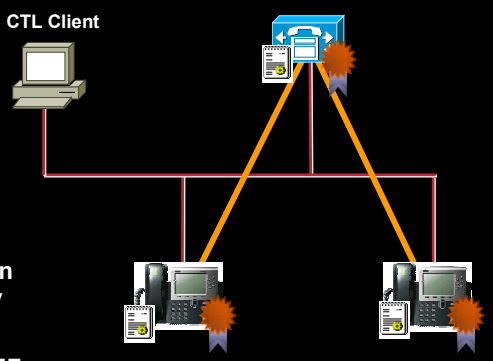
- **Certificate Trust List contains list of trusted devices**
- **Similar to Trusted Root CAs in IE**
- **Generated by CTL client**
- **Loaded into phones during TFTP download**
- **All phones in a cluster have the same CTL file**
- **CCM has a dynamic CTL file**
  - Populated during TLS registration
  - Contained in OpenSSL database



TLS: Transport Layer Security

Cisco Uses TLS for Secure Signaling Between CCM and IP Phones

- Bidirectional exchange of certificates for mutual authentication
- RSA signatures
- HMAC-SHA-1 authentication tags insure packet integrity
- AES-128-CBC encryption protects session keys, DTMF tones and other data*

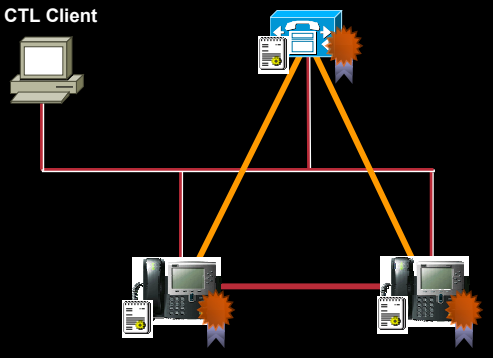


TLS Has a 20–25% Hit on Cisco CallManager Performance

* 7970 Only at This Time

SRTP: Secure RTP

- SRTP is the transport for authenticated and encrypted media
- IETF RFC3711
- Uses HMAC-SHA-1 for authentication and AES-128-CM for encryption
- Keys derived in CCM—sent to phones over TLS
- Currently only supported on 7970
- Over time, SRTP will role out to a broad range of phones, gateways and applications



SRTP Packets Add 15 Microseconds to Latency and Are 4–7 Bytes Bigger than RTP Packets