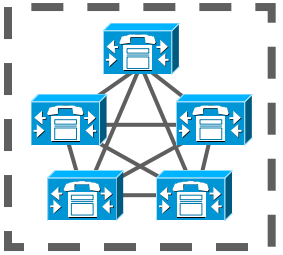
VoIP Security:
Are we risking the security and integrity of our voice communications?

Kip Schroeder, CISSP
Cisco Systems Engineer
kips@cisco.com

Ron Shuck, CISSP
SKT Security Practice Manager
ron.shuck@sktbcs.com

Do You Know What a Phreaker (Voice) or a Hacker (Data) Looks Like?

- **Attacks against IP Telephony endpoints**
  - Reconnaissance
  - DHCP starvation
  - Eavesdropping/Man-in-the-middle
  - Directed TCP and ICMP attacks
- **Attacks against IP Telephony servers**
  - Worms, viruses and trojans
  - DoS and DDoS
  - Directed probes, floods
- **Attacks against IP Telephony applications**
  - Intercept administration and user traffic
  - Exploit programming weakness
  - Rogue servers
  - Toll fraud



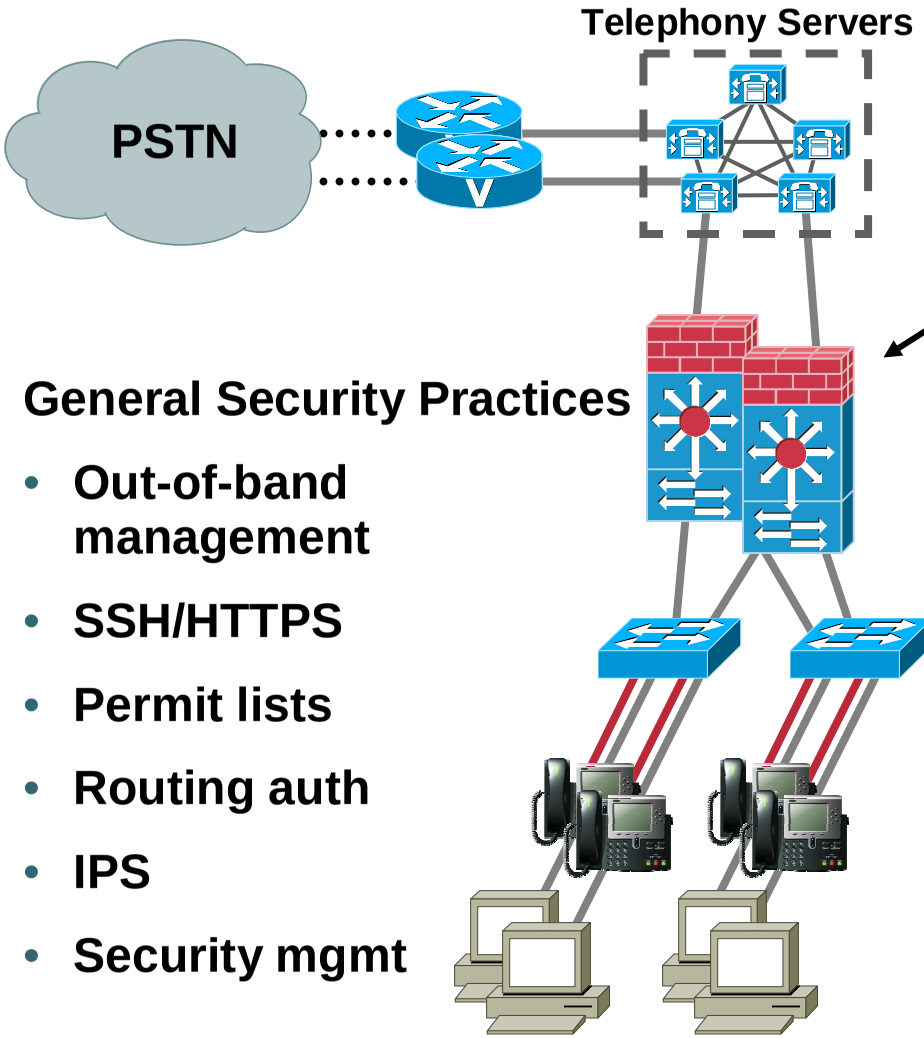
Voice Security Defense-in-Depth

- **Protect IP Telephony Endpoints**
- **Protect IP Telephony Servers**
- **Protect IP Telephony Applications**

Voice Security Defense-in-Depth

- **Protect IP Telephony Endpoints**
  - **Network Hardening for Phones**
  - **Phone Hardening**
  - **Securing TFTP**
  - **Encrypted Communications**
  - **802.1X and IP Phones**
  - **Phones over the Internet**
- **Protect IP Telephony Servers**
- **Protect IP Telephony Applications**

Secure Voice by First Securing the Network



- Firewall or ACL in front of telephony servers
- Rate Limiting

General Security Practices

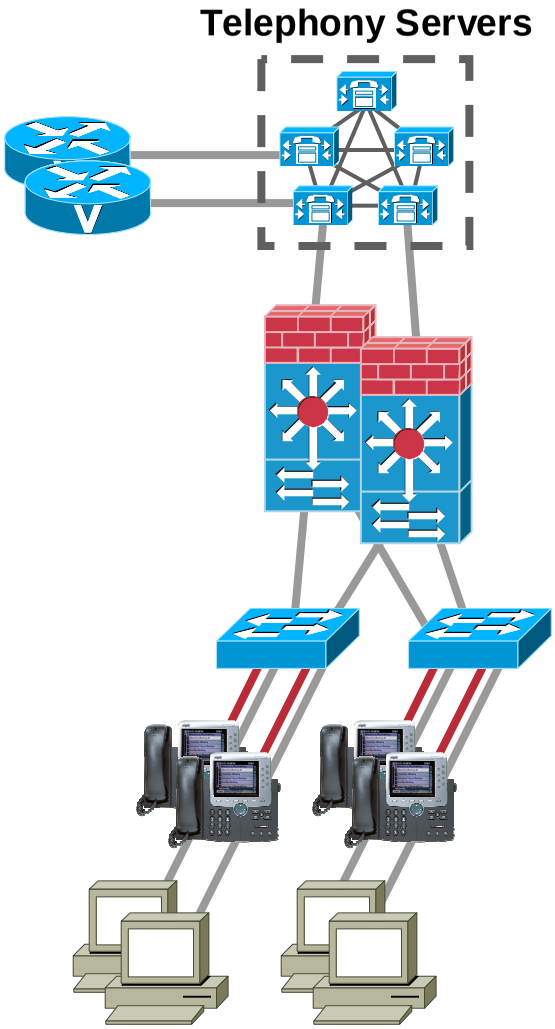
- Out-of-band management
- SSH/HTTPS
- Permit lists
- Routing auth
- IPS
- Security mgmt

Network Security Features

- Separate voice & data VLANs
- VLAN ACLs (VACLs)
- DHCP Snooping*
- Dynamic ARP Inspection*
- IP Source Guard*
- Port Security
- Scavenger-class QoS

Separate Voice and Data VLANs

- **VLAN Access Control Lists (VACLs)**
  - **Phones only need to send RTP to each other and a small number of TCP/UDP protocols to servers**
  - **Phones have no reason to send TCP or ICMP to each other**
  - **Stops all TCP and ICMP attacks against the phones**
- **802.1AE (MACSec) Link-Layer Integrity will require it—part of next-generation switches and phones***



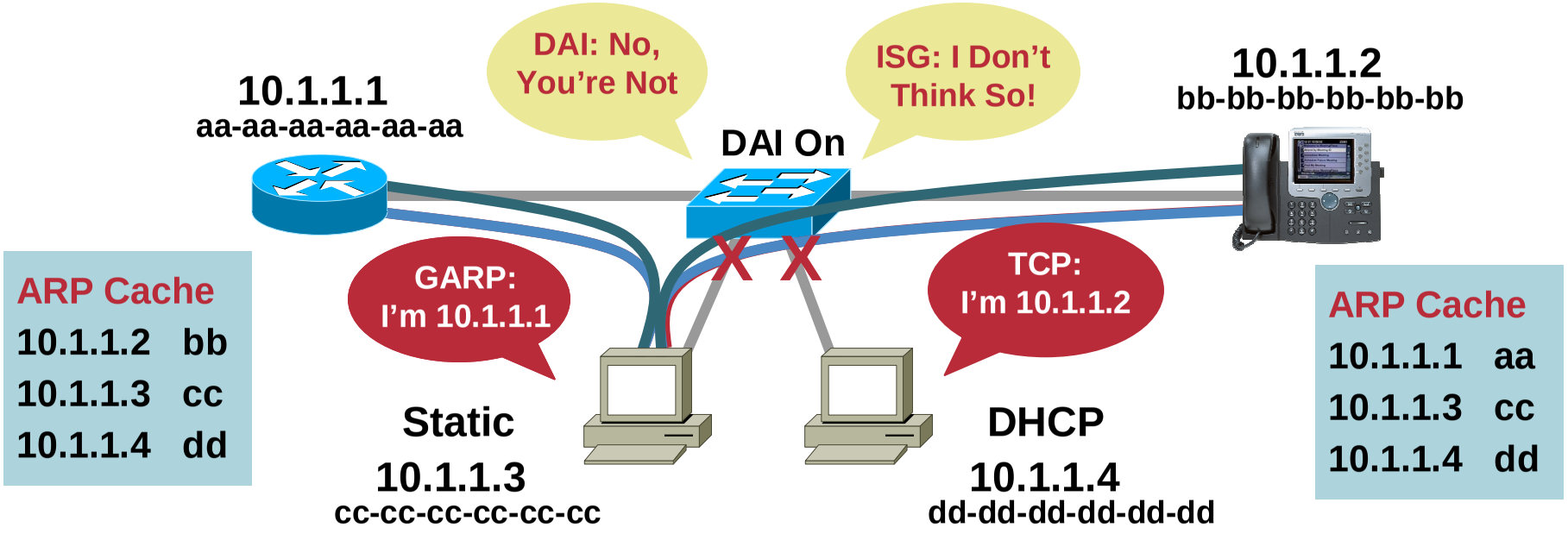
* http://www.networkworld.com/news/tech/2005/101005techupdate.html

Stop Man-in-the-Middle Attacks

- Built on DHCP snooping binding table
- Dynamic ARP inspection watches ARP/GARP for violations
- IP source guard examines every IP packet
- Will drop packets or disable port

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

Successfully Stops ettercap, dsniff



Voice Security Defense-in-Depth

- **Protect IP Telephony Endpoints**
  - **Network Hardening for Phones**
  - **Phone Hardening**
  - **Securing TFTP**
  - **Encrypted Communications**
  - **802.1X and IP Phones**
  - **Phones over the Internet**
- **Protect IP Telephony Servers**
- **Protect IP Telephony Applications**

Hardening the Endpoints

- **Signed firmware**
- **Signed config files**
- **Disable**
  - **PC port / VLAN**
  - **Settings**
  - **Web Access**
  - **Gratuitous ARP**
- **Authentication**

Secure Shell Information

Secure Shell User

Secure Shell Password

Product Specific Configuration

☐ Disable Speakerphone

☐ Disable Speakerphone and Headset

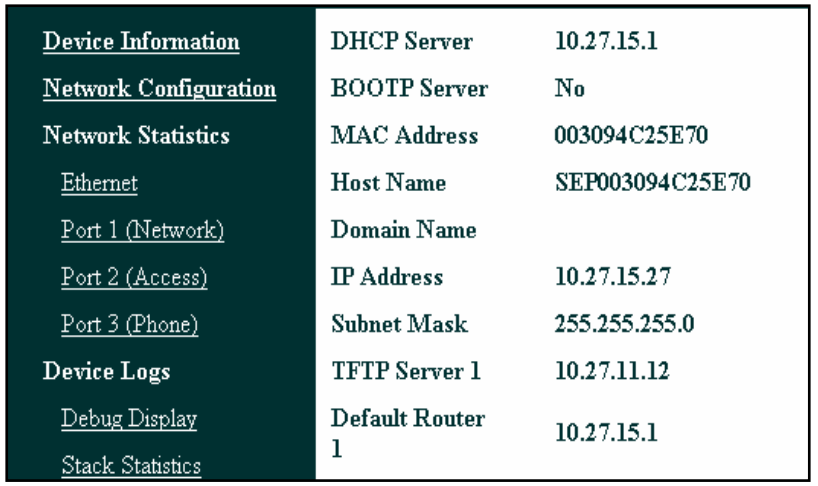
PC Port *	Disabled
Settings Access *	Restricted
Gratuitous ARP *	Disabled
PC Voice VLAN Access *	Disabled
Web Access *	Disabled
Span to PC Port *	Disabled
Logging Display *	Disabled

Browse into a Phone

I Learn

- IP address/mask
- Default gateway
- DHCP server
- DNS server
- TFTP server
- Telephony Server
- Directory server
- Logon server
- XML server
- If I'm reconning your network, I can learn an awful lot about your network by webbing into a single phone
- But, disabling web access also breaks XML pushing apps

  Instead, use ACLs to only allow port 80 between phones and servers

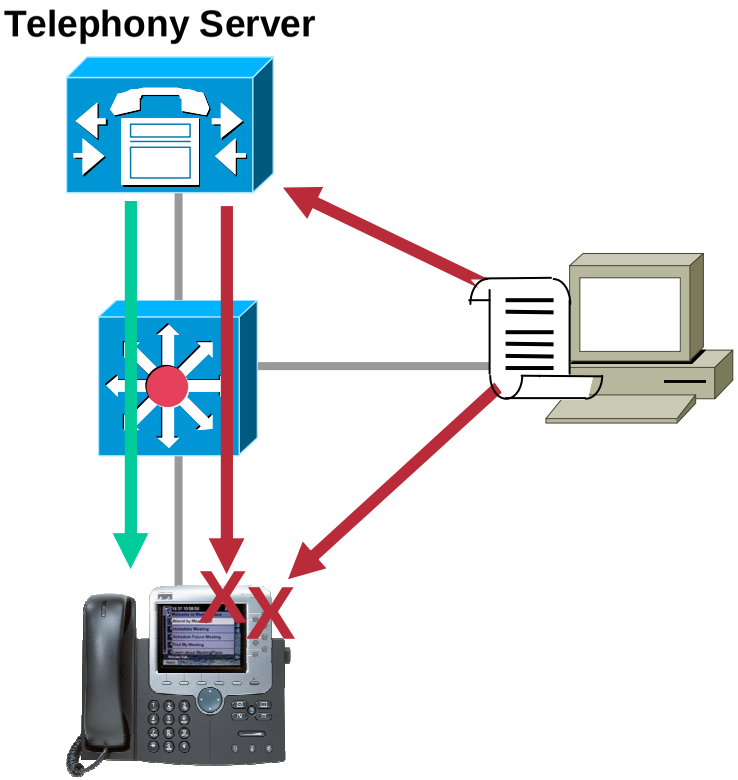


Voice Security Defense-in-Depth

- **Protect IP Telephony Endpoints**
  - **Network Hardening for Phones**
  - **Phone Hardening**
  - **Securing TFTP**
  - **Encrypted Communications**
  - **802.1X and IP Phones**
  - **Phones over the Internet**
- **Protect IP Telephony Servers**
- **Protect IP Telephony Applications**

Securing TFTP

- **TFTP is used to download firmware and configurations into phones**
- **Many companies disallow TFTP as an insecure protocol**
- **Must solve this by securing the payload that TFTP carries**
  - **Signed firmware images**
  - **Signed config files**
  - **Encrypted config Files**

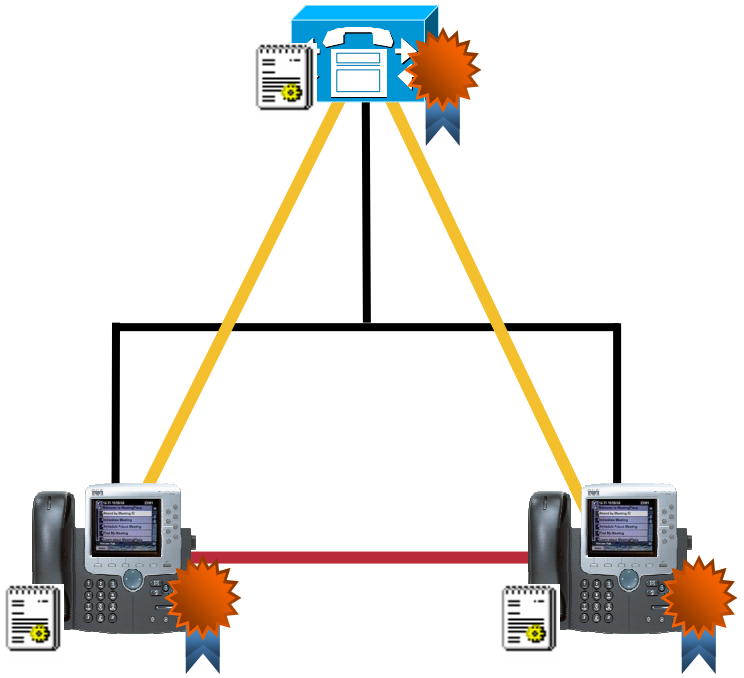


Voice Security Defense-in-Depth

- **Protect IP Telephony Endpoints**
  - **Network Hardening for Phones**
  - **Phone Hardening**
  - **Securing TFTP**
  - **Encrypted Communications**
  - **802.1X and IP Phones**
  - **Phones over the Internet**
- **Protect IP Telephony Servers**
- **Protect IP Telephony Applications**

Certificate-Based Authentication and Encryption

- **TLS—Transport Layer Security (RFC 2246) protects signaling between Telephony Server and endpoints**
  - **RSA signatures**
  - **HMAC-SHA-1 auth tags**
  - **AES-128-CBC encryption**
- **SRTP—Secure RTP (rfc3711) protects media between endpoints**
  - **HMAC-SHA-1 auth tags**
  - **AES-128-CM encryption**

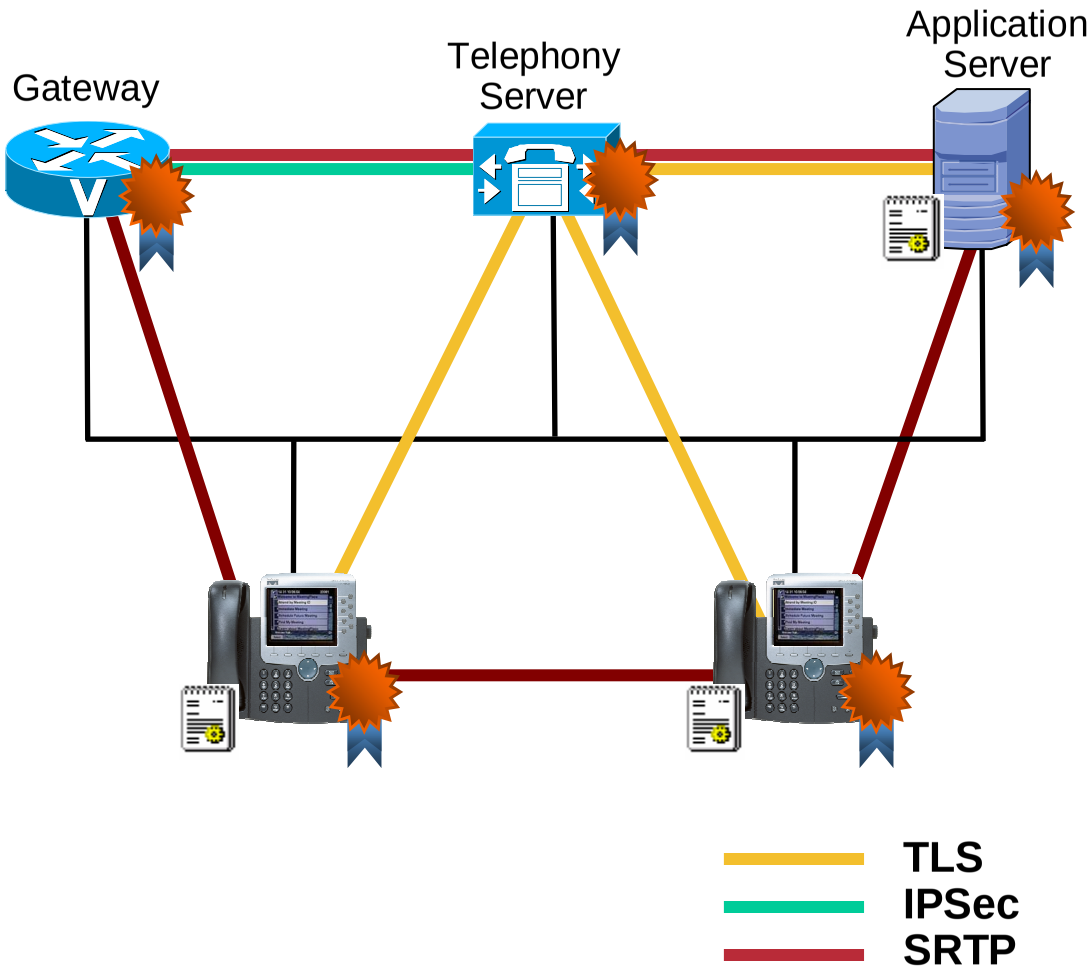


Certificate-Based Authentication and Encryption

IPSec and SRTP to MGCP and H.323 Gateways

TLS to SIP Trunks

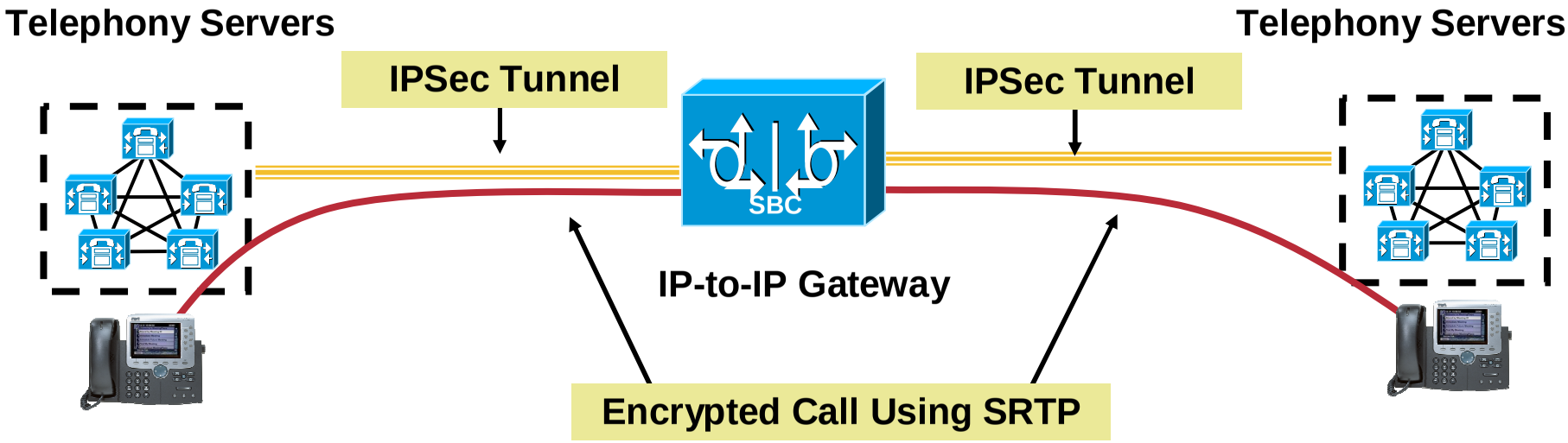
TLS and SRTP for Applications



SRTP for SIP Phones

- **SIP phones indicate capability for SRTP in SDP of SIP message**
- **SIP phones generate their own encryption keys**
- **Interoperates with SCCP, H.323, MGCP, etc.**

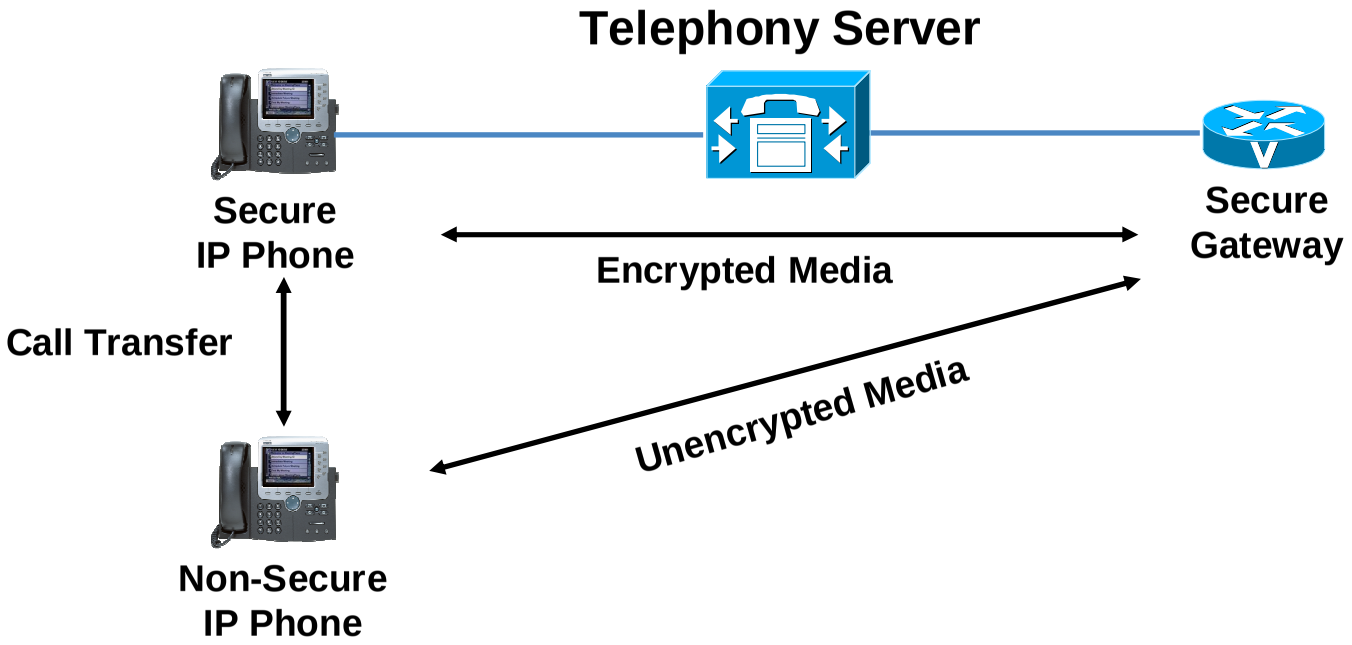
IPSec and SRTP Secure Calls Through IP-to-IP Gateway



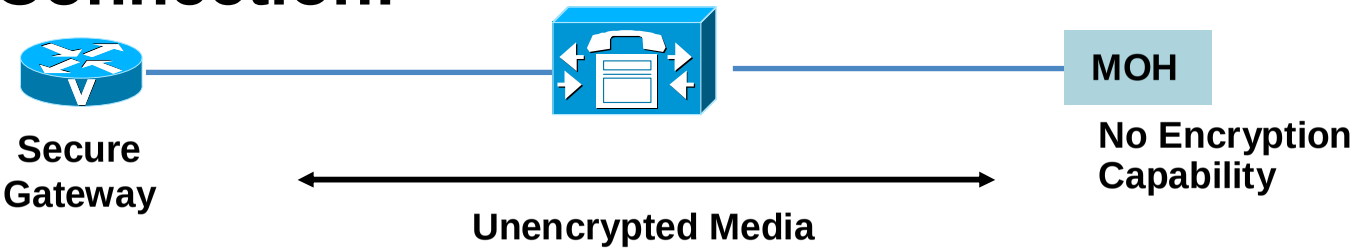
- Inter-cluster SRTP over IPSec works with or without IP-IP Gateway in place
- Media authentication and encryption uses SRTP—GW to GW or phone
- Signaling authentication and encryption uses IPSec—GW to GW or Telephony Server
- IP-to-IP Gateway supports secure calls

Understanding RTP/SRTP Mixed-Mode

Secure Call Transfer:



MOH Connection:



Voice Security Defense-in-Depth

- **Protect IP Telephony Endpoints**
  - **Network Hardening for Phones**
  - **Phone Hardening**
  - **Securing TFTP**
  - **Encrypted Communications**
  - **802.1X and IP Phones**
  - **Phones over the Internet**
- **Protect IP Telephony Servers**
- **Protect IP Telephony Applications**

802.1X and IP Telephony

Requirement

- Phone only transmits on voice VLAN
- PC only transmits on data VLAN

Limitations – The 802.1X spec has no provision for

- More than one device on a port
- No authentication to a specific VLAN
- No binding to restrict an authenticated device to only transmit on authorized VLAN

Future Solution

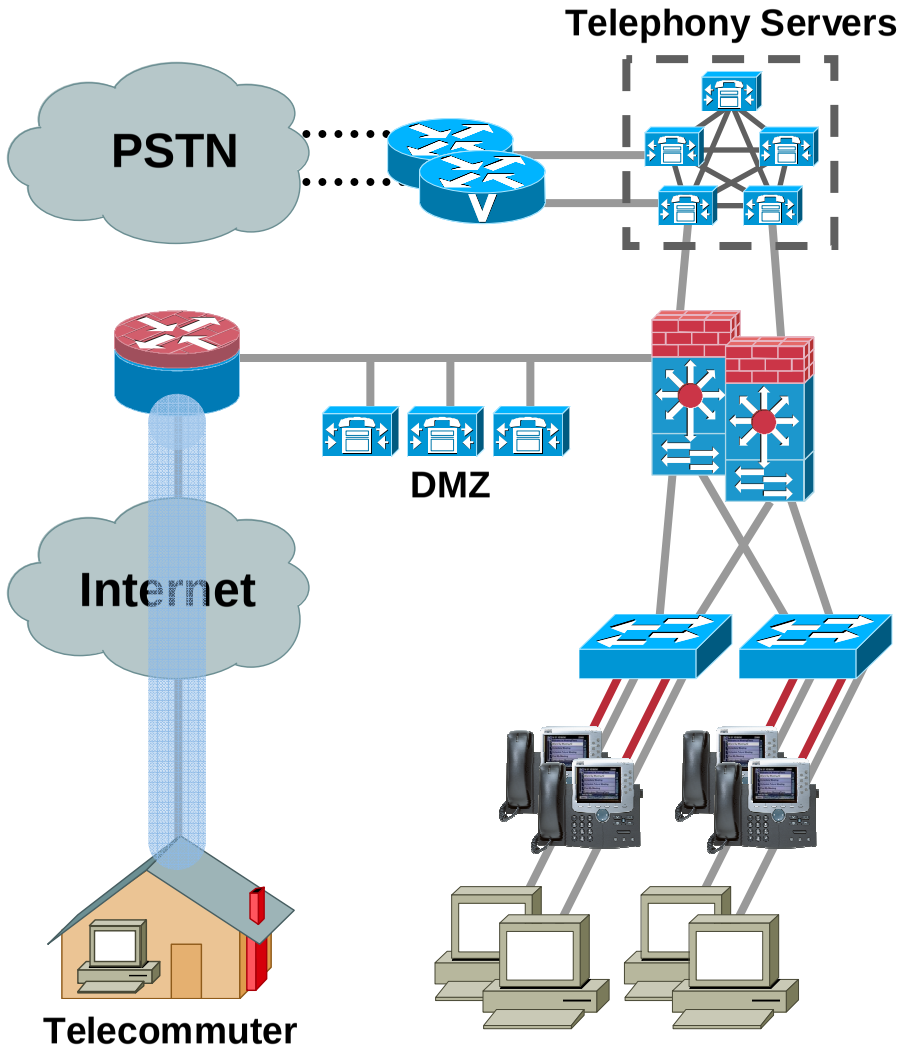
- Switch changes to support multiple devices on different VLANs
- 802.1AE – Link-layer integrity

Voice Security Defense-in-Depth

- **Protect IP Telephony Endpoints**
  - **Network Hardening for Phones**
  - **Phone Hardening**
  - **Securing TFTP**
  - **Encrypted Communications**
  - **802.1X and IP Phones**
  - **Phones over the Internet**
- **Protect IP Telephony Servers**
- **Protect IP Telephony Applications**

IP Phones over the Internet

- **Use IPSec to protect all traffic from SOHO location, not just voice**
- **Terminate at HQ end in VPN concentrator or large router**
- **VPN client in phones available in some vendor phones**



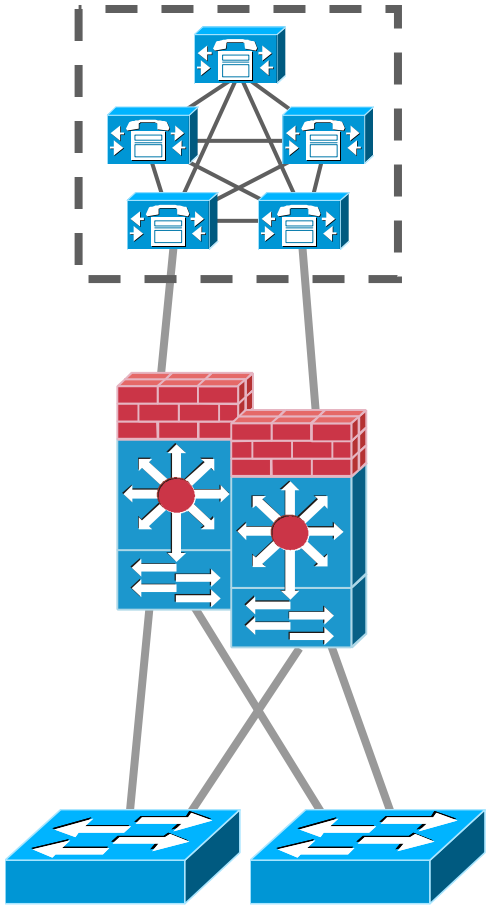
Voice Security Defense-in-Depth

- **Protect IP Telephony Endpoints**
- **Protect IP Telephony Servers**
  - **Firewall Traversal**
  - **Telephony Server and IPSec**
  - **Windows Telephony Servers and Other Applications**
  - **Linux Telephony Servers**
- **Protect IP Telephony Applications**

Place a Firewall or ACL in Front of Telephony Servers

Why Firewall?

- Need a network mechanism to isolate and protect telephony servers
- Consistent with data center best practices
- Firewalls provide stateful inspection of protocols that use ephemeral port ranges; otherwise, have to open entire port range in static ACL
- LLQ and Rate Limiting now supported in major firewalls

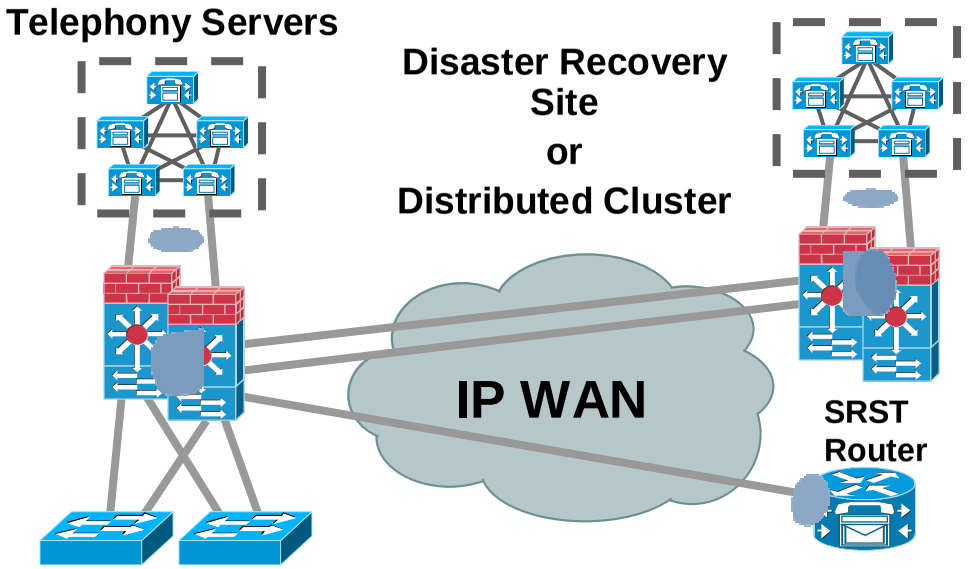


Voice Security Defense-in-Depth

- **Protect IP Telephony Endpoints**
- **Protect IP Telephony Servers**
  - **Firewall Traversal**
  - **Telephony Server and IPSec**
  - **Windows Telephony Servers and Other Applications**
  - **Linux Telephony Servers**
- **Protect IP Telephony Applications**

IPSec to a Branch Office or DR Site

- A question of trust
- Use IPSec to protect all traffic,
  not just voice
- Easier to get through FW than defining all ports in an ACL
- Remember clustering-over-the-WAN metrics



- Better to terminate in VPN concentrator or large router as needed on inside of Firewall or ACL
  - Performance
  - Configuration complexity
  - Organizational boundaries

Voice Security Defense-in-Depth

- **Protect IP Telephony Endpoints**
- **Protect IP Telephony Servers**
  - **Firewall Traversal**
  - **Telephony Server and IPSec**
  - **Windows Telephony Servers and Other Applications**
  - **Linux Telephony Servers**
- **Protect IP Telephony Applications**

Protecting the Windows Operating System

- **Hardened Windows OS should be shipped by default**
  - **File and registry settings**
  - **Unused services deleted, Guest users disabled**
  - **Designed to meet specifications by Microsoft, CERT, etc.**
- **Aggressive security patch and hotfix policy**
- **End point security on all telephony apps**
- **Anti-virus Installed**
- **Don’t forget physical security**

Manual Security Settings

Recommended

- Create individual users placed in administrators group
- Disable web access on Subscribers
- Add screensaver and logon passwords

Not Recommended

- Account lockout settings
- Clear page file at shut down

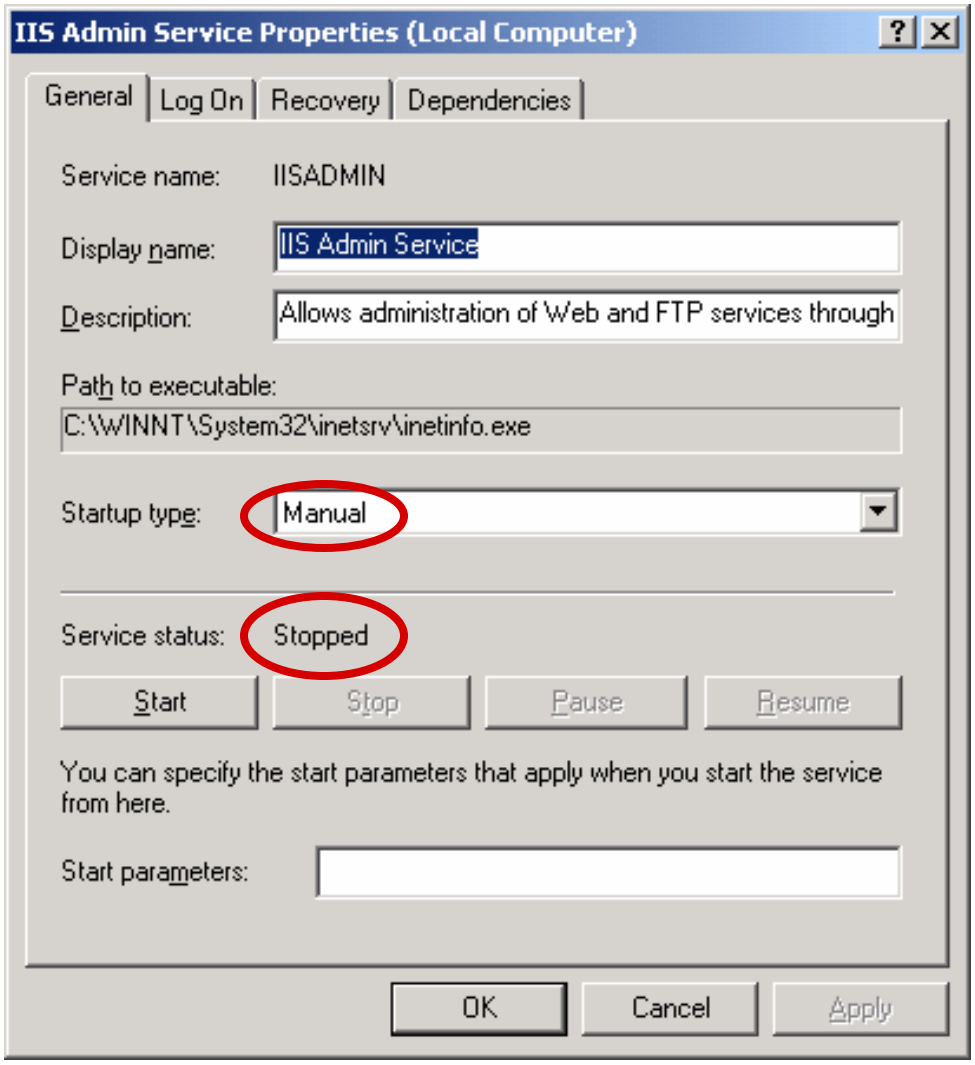
Don’t Do at All

- Delete service accounts
- Change file or registry permissions
- Inherit local OS policy from Active Directory

Eliminate the Biggest Threat Against Windows

80% of attacks against Windows are targeted at IIS !!!

- **Turn off IIS & WWW**
- **Failure to turn off WWW will result in IIS being Manual / Started after next reboot**
- **Set to Manual for Installer**



Voice Security Defense-in-Depth

- **Protect IP Telephony Endpoints**
- **Protect IP Telephony Servers**
  - **Firewall Traversal**
  - **Telephony Server and IPSec**
  - **Windows Telephony Servers and Other Applications**
  - **Linux Telephony Servers**
- **Protect IP Telephony Applications**

Linux Telephony Server Model

- **Make file system and OS apps inaccessible**
  - **GUI for needed services implemented in Platform web pages**
  - **CLI for some system services**
- **Only allows images to be installed that have been signed by vendor**
- **SSH / SFTP / SNMPv3 / Security Passphrase / Password Recovery**
- **Industry-recommended security practices followed**
  - **Unused services removed, Default usernames (root, bin, daemon, ….) disabled**
  - **Continuous improvement to keep up with new threats over time**
- **Monitor Security event logs**

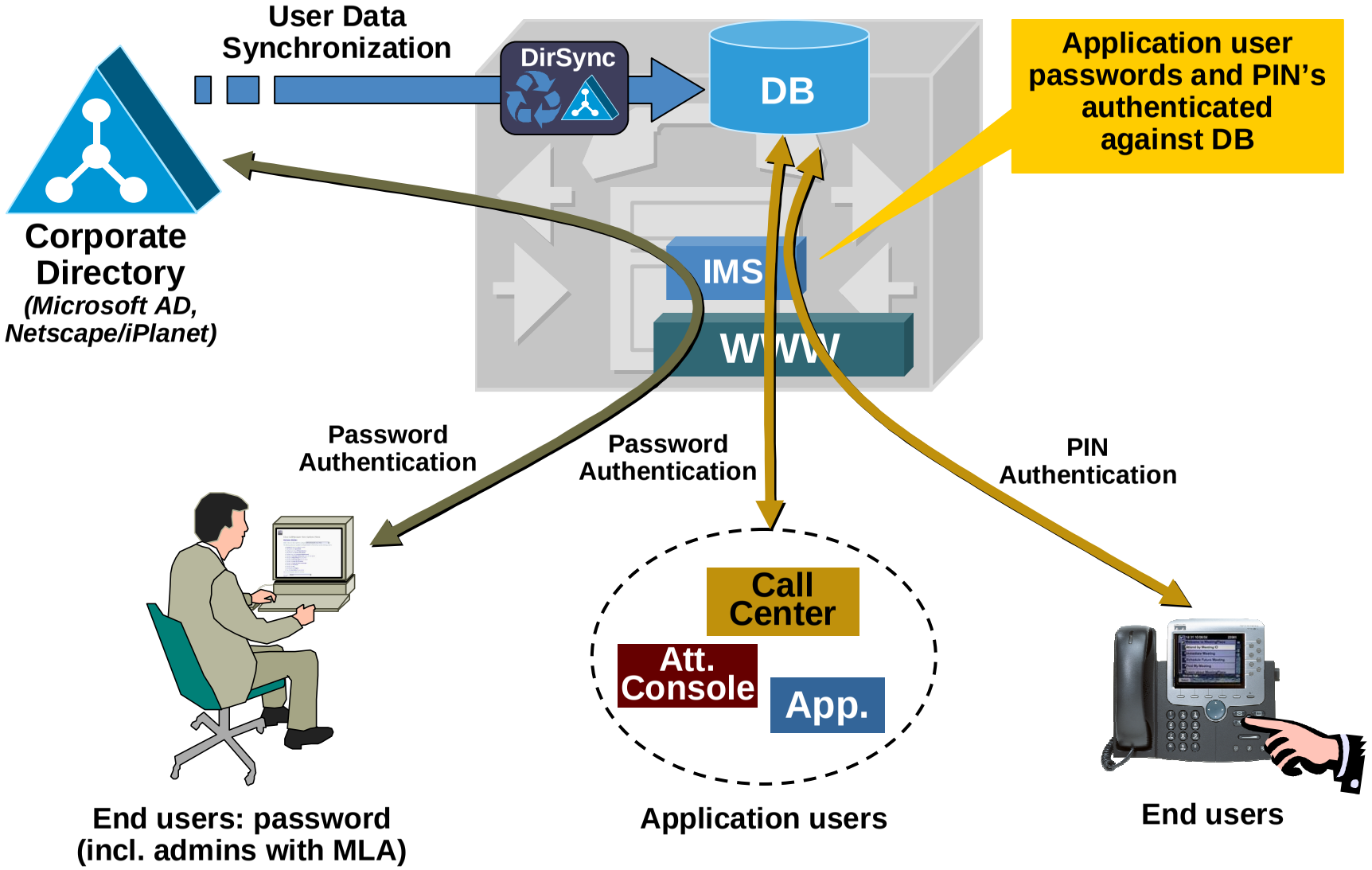
Voice Security Defense-in-Depth

- **Protect IP Telephony Endpoints**
- **Protect IP Telephony Servers**
- **Protect IP Telephony Applications**
  - **Telephony Server**
  - **Voice Mail**

Digest Authentication for SIP

- **Based on RFC 3261 & RFC 2617**
- **Username / Password Auth Mechanism**
- **Client / Server Model**
  - **Server Challenges, Client responds**
  - **Authorization Header is an MD5 hash of username, password, SIP URI , ….**
- **The trick is getting the password into the phone**
  - **Can use public key for phones with MIC**
  - **Must manually enter into phone otherwise**

Directory Authentication Architecture



Prevent User Toll Fraud

- Protect against call forwarding, remote call forwarding, and trunk-to-trunk transfers
- Partitions and Calling Search Spaces limit to what parts of the dial plan certain phones have access
- Dial plan filters control access to exploitive phone numbers, such as 900
- Ad-hoc conference calls can optionally be dropped when the originator hangs up
- Forced authentication codes or client matter codes prevent unauthorized calls and provide a mechanism for billing and tracking

Voice Security Defense-in-Depth

- **Protect IP Telephony Endpoints**
- **Protect IP Telephony Servers**
- **Protect IP Telephony Applications**
  - **Telephony Server**
  - **Voice Mail**

Host and Network Hardening

- **Manually harden Win2K OS, SQL, LDAP and SMTP Exchange/Domino servers**
- **User account policies**
  - **Minimum password/PIN lengths and complexity**
  - **Password/PIN reuse and expiration**
  - **One-time PIN tokens**
  - **Number of login failures**
- **Class-of-service restrictions**
- **Secure active directory infrastructure**
- **HTTPS for all web access—admin and user**

How Much Security Is Enough?

Security Is a Balance Between Risk and Cost

Cost—Complexity—Manpower—Overhead

Bronze Default, Easy, No-Brainer	Silver Moderate, Reasonable	Gold New, Hard, Not Integrated
Basic Layer 3 ACLs	Simple Firewalls	Complex Firewalls
Standard OS Hardening	Rate Limiting	NAC / 802.1X
Unmanaged End Point Security	Switch Integrated Security	Network Anomaly Detection
Antivirus	VPN—SOHO/Mobile	Security Info Management
HTTPS	Optional OS Hardening	
SLDAP	Managed Endpoint Security	
Signed Firmware and Configs	Directory Integration	
Phone Security Settings	TLS / SRTP to Phones	
	IPSec / SRTP to Gateways	

Further Reading

Outside Publications

- **NetworkWorldFusion: Breaking Through IP Telephony**
  http://www.networkworld.com/reviews/2004/0524voipsecurity.html
- **US DoD PBX1 and PBX2 Accreditation**
  http://jitc.fhu.disa.mil/tssi/apl/apl_cisco.html
- **NIST: 'Security Considerations for VoIP Systems'**
  http://csrc.nist.gov/publications/nistpubs/800-58/SP800-58-final.pdf
- **eWeek: 'VoIP Is As Secure As You Make It'**
  http://www.eweek.com/article2/0,1759,1592801,00.asp
- **Ziff Davis: 'Securing Your Network for VoIP'**

  http://www.cisco.com/application/pdf/en/us/guest/netsol/ns391/c654/cdccont_0900aecd801e6159.pdf
- **Converge!: 'Enterprise Security – An Enabler of VoIP'**
  http://www.convergedigest.com/blueprint/ttp04/z4cisco1.asp?ID=141&ctgy=4


ISSA™
Information Systems Security Association


CENTRAL PLAINS CHAPTER


cisco


SKT