

VoIP Penetration Testing: Lessons Learned, Tools and Techniques

Jason Ostrom
Sr. Security Consultant

John Kindervag, CISSP, QSA
Sr. Security Architect



www.vigilar.com



Agenda

- Security and the Converged Network
- The Business Risk
- VoIP Attack Vectors
- VoIP Hopping Attacks
- The VoIP Hopper Tool
- Live Demonstration

Security and the Converged Network

- Convergence – Multiple Types of Information on same Pipe
 - Voice
 - Data
 - Video
- Less Cabling
- Simplify Moves/Adds/Changes
- Toll Bypass
- You can get your Voice Mail in you Inbox!
- But what about Security?



The Business Risk

- Low Awareness as to Security Threats
- Publicly Accessible IP Phones
 - Waiting Areas
 - Conference Rooms
 - Hotel Rooms
- Can an Attacker Gain Privileged Access?




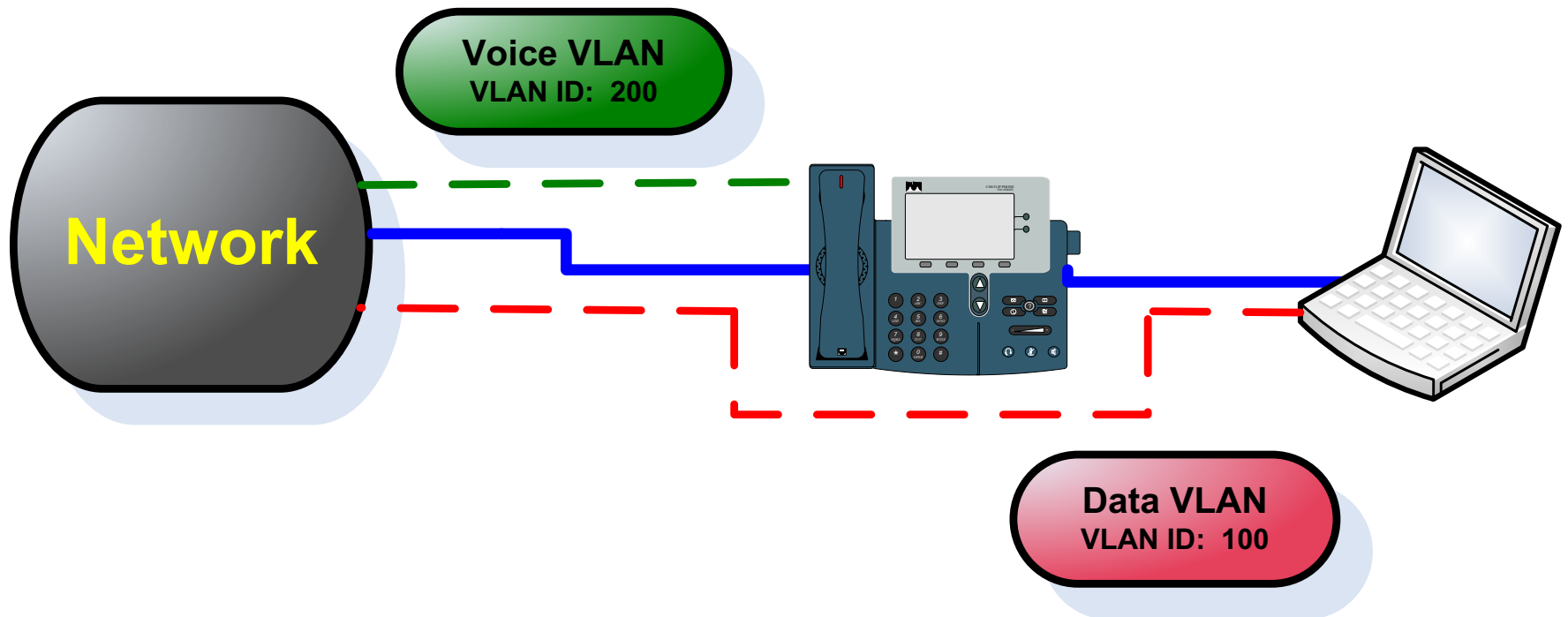
The Business Risk

- The Voice VLAN
- Allows IP Phones to auto-configure
- Phones easily associate to a logically separate VLAN
- Allow simultaneous access for a regular PC

Voice VLAN

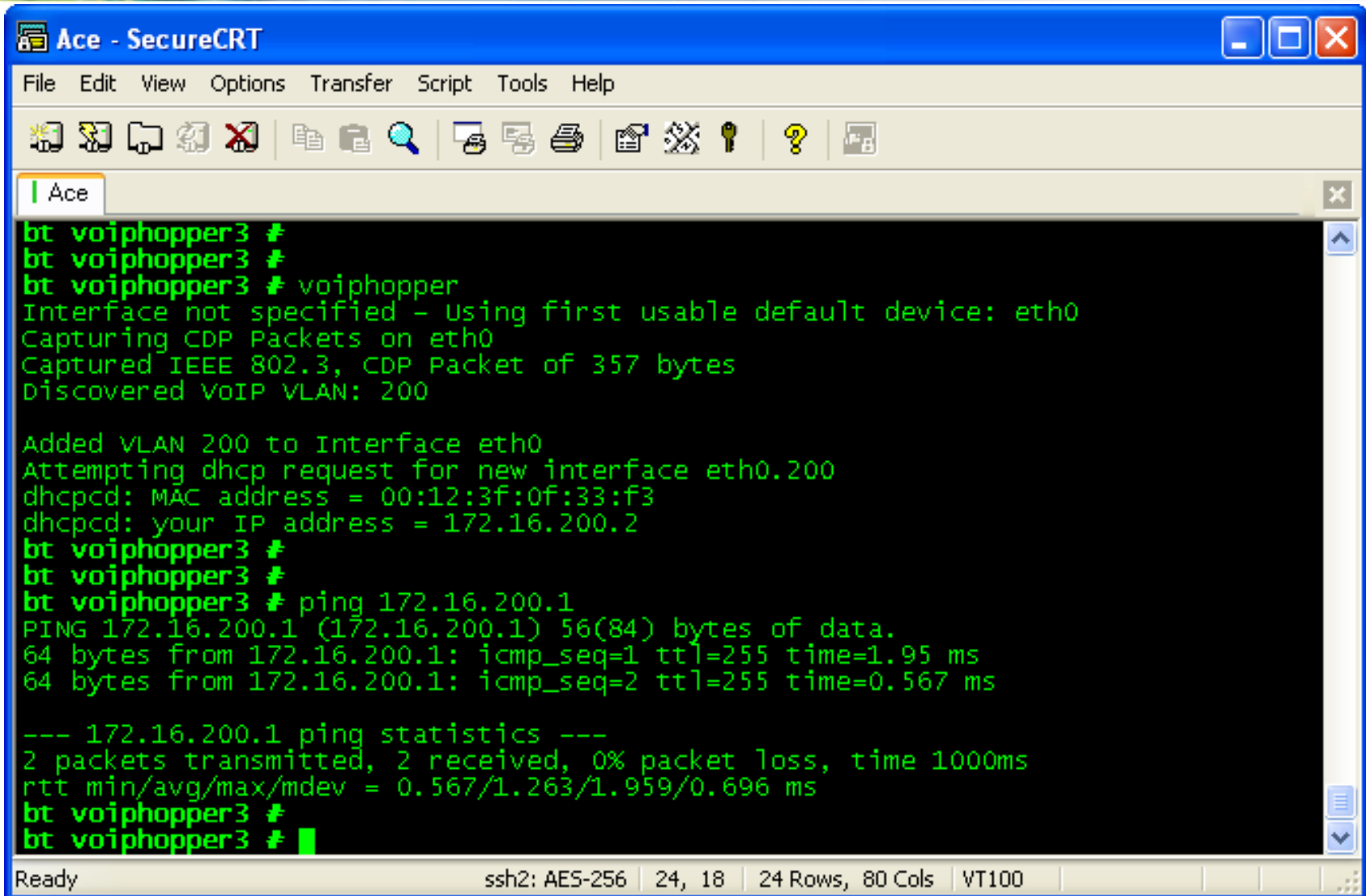
Legend

-  Ethernet Cable
-  Data Traffic
-  Voice Traffic



- “You can’t access our corporate data network from the IP Phones.”
- VoIP Vulnerability Assessment
- Controls Validation
- Gained Administrator access to servers in the data center
- Remote, physically isolated location where the IP Phones were located and believed to be “secure”.

The VoIP Hopper Tool



The screenshot shows a SecureCRT terminal window titled "Ace - SecureCRT". The window has a menu bar (File, Edit, View, Options, Transfer, Script, Tools, Help) and a toolbar with various icons. The terminal session is running a script named "voiphopper" and displays the following output:

```
bt voiphopper3 #  
bt voiphopper3 #  
bt voiphopper3 # voiphopper  
Interface not specified - Using first usable default device: eth0  
Capturing CDP Packets on eth0  
Captured IEEE 802.3, CDP Packet of 357 bytes  
Discovered VoIP VLAN: 200  
  
Added VLAN 200 to Interface eth0  
Attempting dhcp request for new interface eth0.200  
dhcpd: MAC address = 00:12:3f:0f:33:f3  
dhcpd: your IP address = 172.16.200.2  
bt voiphopper3 #  
bt voiphopper3 #  
bt voiphopper3 # ping 172.16.200.1  
PING 172.16.200.1 (172.16.200.1) 56(84) bytes of data.  
64 bytes from 172.16.200.1: icmp_seq=1 ttl=255 time=1.95 ms  
64 bytes from 172.16.200.1: icmp_seq=2 ttl=255 time=0.567 ms  
  
--- 172.16.200.1 ping statistics ---  
2 packets transmitted, 2 received, 0% packet loss, time 1000ms  
rtt min/avg/max/mdev = 0.567/1.263/1.959/0.696 ms  
bt voiphopper3 #  
bt voiphopper3 # █
```

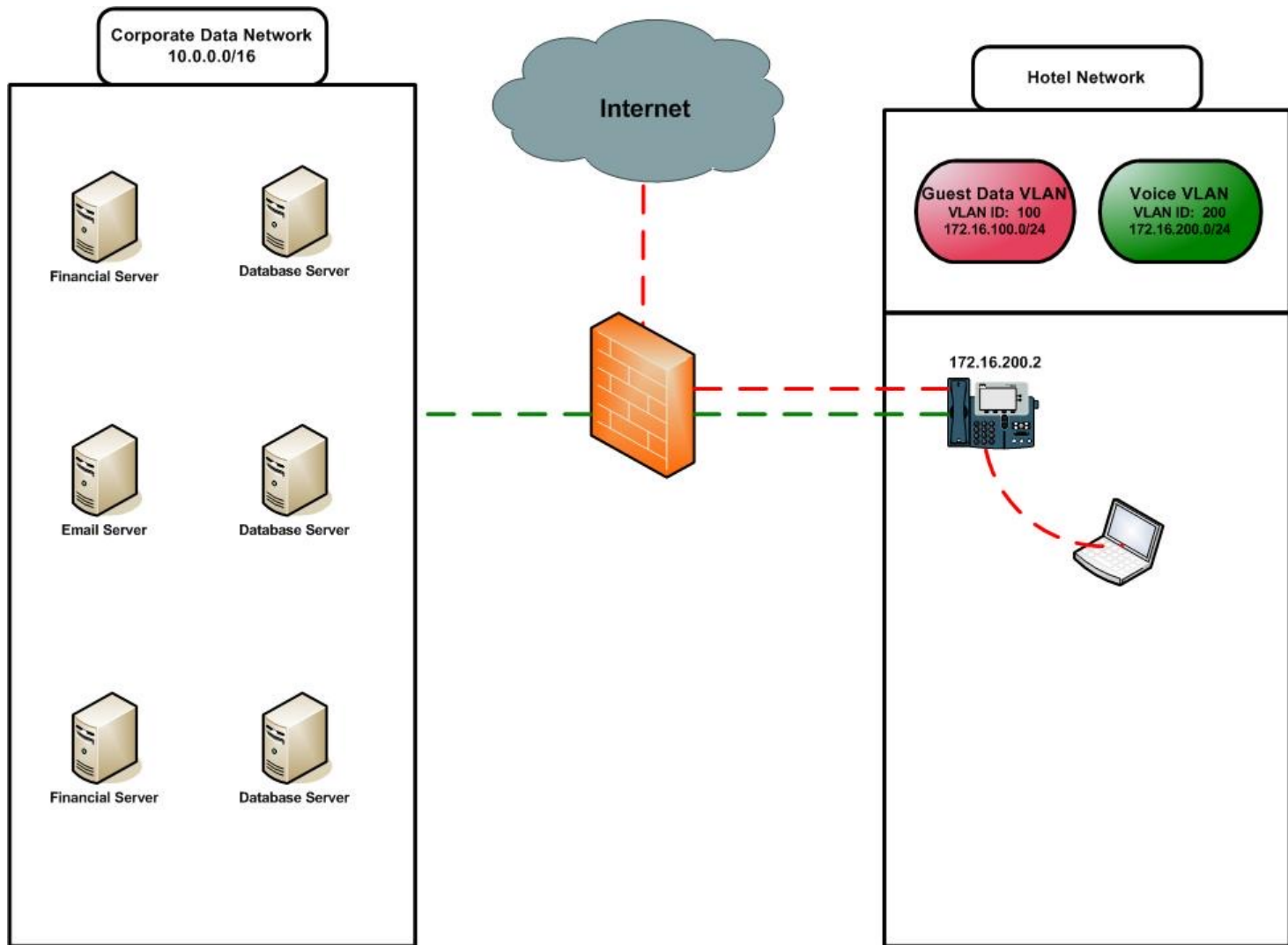
The status bar at the bottom of the window shows "Ready", "ssh2: AES-256", "24, 18", "24 Rows, 80 Cols", and "VT100".

Live Demonstration

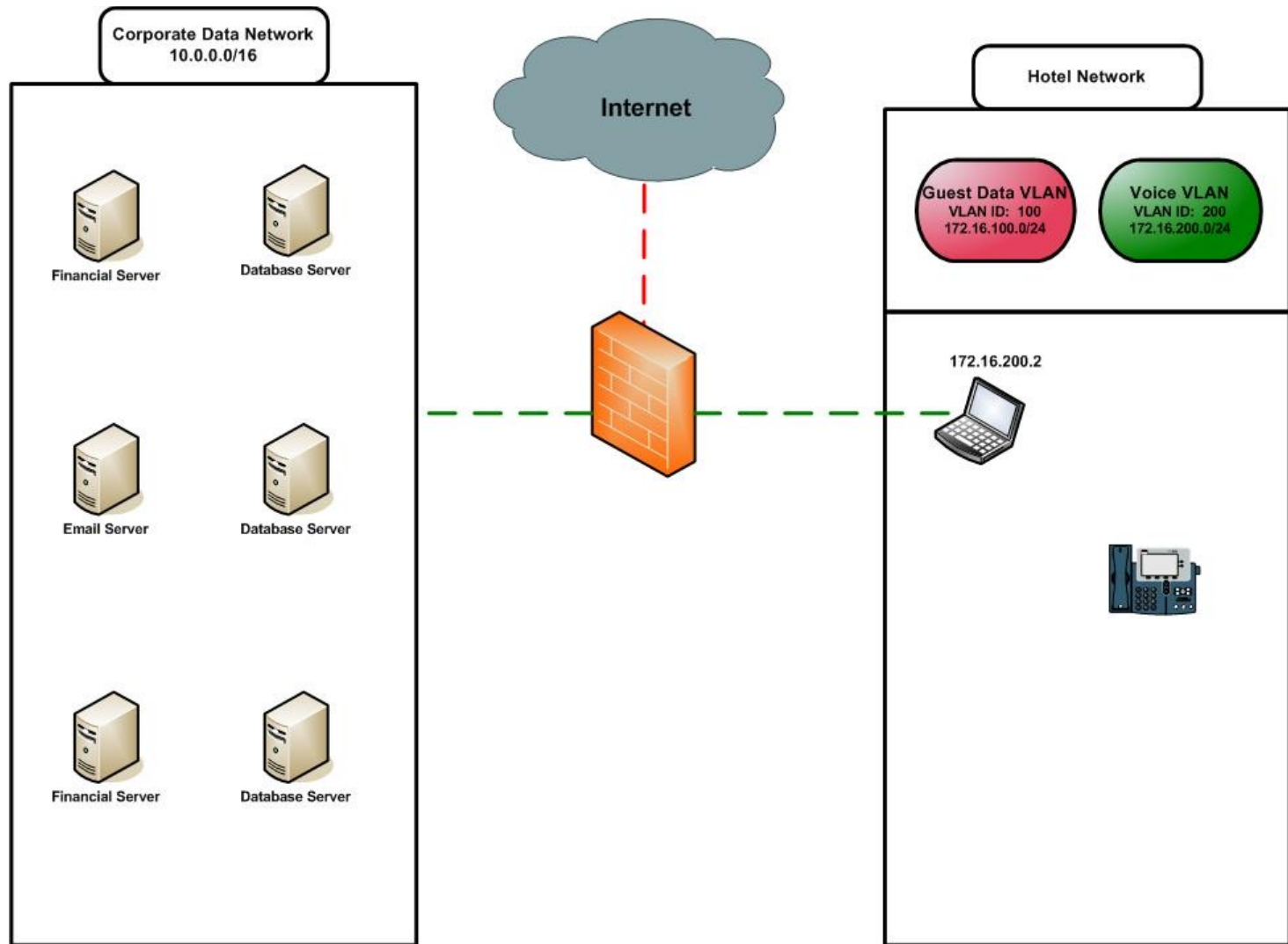


www.vigilar.com

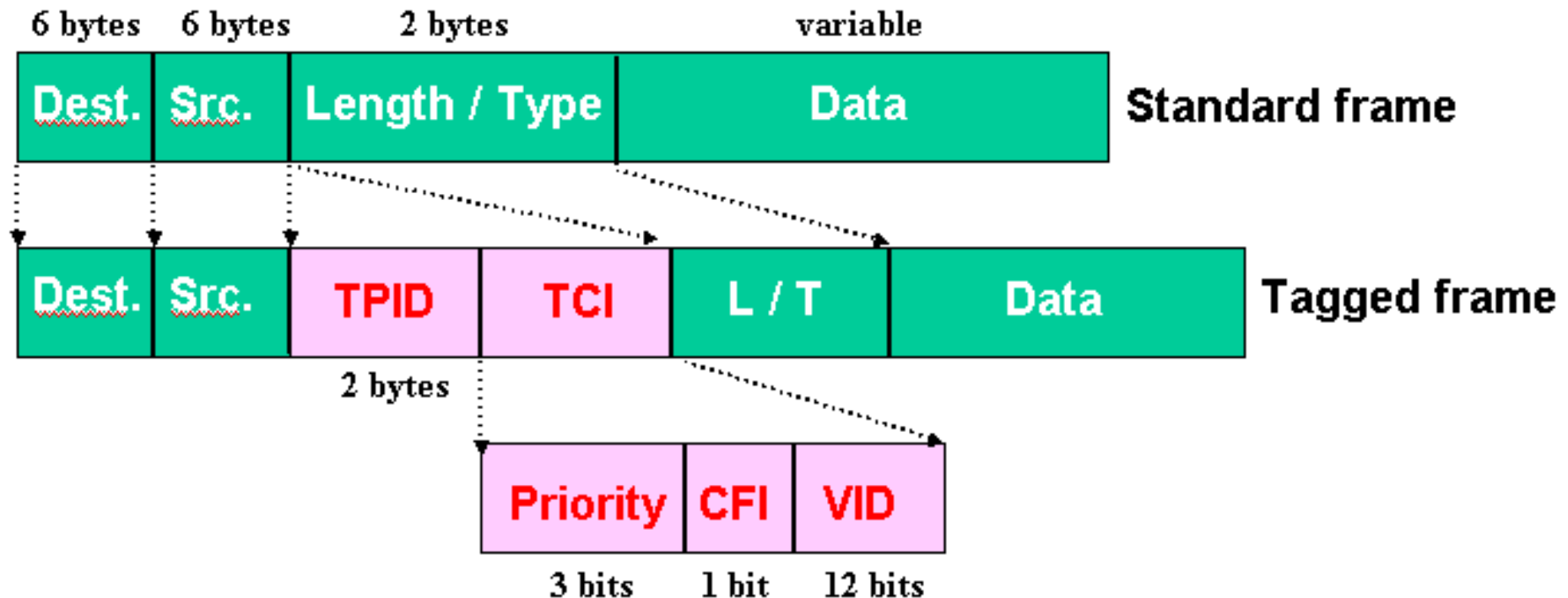
Customer VoIP Network



How this happens



Create a new VLAN Interface on the PC





Clarify Risks

- This is about:
 - Network Infrastructure Security
 - Poor Network Design
- Not About:
 - Exploiting Cisco Unified Communication Manager platform
 - Exploiting Avaya platform

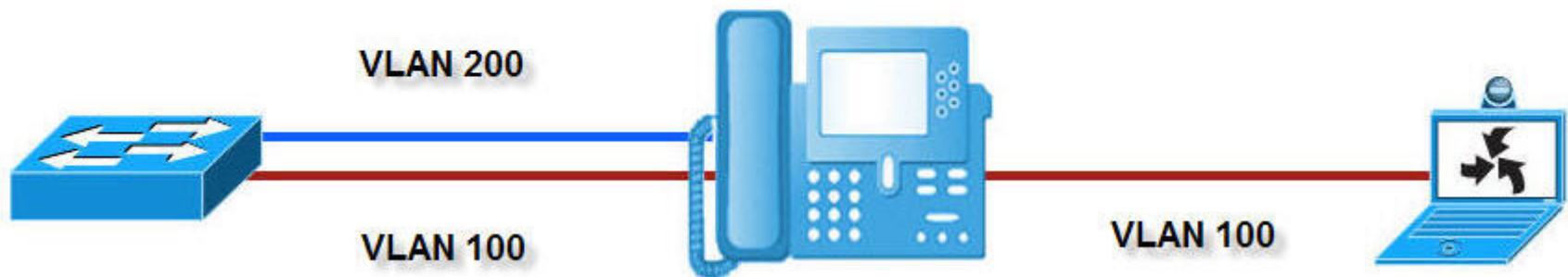
VLAN Hopping Risks

- DoS against IP Phones
- Attacking open ports/services on CallManager platform
- Gaining access to internal network resources when no firewall is in place
- VoIP Hopper doesn't enable Sniffing / Eavesdropping on calls

Demo Setup and IP Addressing

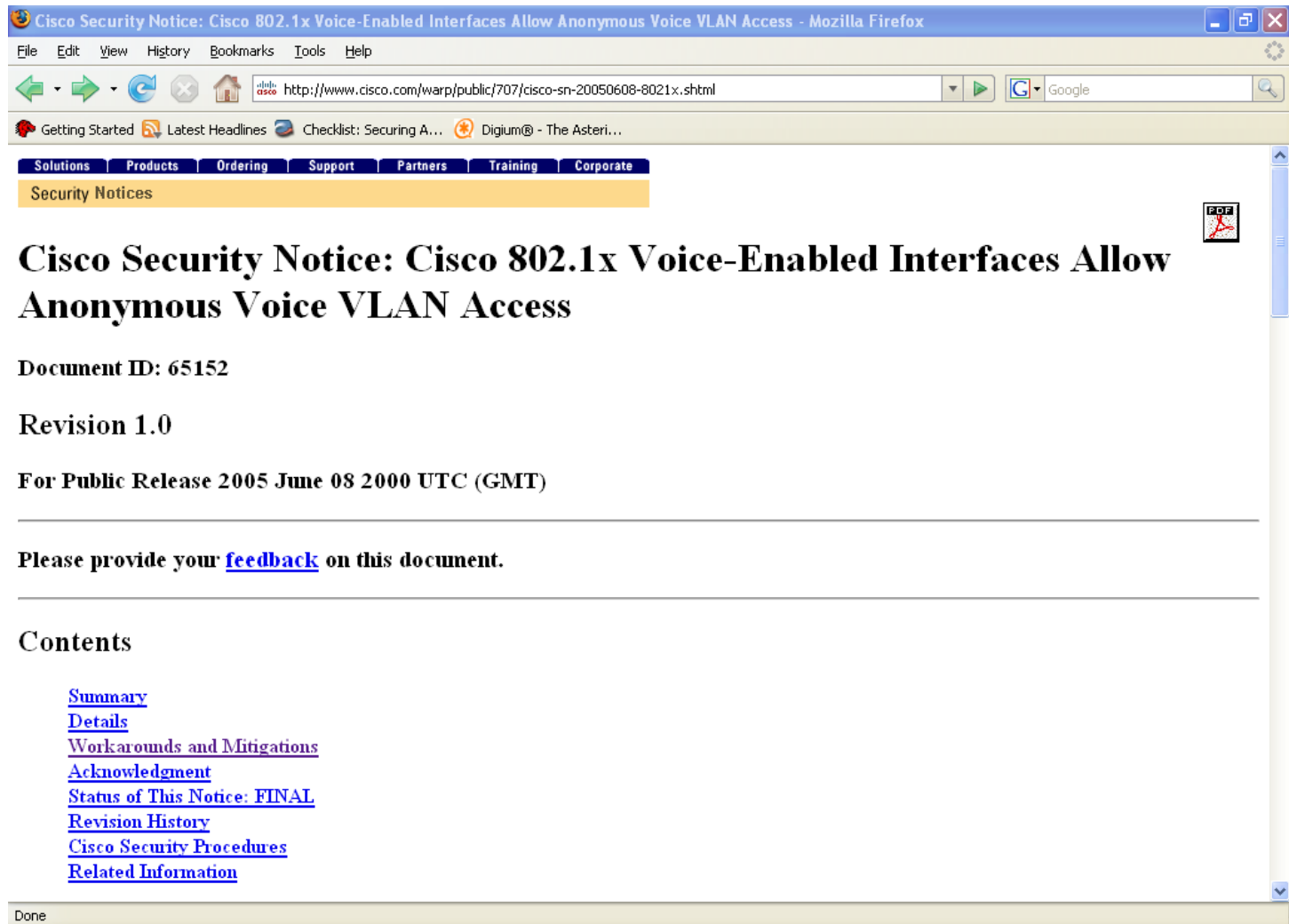
IP Phone Network: 172.16.200.0/24

PC Network: 172.16.100.0/24



Cisco 802.1x Voice Enabled Ports

Credit: Jamal Pecou



The screenshot shows a Mozilla Firefox browser window with the title "Cisco Security Notice: Cisco 802.1x Voice-Enabled Interfaces Allow Anonymous Voice VLAN Access - Mozilla Firefox". The address bar shows the URL "http://www.cisco.com/warp/public/707/cisco-sn-20050608-8021x.shtml". The browser's menu bar includes File, Edit, View, History, Bookmarks, Tools, and Help. The toolbar contains navigation buttons (back, forward, home, stop, reload) and a search bar with the Google logo. Below the toolbar is a navigation bar with links: Getting Started, Latest Headlines, Checklist: Securing A..., and Digium® - The Asteri... The main content area has a navigation bar with links: Solutions, Products, Ordering, Support, Partners, Training, and Corporate. Below this is a section titled "Security Notices". The main heading is "Cisco Security Notice: Cisco 802.1x Voice-Enabled Interfaces Allow Anonymous Voice VLAN Access". Below the heading is a PDF icon. The document ID is "65152". The revision is "1.0". The release date is "For Public Release 2005 June 08 2000 UTC (GMT)". A line of text says "Please provide your [feedback](#) on this document." Below this is a "Contents" section with a list of links: [Summary](#), [Details](#), [Workarounds and Mitigations](#), [Acknowledgment](#), [Status of This Notice: FINAL](#), [Revision History](#), [Cisco Security Procedures](#), and [Related Information](#). The status bar at the bottom says "Done".

Cisco Security Notice: Cisco 802.1x Voice-Enabled Interfaces Allow Anonymous Voice VLAN Access - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://www.cisco.com/warp/public/707/cisco-sn-20050608-8021x.shtml

Getting Started Latest Headlines Checklist: Securing A... Digium® - The Asteri...

Solutions Products Ordering Support Partners Training Corporate

Security Notices

Cisco Security Notice: Cisco 802.1x Voice-Enabled Interfaces Allow Anonymous Voice VLAN Access

Document ID: 65152

Revision 1.0

For Public Release 2005 June 08 2000 UTC (GMT)

Please provide your [feedback](#) on this document.

Contents

- [Summary](#)
- [Details](#)
- [Workarounds and Mitigations](#)
- [Acknowledgment](#)
- [Status of This Notice: FINAL](#)
- [Revision History](#)
- [Cisco Security Procedures](#)
- [Related Information](#)

Done

Mitigation of VLAN Hop from Port 2 of IP Phone

Cisco CallManager 4.1 Administration - Phone Configuration - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Address <https://ccm-justice/CCMAdmin/phoneconfig.asp?pkid={44268B5E-6284-4C84-96E2-7E2B8A280671}&status=uc> Go Links

Key Size (bits) 1024

Operation Completes By** : : : (YYYY : MM : DD : HH)

Certificate Operation Status : None

Multilevel Precedence and Preemption (MLPP) Information

MLPP Domain (e.g., "0000FF")

MLPP Indication Default

MLPP Preemption Default

Product Specific Configuration ⓘ

Disable Speakerphone ☐

Disable Speakerphone and Headset ☐

Forwarding Delay* Disabled

PC Port* Enabled

Settings Access* Enabled

Gratuitous ARP* Enabled

PC Voice VLAN Access* Disabled

Video Capabilities* Disabled

Auto Line Select* Disabled

Web Access* Enabled

* indicates a required item.
** Indicates time on Publisher.

[Back to top of page](#)
[Back to Find/List Phones](#)

Reset succeeded.

Local intranet

Mitigation of VLAN Hop from Port 2 of IP Phone

Cisco CallManager 4.1 Administration - Phone Configuration - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Address <https://ccm-justice/CCMAdmin/phoneconfig.asp?pkid={44268B5E-6284-4C84-96E2-7E2B8A280671}&status=uc> Go Links

Key Size (bits) 1024

Operation Completes By** : : : (YYYY : MM : DD : HH)

Certificate Operation Status : None

Multilevel Precedence and Preemption (MLPP) Information

MLPP Domain (e.g., "0000FF")

MLPP Indication Default

MLPP Preemption Default

Product Specific Configuration ⓘ

Disable Speakerphone ☐

Disable Speakerphone and Headset ☐

Forwarding Delay* Disabled

PC Port* Enabled

Settings Access* Enabled

Gratuitous ARP* Enabled

PC Voice VLAN Access* Disabled

Video Capabilities* Disabled

Auto Line Select* Disabled

Web Access* Enabled

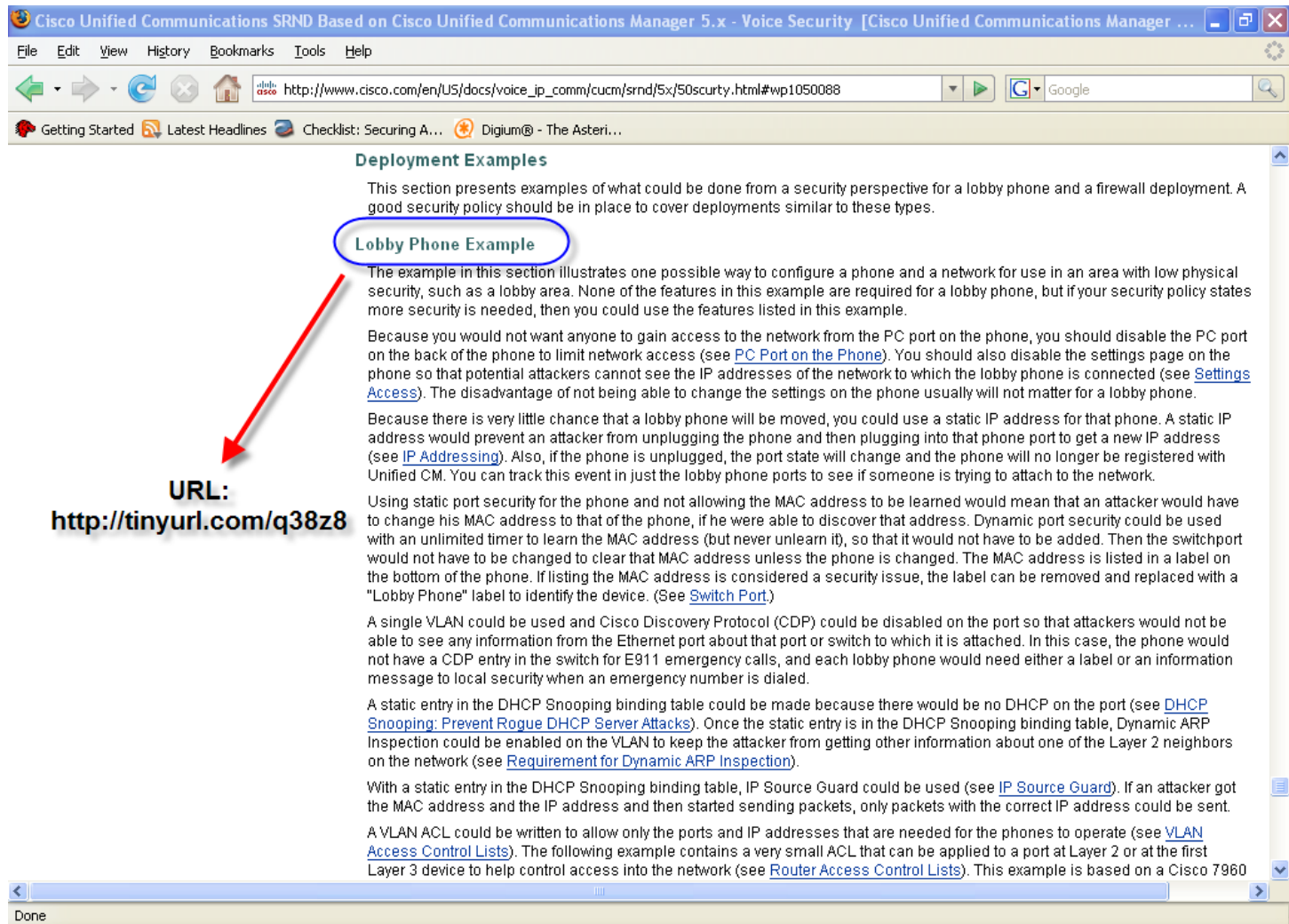
* indicates a required item.
** Indicates time on Publisher.

[Back to top of page](#)
[Back to Find/List Phones](#)

Reset succeeded.

Local intranet

Lobby Phone Deployment Cisco Recommendations



Cisco Unified Communications SRND Based on Cisco Unified Communications Manager 5.x - Voice Security [Cisco Unified Communications Manager ...]

File Edit View History Bookmarks Tools Help

http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/srnd/5x/50scurty.html#wp1050088

Getting Started Latest Headlines Checklist: Securing A... Digium® - The Asteri...

Deployment Examples

This section presents examples of what could be done from a security perspective for a lobby phone and a firewall deployment. A good security policy should be in place to cover deployments similar to these types.

Lobby Phone Example

The example in this section illustrates one possible way to configure a phone and a network for use in an area with low physical security, such as a lobby area. None of the features in this example are required for a lobby phone, but if your security policy states more security is needed, then you could use the features listed in this example.

Because you would not want anyone to gain access to the network from the PC port on the phone, you should disable the PC port on the back of the phone to limit network access (see [PC Port on the Phone](#)). You should also disable the settings page on the phone so that potential attackers cannot see the IP addresses of the network to which the lobby phone is connected (see [Settings Access](#)). The disadvantage of not being able to change the settings on the phone usually will not matter for a lobby phone.

Because there is very little chance that a lobby phone will be moved, you could use a static IP address for that phone. A static IP address would prevent an attacker from unplugging the phone and then plugging into that phone port to get a new IP address (see [IP Addressing](#)). Also, if the phone is unplugged, the port state will change and the phone will no longer be registered with Unified CM. You can track this event in just the lobby phone ports to see if someone is trying to attach to the network.

Using static port security for the phone and not allowing the MAC address to be learned would mean that an attacker would have to change his MAC address to that of the phone, if he were able to discover that address. Dynamic port security could be used with an unlimited timer to learn the MAC address (but never unlearn it), so that it would not have to be added. Then the switchport would not have to be changed to clear that MAC address unless the phone is changed. The MAC address is listed in a label on the bottom of the phone. If listing the MAC address is considered a security issue, the label can be removed and replaced with a "Lobby Phone" label to identify the device. (See [Switch Port](#).)

A single VLAN could be used and Cisco Discovery Protocol (CDP) could be disabled on the port so that attackers would not be able to see any information from the Ethernet port about that port or switch to which it is attached. In this case, the phone would not have a CDP entry in the switch for E911 emergency calls, and each lobby phone would need either a label or an information message to local security when an emergency number is dialed.

A static entry in the DHCP Snooping binding table could be made because there would be no DHCP on the port (see [DHCP Snooping: Prevent Rogue DHCP Server Attacks](#)). Once the static entry is in the DHCP Snooping binding table, Dynamic ARP Inspection could be enabled on the VLAN to keep the attacker from getting other information about one of the Layer 2 neighbors on the network (see [Requirement for Dynamic ARP Inspection](#)).

With a static entry in the DHCP Snooping binding table, IP Source Guard could be used (see [IP Source Guard](#)). If an attacker got the MAC address and the IP address and then started sending packets, only packets with the correct IP address could be sent.

A VLAN ACL could be written to allow only the ports and IP addresses that are needed for the phones to operate (see [VLAN Access Control Lists](#)). The following example contains a very small ACL that can be applied to a port at Layer 2 or at the first Layer 3 device to help control access into the network (see [Router Access Control Lists](#)). This example is based on a Cisco 7960

URL:
<http://tinyurl.com/q38z8>

Done



Hiding & Filtering MAC Address?

- Placing a hub between the IP Phone and wall, an attacker can sniff the MAC Address. This bypasses Administrator attempts to hide the MAC Address by removing the sticker or locking the Phone settings.
- Physical Security of the IP Phone switchport

Phone CDP Security: Is it the Answer?

- A new Cisco IOS Feature available in 12.2.36 SE and later
- Uses Line Power, CDP, and Full Duplex to only allow the Cisco Unified IP Phone Voice VLAN traffic
- Port goes into err-disable when a PC is attached directly to the port.

Can be bypassed

- Scenario 1: With only Phone CDP Security enabled, plug into PC Port on IP Phone and run VoIP Hopper.
- Scenario 2: Customer has disabled PC Port on their IP Phones and Phone CDP Security is enabled. When MAC Address filtering is not implemented, a rogue IP Phone can be brought into the environment, and used to gain access to Voice VLAN.



Mitigate VLAN Hopping (Cisco)

- 1. Phone CDP Security
- 2. MAC Address filtering to only allow MAC of IP Phone on switchport
- 3. Disable PC Port, and/or PC Voice VLAN Access



VoIP Hopper future

- Ethernet card supporting PoE
- Fix DHCP code
- New DHCP Option for Avaya
- Alcatel support for DHCP Option
- Trunk port encapsulation features

VoIP Hopper Information

- Project Download –
<http://voiphopper.sourceforge.net>
- Included in BackTrack3
- <http://remote-exploit.org> – thanks Martin Muench
- Security Focus Article
- <http://www.securityfocus.com/infocus/1892>



Contact Information

Jason Ostrom, CCIE Security #15239
Sr. Security Consultant
jostrom@vigilar.com

John Kindervag, CISSP, QSA
Sr. Security Architect
jkindervag@vigilar.com

**If you would like a copy of this
presentation please contact:**
marketing@vigilar.com

VoIP Hacker Clowns

Hackers gain access to private hotel network using Cisco VoIP | NetworkWorld.com Community - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://www.networkworld.com/community/node/20894

Getting Started Latest Headlines Checklist: Securing A... Digium® - The Asteri...

[Permalink](#)
Read more about:
[Cisco](#) [convergence](#) [hackers](#) [VoIP](#)

VoIP hacker clowns

Submitted by [meatpieandtatters](#) on Tue, 10/23/2007 - 10:04am.

What a freaking joke! Two bozos hack into a Cisco system, and then laud Avaya for it's security? Gorilla marketing if ever I heard it!

[report spam](#) [Reply](#) [Forward to a friend](#)

Saw the presentation

Submitted by palabraup (not verified) on Wed, 10/24/2007 - 11:28am.

Saw the presentation meatpie, you might tap the breaks. The comment was that Avaya had *slightly* better security. They are just as vulnerable as Cisco IP Phones and they demonstrated that as well.

[report spam](#) [Reply](#) [Forward to a friend](#)

Reply to Meatpie

Submitted by Bithead (not verified) on Fri, 10/26/2007 - 8:05am.

Typical reaction from a cisco drone. It appears you have been swimming in your large VAT of Cisco Kool Aid for far too long. None of this should be surprising to anyone with a modicum of objectivity. Cisco is typically the target because they are the most

Done

VHC (VoIP Hacker Clowns)



