

VoIP Security

A thorough, comprehensive, in-depth study in 5 – 8 minutes

Association of Collegiate Computing Services (ACCS) of Virginia

Spring Workshop

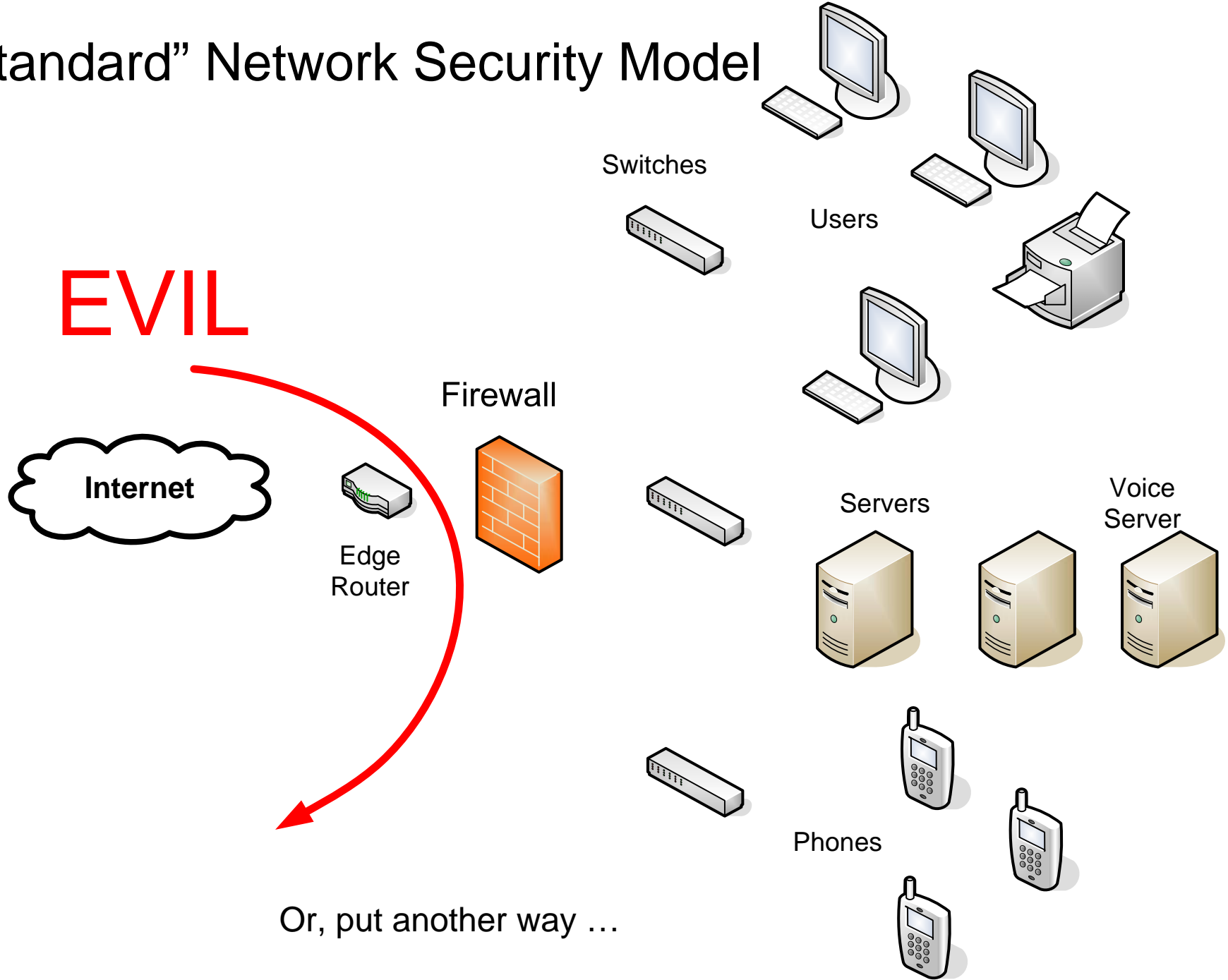
John York, Blue Ridge Community College

April 20, 2006

Executive Summary

- Build security in from the beginning
- Isolate your phones from your computers^(1,2,3)

“Standard” Network Security Model

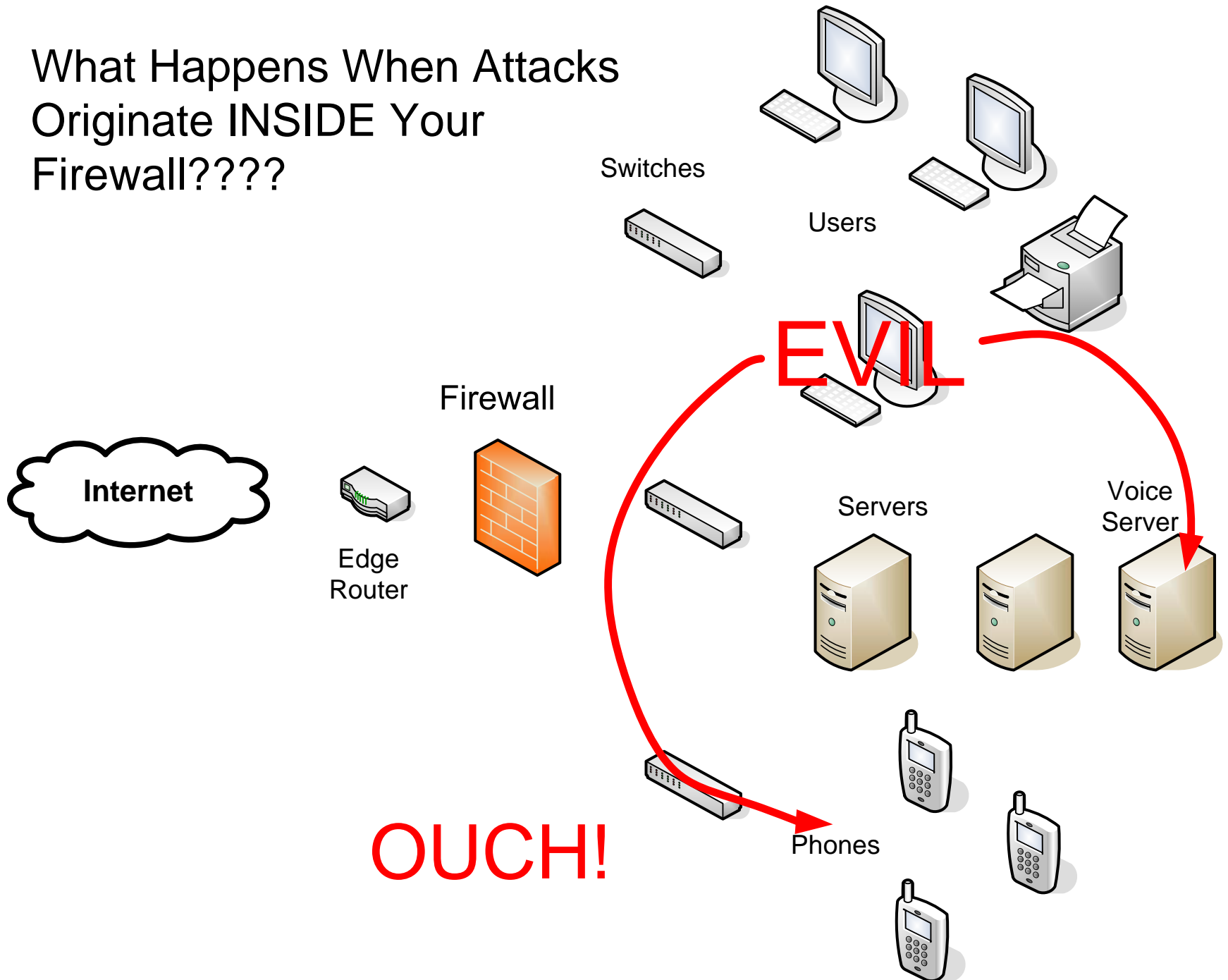


Standard Network Security Model



Hard on the outside, soft and gooey on the inside

What Happens When Attacks Originate INSIDE Your Firewall????



“Attacks Don’t Originate Inside MY Network!!”

Hmmm...what about:

- Laptops that bring Botnets to your net?
- Clueless users who get rooted or backdoored?
- Disgruntled faculty/staff/students?
- Experimenting IT faculty/students⁽⁴⁾?
- Self-inflicted DoS?

“What Can a Bad Guy Do to Me, Anyway?”

- Most VoIP protocols (SIP, H.323, Cisco Skinny Station, RTP) are completely open, ~ clear text
- With access to the voice LAN, she can
 - Own the voice server
 - DoS all or selected phones
 - Eavesdrop on any conversation
 - Make free toll calls
 - Use phones as listening devices

“But My Network is Fully Switched! They Can’t get Me!”

- ARP-cache poisoning works great⁽⁵⁾
 - Send gratuitous ARP packets to both hosts
 - Hosts send traffic to the attacker
 - Attacker relays traffic to the correct host
- There are many session hijackers available
 - Ettercap⁽⁶⁾
 - Cain⁽⁷⁾
 - Write your own with Nemesis⁽⁸⁾ and Perl
- Nice “How-to” on Security Focus⁽⁹⁾

The Biggest Needs

- Protect your VoIP network from the evil coming from the Internet
 - Standard firewall
- Protect your VoIP network from session hijacking and ARP-cache poisoning from within your network
 - ???

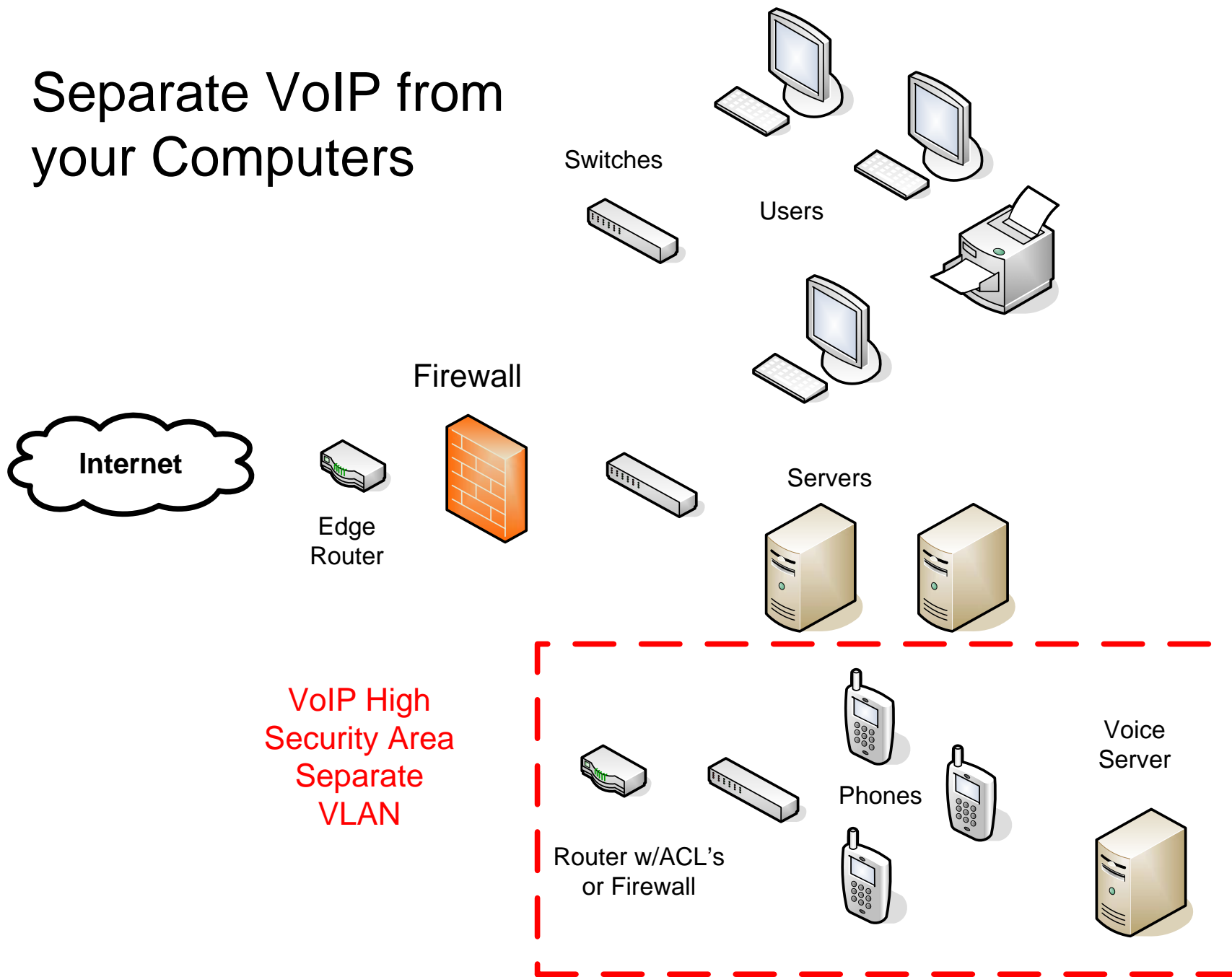
There's Got to be an Easier Way!!

- “Cisco's "maximum-security" VoIP configuration - a midsize CallManager-based system, with call control, voice mail, gateway; a Catalyst 4500- and 6500-based Layer 2/Layer 3 infrastructure; a copious supply of intrusion-detection system (IDS) and PIX firewall security add-ons; **plus a half-dozen Cisco security gurus** supporting the test - earned our **most Secure rating** (see rating criteria, below). Our attack team couldn't disrupt, or even disturb, Cisco's phone operations after three days of trying.” ⁽¹⁰⁾

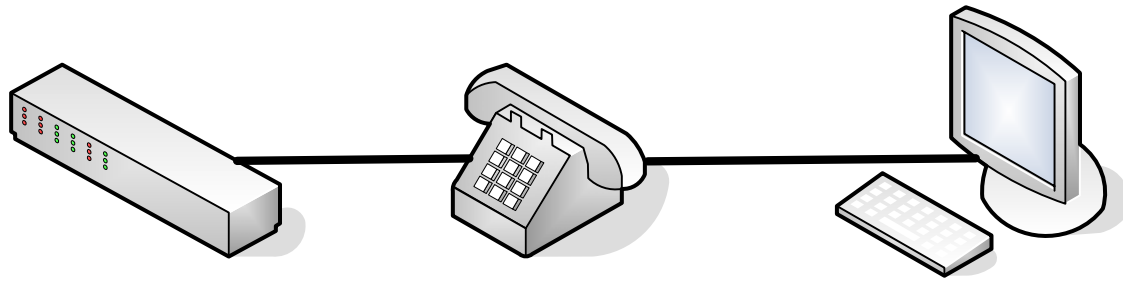
Basic VoIP Security Rule #1

- Isolate your voice and data networks
 - Won't solve all your problems, but it's a great first step.
 - Mantra for VoIP Engineers:
 - PC's are evil
 - PC's are evil
 - PC's are evil
 - ...

Separate VoIP from your Computers



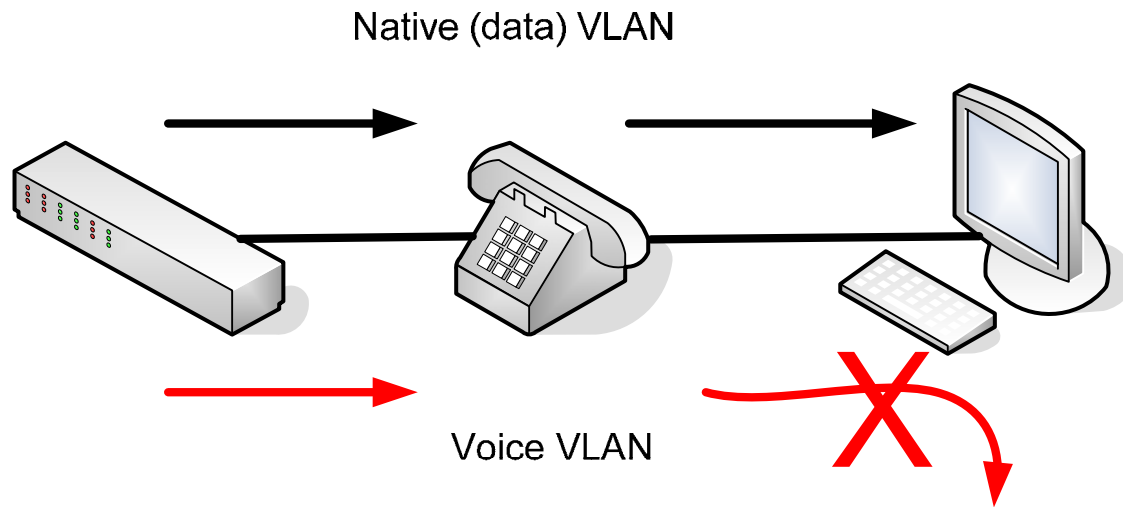
“Phone and Computer Use the Same Cable—How is that Separate?”



Voice VLAN (Cisco⁽¹¹⁾)

- Uses “Native VLAN” feature of IEEE 802.1Q VLAN tagging
- Format of frame for Native VLAN looks the same as a non-VLAN frame—no tagging
 - PC sees Native VLAN traffic as normal
- Frames for all other VLAN’s include tagging
 - PC ignores tagged packets (unless it’s EVIL)

Voice VLAN, continued



- By default (CM 3.3), Cisco phones forward the Voice VLAN traffic to the PC, even though it normally ignores it (allows for phone add-on's in PC)
- TURN THIS OFF!!** If the PC is Øwned, so is the phone!

Other Options

- Deploy an encrypted VoIP system
 - Major vendors' VoIP can be encrypted
 - Generally requires a key infrastructure and requires configuration
- Deploy measures to prevent ARP cache poisoning
 - ARPwatch⁽¹²⁾ (detection only)
 - Cisco DHCP snooping⁽¹³⁾ and Dynamic ARP Inspection⁽¹⁴⁾ (prevention)
 - None of these are easy, especially for large networks
- CallManager 3.3(3) or later can disable gratuitous ARP

Side Benefit of VoIP—no Modems!

- It's hard to connect modems to VoIP
 - Requires an analog telephone adapter
 - Usually configured by the VoIP admin
- No more war-dialing attacks!!
 - Assuming, of course, you get rid of the old analog system...

Conclusion

- Build security in from the beginning
- Isolate your phones from your computers

References

1. Security Considerations for Voice Over IP Systems
 - <http://csrc.nist.gov/publications/nistpubs/800-58/SP800-58-final.pdf>
2. Securing Your Network for IP Telephony
 - http://www.cisco.com/application/pdf/en/us/guest/netsol/ns391/c654/cdccont_0900aecd801e6159.pdf
3. SECURING IP VOICE
 - http://www.cisco.com/en/US/netsol/ns340/ns394/ns165/networking_solutions_white_paper0900aecd80240249.shtml
4. An Assignment From Professor Packetslinger of the School of Loose Screws
 - <http://isc.sans.org/diary.php?storyid=1155>
5. TRAFFIC TRICKS--ARP spoofing and poisoning
 - http://www.linux-magazine.com/issue/56/ARP_Spoofing.pdf
6. Ettercap
 - <http://ettercap.sourceforge.net/>
7. Cain
 - <http://www.oxid.it/cain.html>
8. Nemesis
 - <http://nemesis.sourceforge.net/>
9. Two Attacks Against VoIP
 - <http://www.securityfocus.com/infocus/1862>

References, continued

10. Breaking through IP telephony
 - <http://www.networkworld.com/reviews/2004/0524voipsecurity.html>
11. Configuring Voice VLAN
 - <http://www.cisco.com/univercd/cc/td/doc/product/lan/c3550/12113ea1/3550scg/swvoip.htm>
12. ARPwatch
 - <http://ee.lbl.gov/>
13. Understanding and Configuring DHCP Snooping
 - http://www.cisco.com/univercd/cc/td/doc/product/lan/cat4000/12_1_13/config/dhcp.htm
14. Configuring Dynamic ARP Inspection
 - http://www.cisco.com/en/US/products/hw/switches/ps4324/products_configuration_guide_chapter09186a008019d0ca.html