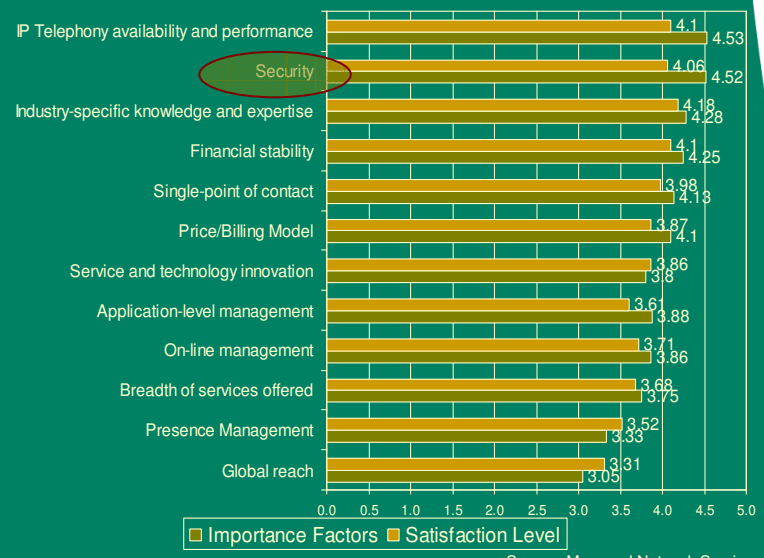
Securing Enterprise IP Telephony

Roland Chia
CCIE #1277

Agenda

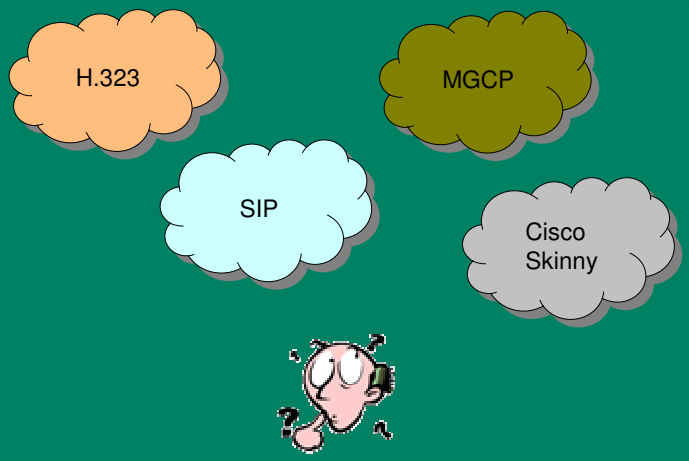
- IP Telephony Overview
- IP Telephony Vulnerabilities
- IP Telephony Security Best Practices
- Risk vs Cost

Importance and Satisfaction Level Factors When Choosing an IP Telephony Solution



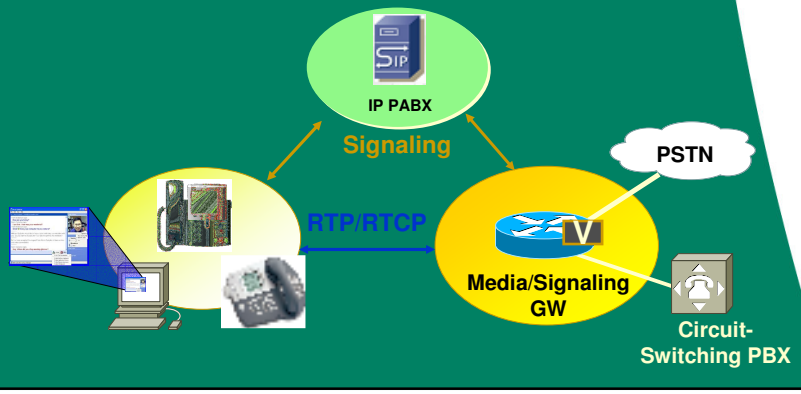
Source: Managed Network Services Survey, IDC, 2003

VoIP Standards & Protocols

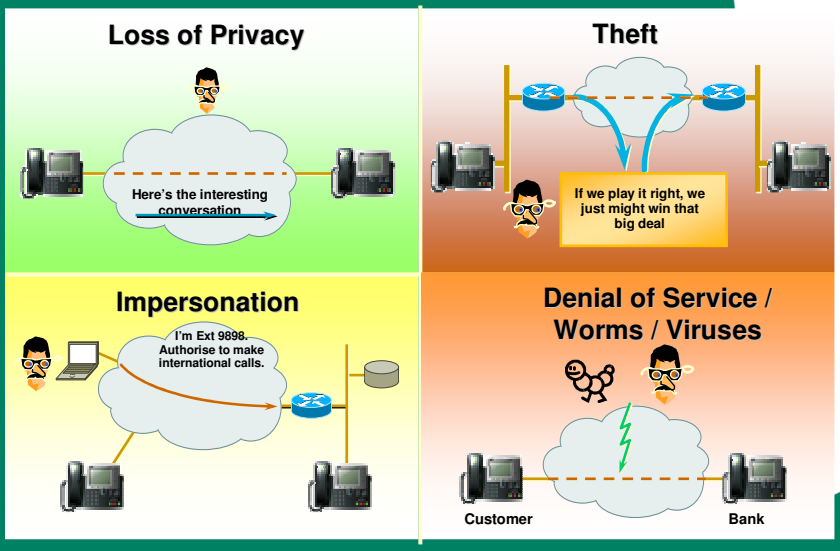


IP Telephony Architecture - Basic

- Signaling protocols run on well-known ports that require static pinholes in a firewall
- Signaling packets contain IP addresses and port numbers for the RTP stream
- Media is carried by RTP on undefined UDP ports

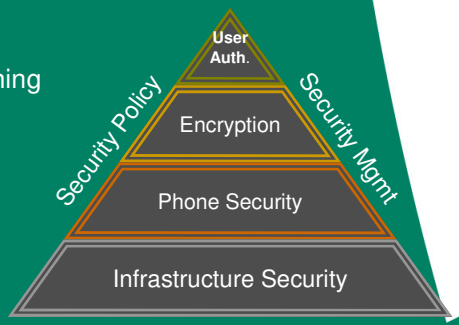


IP Telephony Vulnerabilities



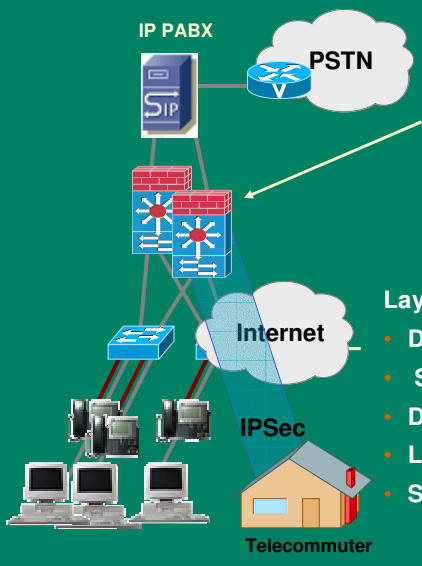
IP Telephony Security Axioms

- Data network QoS and security is essential
- Build it in layers providing end-to-end security solution
  - Device Security
  - Infrastructure Security
  - Phone Hardening
  - OS & Application Hardening
- Risk vs cost



Infrastructure Security

IP Telephony Security Design



Layer 3 Best Practices

- Private IP Addresses
- Separate voice & data VLANs
- ACLs or App-aware FWs

Layer 2 Best Practices

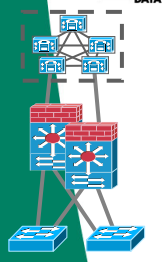
- Disable unused Ethernet ports
- Separate voice & data VLANs
- DHCP / ARP protections
- Limit MAC addresses on ports
- STP Attack Mitigation

The BIG Question

To use Security Appliances or not:

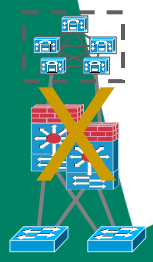
Why Yes

- Need a network mechanism to isolate and protect telephony servers
- Consistent with data centre Network Design
- Firewalls provide stateful inspection of protocols that use ephemeral port ranges. Otherwise, have to open entire port range in static ACL.
- Rate limiting rules should also be implemented
- Monitoring and Intrusion prevention



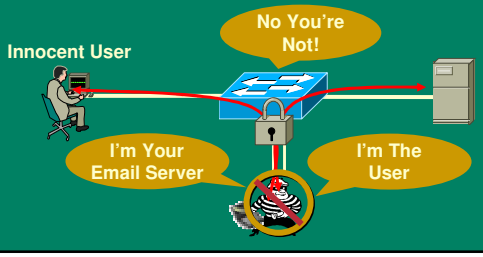
Why No

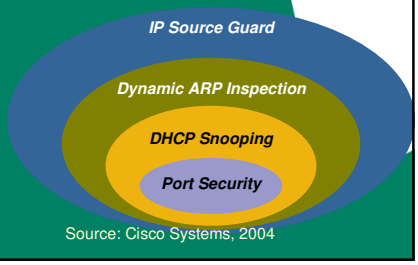
- Limited throughput with voice
- No solid configuration guideline
- As load increases so does jitter and latency
- Firewall feature capabilities of mixing non-voice traffic with voice may impact
- No multicast or QoS



DHCP and ARP Vulnerabilities

- Infrastructure
  - DHCP spoofing, DHCP DoS, Rogue DHCP Server
    - Untrusted DHCP Server providing non corporate addresses – in particular to send traffic route to Sniffing device
  - ARP spoofing, MAC Address Spoofing
    - Used to spoof real devices such as routers – another method to intercept traffic





Source: Cisco Systems, 2004

DoS and DDoS

- Traffic Rate Limiter configured per switch port
  - Configured close to endpoints
  - Signaling at 10pps
  - Media at 50-100pps
  - QoS and Scavenger Class
- Intrusion Detection/Prevention Systems

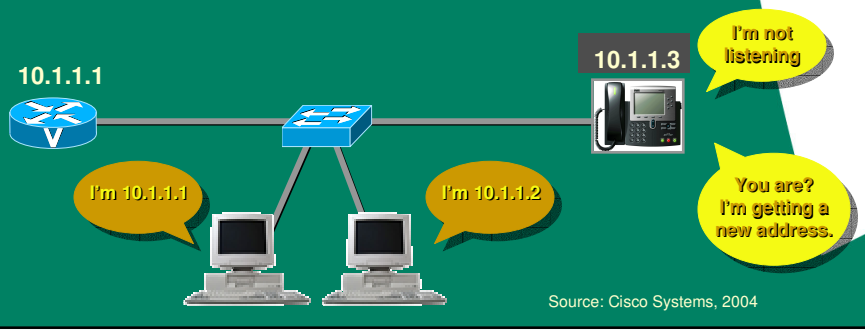
Phone Hardening

Phone Authentications & Encryptions

- Auto-Registrations must be disabled
- Phone Authentications
  - Phone images with digital signatures
  - Configuration files are signed by the site administrator
- Media Encryptions
  - Secure RTP (SRTP), RFC3711
  - Keys exchanged in TLS-encrypted signaling
    - draft-ietf-mmusic-sdescriptions

Phone Hardening: Ignore GARP

- IP protocol that allows devices to announce themselves.
- Blocks acceptance of Gratuitous ARP (GARP) by the phone.
- Prevents malicious device from assuming the identity of something else (default router) to become man-in-the-middle.

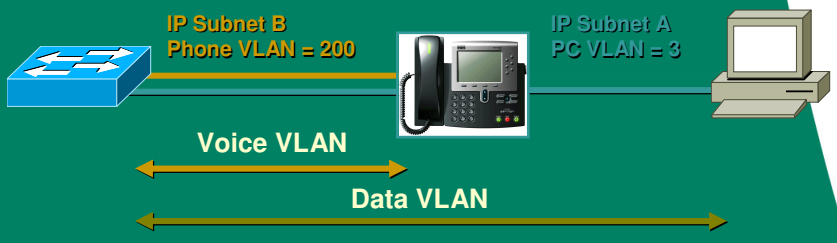


Source: Cisco Systems, 2004

Block PC Access to Voice VLAN

- 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



Source: Cisco Systems, 2004

O/S & Application Hardening

IP PABX Security

- OS build has unnecessary services/daemons turned on
- Microsoft/OS critical patches
- Host and Network IDS/IPS
- Anti-virus
- Patch & Release Management

User Authorisation

- Authorisation codes
- Call Detail Reporting
- Toll Fraud Detection
  - Protect against call forwarding, remote call forwarding, and trunk-to-trunk transfers
  - Restrictions on which parts of the dial plan certain phones have access to
  - Dial plan filters control access to exploitative phone numbers, such as 900
  - Forced Authentication Codes or Client Matter Codes prevent unauthorised calls and provide a mechanism for billing and tracking

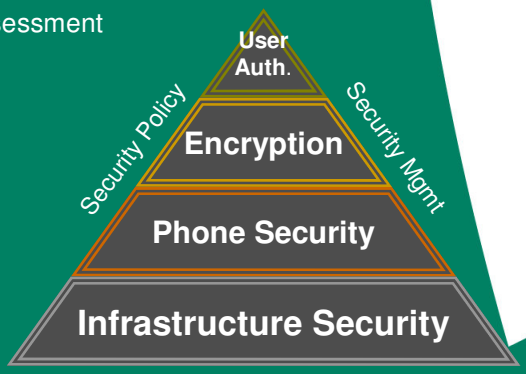
How Much Security Do You Need?

Cost – Complexity – Manpower – Overhead

Bronze Default, Standard.	Silver Moderate, Reasonable	Gold Difficult, Expensive, New
Basic Layer 3 ACL's	Basic Firewalls	Advanced Firewalls
Standard OS Hardening	Advanced Layer 3 ACLs	IPSec / SRTP to Gateways
Unmanaged Host IPS/IDS	Rate Limiting	IPSec to Servers
Anti-Virus	Infrastructure Integrated Security	OOB Management
HTTPS for management traffic	VPN – SOHO/Mobile	NAC / 802.1X
Signed Firmware & Configs	Managed Host IPS/IDS	Network IPS/IDS
Phone Security Settings	SRTP to Phones	Distributed DDoS Protection Sys
	SYSLOG	Incident Mgmt & Response

Summary

- Understand what you are trying to protect
- Determine what you are trying to protect it from
- Build it in layers
- Monitoring & Regular Assessment



Q & A