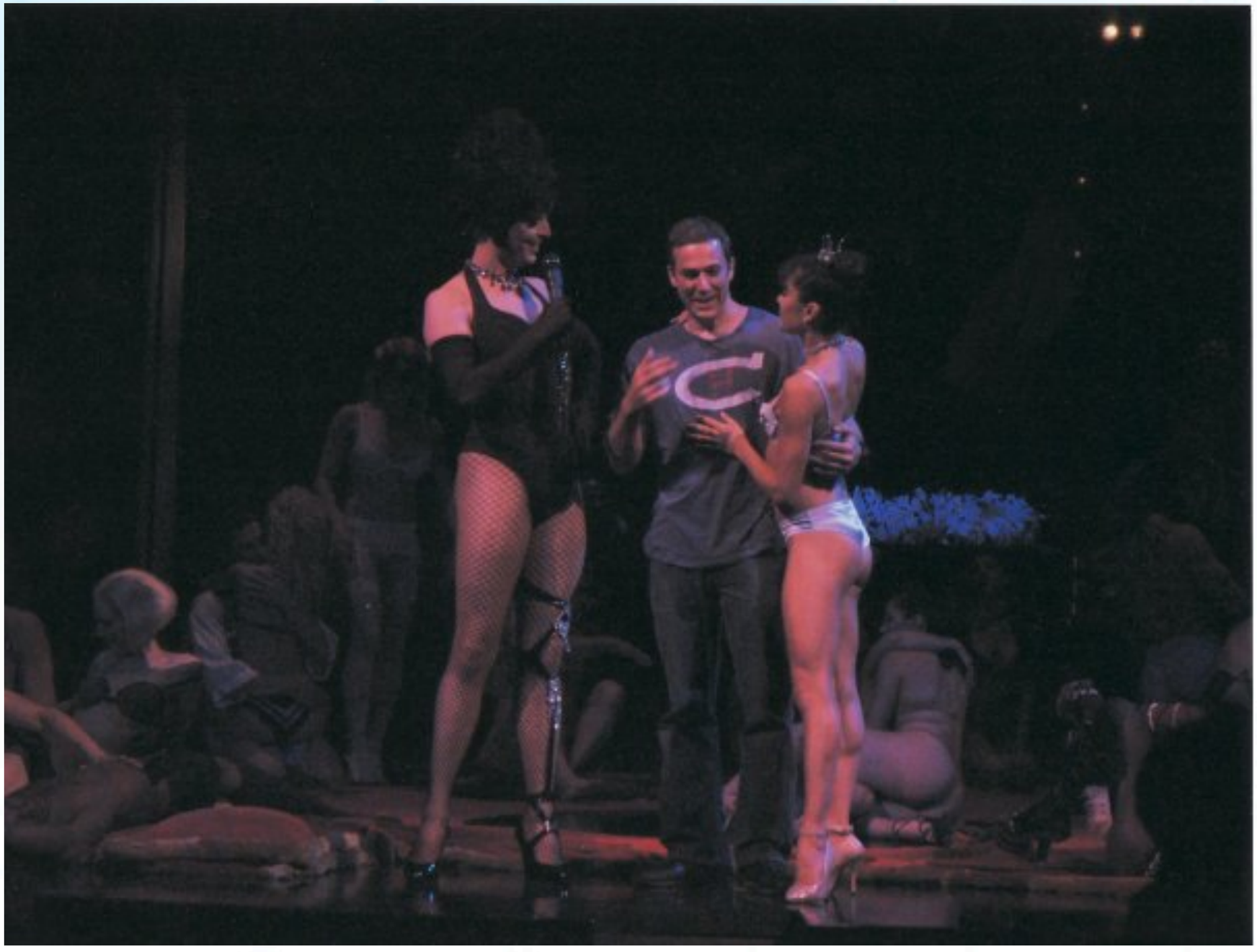
VIPER Lab

WWW.VIPERLAB.NET

VoIP Hopping the Hotel: Attacking the Crown Jewels through VoIP

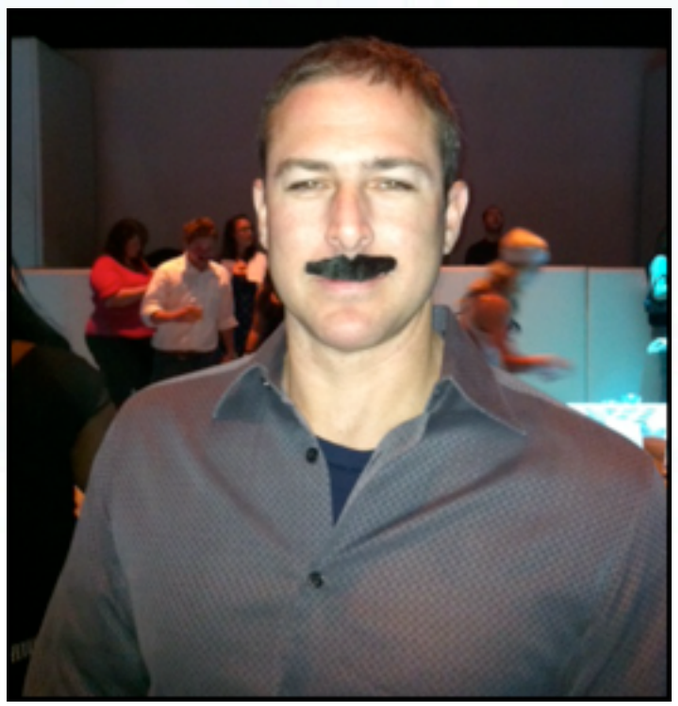
Jason Ostrom

VIPER “Research” in Las Vegas



Thank you

- Friends and associates
  - Who might be here
    - Charles, Arjun, Tom, Victor, Zack, Brian, Chris, Shaq
  - Who couldn't make it here
    - Ed S.
    - Erik G.
    - Camey Y.



Thanks to everyone else in this room right now, for attending my talk.

Agenda

- VIPER Intro
- UC Business Examples
- Live Demo & Case Study: Hotel VoIP Vulnerability
- Live Demo & Case Study: LLDP-MED
- Conclusion

What is VIPER

- VIPER R&D (Voice over IP Exploit Research)
  - Author open source security tools (VAST)
  - LAVA (Load Analysis & Vulnerability Assessment)
  - VoIP Honeypot
- Penetration Testing of VoIP and UC Networks
  - "field research" - understand real vulnerabilities & problems in production networks
  - Proactive identification of client vulnerabilities before someone else

Market: VoIP in Hotels

- Market is growing
  - Worldwide revenue $869 million in 2008
  - By end of 2014, will exceed $2 billion (ABI Research)
- Currently most adopted in luxury resort hotels
  - Catering to clientele willing to spend > $300 night
- Expected to penetrate mid-range hotels soon
- High-end hotels using technology as a differentiator

Market: VoIP in Hotels

ABIresearch®
technology market intelligence

About ▼ | Research ▼ | Consulting ▼ | Media ▼ | Events ▼ | Careers | Contact ▼

Mobile Devices & Tablets | Mobile Software & Services | Connected Home & Broadband | Media & Content | Consumer Trends | Teardowns & Components | Mobile Infrastructure | M2M & Embedded | Security Identifica

IP Telephony Revenue in the Hospitality Industry Will Top $2 Billion in 2014

NEW YORK - January 22, 2010

Sophisticated systems based on IP telephone networks in hotels will increasingly enable a range of new services aimed at improving customer service in hotels and resorts. Although worldwide revenue from such systems totaled only $869 million in 2008, by the end of 2014 annual earnings will exceed $2 billion.

These systems will eventually penetrate mid-range hotels, but in the initial period will be found mainly in the top-tier of properties catering to those willing to spend $300 or more a night. According to ABI Research vice president Stan Schatt, "High-end hotels are increasingly turning to technology as a differentiator to attract a high-spending clientele. These services put a premium on improving customer service and staff accountability."

Benefits to Hotel

- Well known benefits of VoIP
  - Simplicity of Network Management
  - Reduction of cabling cost (VoIP, data, video over single cabling plant)
  - Reduction of telecom expenses (Global offices)
- Ad and marketing revenue directly on the IP Phones ~ revenue stream to hotel
- Improved customer service ~ increased revenue from repeat customers

Benefits to Hotel (continued)

- New VoIP applications provide improved guest service ~ technology differentiator (competition)
- VoIP as a QA tool, to improve customer service
- Rebuild lost telephone service revenue (from mobile phones)
  - European roaming charges outside home area are inflated
  - VoIP can provide lower costs than roaming charges, benefiting Hotel and guests

Benefits to Hotel (continued)

- Low cost of international calling over VoIP
  - Provide an international inbound number in home country of guest, increasing reservations
  - Growing Trend in Hospitality: Giving guests free limited or unlimited international calling
- VoIP over Wi-Fi Wireless in Hotels
  - For employee communication
  - For guests, ordering products and services with click of a button

Benefits to Guests

- Improved service
  - Order room service from IP Phone menu
  - Browse colorful menu displays showing dining options in a hotel, while making reservation
  - New products, services (VoIP over WiFi handsets)
- Convenient, advanced call features
  - Automated wake up call, Voice mail, Call Forwarding
- Lowered telecom costs passed on to guests
  - Cheaper guest International, domestic calling

VoIP Security benefits

- For the hotel
  - Prevents unauthorized access to internal systems
  - Protects hotel guests from UC specific attacks, like eavesdropping
  - Of course, it is the responsibility of the hotel to provide security for the hotel guest
- For the guest
  - Prevents eavesdropping on private communications through IP Phones
    - Recording VoIP conversations, re-construction of media
    - Trapping sensitive data, such as credit card data, sent over VoIP

Case Studies: VoIP in Hotels

Sources for Case Studies

← ITU TELECOM Africa 2008:A formidable Tanzanian success story

Vintag

Can Voip Save Hotel Telephone Revenue?

Posted on April 9, 2011 by

Article by Marty R. Milette

VoIP capabilities save hotel money, keep guests connected

Andrew R. Hickey, Senior News Writer

Published: 8 Feb 2007

VoIP capabilities without rip and replace? Sounds unheard of. But that's what the Seaport Hotel in Boston wanted when implementing a new in-room portal that allows guests to access services such as IP phone calls and other applications.

Harvard Business Review

www.hbr.org

FRONTIERS

Internet telephone technology, rapidly displacing the traditional kind, isn't just inexpensive. It's revolutionizing the way

Using VoIP to Compete

by Kevin Werbach

How VoIP Has Influenced the Hotel Industry: Part 1

By Matthew Nickasch on Wed, 06/11/08 - 2:05pm.

Email Comment Print Recommend Sign Up to see what your frien

Throughout the last few months, we've discussed quite a bit about convergence, VoI the like. What's been increasingly interesting, however, is to chart the "spread" of co technologies from industry to industry.

Hotel 1000 Uses VOIP to Pamper Guests

in LinkedIn 0 Share 0 Tweet 0 ShareThis New

By: Paula Musich

Case Study: Peninsula Hotels

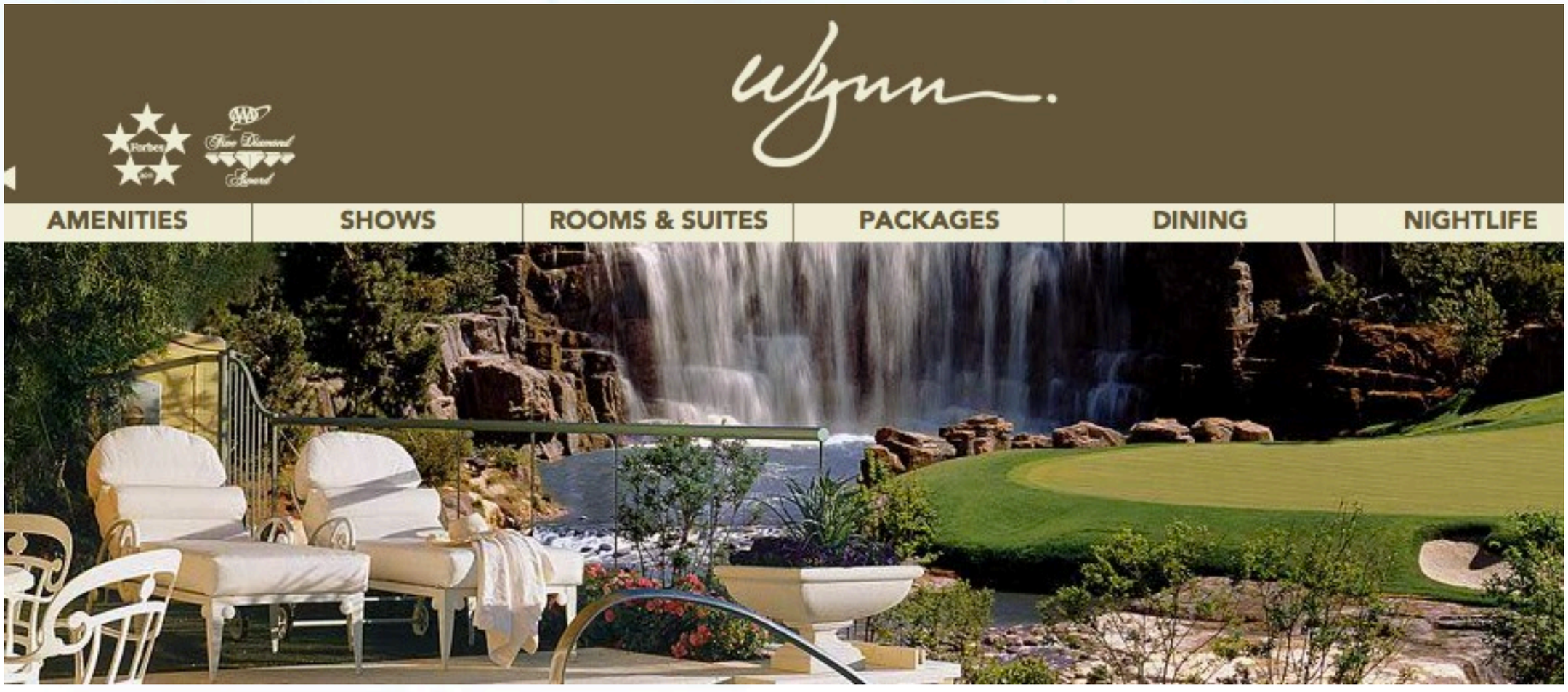
- Five-star luxury hotel chain in North America and Asia
- 14 Hotel Chain presence globally linked by VoIP
- Telecom cost savings from VoIP

Case Study: Peninsula Hotels

- Chain can manage all of its reservations from a Global Customer Service Center
- Employees can communicate with VoIP (significant cost savings)
- Each employee has his or her own number which stays with them no matter what location they're in
- Caller ID from global locations

Case Study: Wynn Las Vegas

- Improved customer service through VoIP
- Improved guest experience through VoIP



Case Study: Wynn Las Vegas

- Strategy to “pamper and delight guests”
- Each guest room has an IP Phone
  - Reservations over touch screen
  - Guests call concierge to arrange dinner reservations while browsing menus and pictures of dining room on phone’s color display
  - When guest calls service staff, VoIP rings their cell and desk phone, to assure the guest gets through

Case Study: Wynn Las Vegas

Quote:

"As Wynn Resorts is showing, the entire organization can become a contact center. The phone is no longer just a communication channel; it's a form of customer service in its own right."

(Harvard Business Review)

Case Study: Hotel 1000 Seattle

Case Study: Hotel 1000 Seattle

- Luxury hotel in Seattle deployed Cisco VoIP technology
- VoIP custom applications created by Percipia
- Convergence in Hotel: Single infrastructure for data, voice, video, and security

Case Study: Hotel 1000 Seattle

- Downtown Seattle, 120 guest rooms and 47 condominium units
- 3 levels of underground parking accessed via valet car elevator
- Multiple custom applications
  - Video valet system
  - Condominium security entry application
  - VoIP application to detect guest presence and set room preferences

Case Study: Hotel 1000 Seattle

- Video Valet system:
  - Guest touches screen on IP Phone, custom app
  - Sends signal to valet drivers mobile phone, vehicle locator system that notifies drivers of vehicle location
  - Driver closest to car accepts request with Cisco 7920 Wi-Fi phone, notifying other drivers that request taken
  - Elevator call button on Wi-Fi phone activates Hotel 1000 car elevator and brings it to the level where car and driver are located.
  - Valet driver can use WiFi phone to send a picture to owner of car ready, which shows up on Cisco IP Phone display

Case Study: Hotel 1000 Seattle

- Good Quotes
  - "It is never just about bricks and mortar, nor is it about technical bells and whistles. It is about the experience that matters to the individual traveler. It made sense to round out the guest experience with the technology experience people have at home or in the office, so that they arrive in an environment that is more familiar to them. That is not the norm for most hotels."

The Security Problem

- VLAN Traversal vulnerability
  - Trivial to exploit
  - Leads to unauthorized IP network access
- The Business Risk
  - Deployed to guest rooms
    - Many business benefits
  - All deployments I've observed are at risk
    - Physical ports by default permit VLAN traversal
    - Low awareness

This is "The Vulnerability" - Credit

info | discussion | exploit | solution | references

IEEE 802.1q Unauthorized VLAN Traversal Weakness

Bugtraq ID:	615
Class:	Design Error
CVE:	CVE-1999-1129
Remote:	Yes
Local:	No
Published:	Sep 02 1999 12:00AM
Updated:	Jul 11 2009 12:56AM
Credit:	This research and the resulting post was sent to the Bugtraq mailing list by Dave Taylor <david.taylor@alphawest.com.au> & Steve Schuppp <Steve.schupp@alphawest.com.au>. Further research was provided by "Andrew A. Vladimirov" <mlists@arhont.com>, Arhont Lt
Vulnerable:	IEEE 802.1q Cisco IOS 11.2.8 SA5 Cisco Catalyst WS-C2924M-XL

IEEE 802.1q Unauthorized VLAN Traversal Weakness

The 802.1q standard is susceptible to issues that allow attackers to send and receive packets from one VLAN to another without authorization.

By spoofing various Ethernet frame fields such as the source or destination MAC addresses, IP addresses, and VLAN tags, attackers may cause packets to traverse from one VLAN to another, and possibly back again. Attackers may also add multiple VLAN tags to packets to cause multiple routers to decapsulate the packets in unexpected ways, aiding the attacker in traversing VLANs.

This issue allows attackers to traverse from one VLAN to another in an unauthorized fashion. As some users may utilize VLANs to segregate network segments containing differing security properties, this may have various consequences.

This issue may be exacerbated by utilizing attacker-controlled external network hosts to bounce packets between VLANs.

IEEE 802.1q Unauthorized VLAN Traversal Weakness

- September 1999 (12 years ago)
- Steve Schupp, Dave Taylor
- Further research by Andrew Vladimirov
- CVE-1999-1129 (BID: 615)
- Cisco PSIRT responded
  - Acknowledges vulnerability
  - Recommended Cisco Security Best Practices
    - Disable trunk ports that shouldn't be in use

Other Researchers

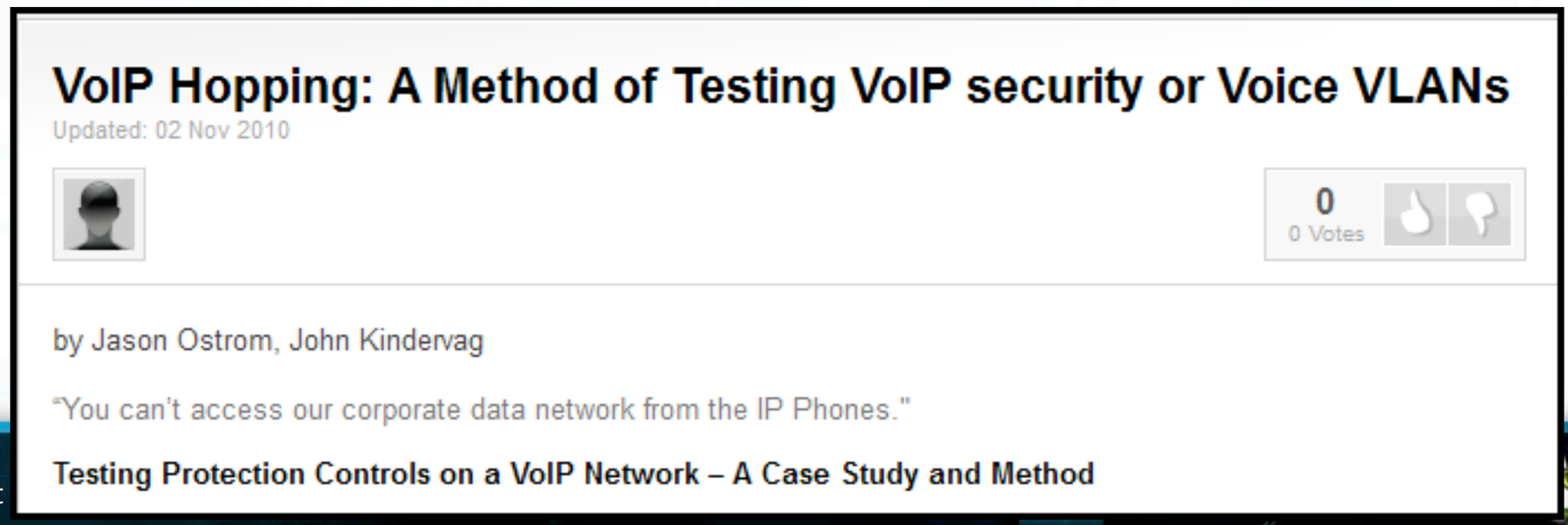
- @Stake Report: "Secure use of VLANS"
  - August 2002
  - Mike Schiffman, David Pollino
- Black Hat USA: "Hacking Layer 2: Fun with Ethernet Switches"
  - 2002
  - Sean Convery, Cisco Systems
- Cisco White Paper: VLAN Security WP
  - "Virtual LAN Security Best Practices"

Other Researchers

- SANS Resources
  - "Intrusion Detection FAQ: Are there vulnerabilities in VLAN Implementations?"
    - David Taylor (July, 2000)
  - "Virtual LAN Security: weaknesses and countermeasures"
    - Steve A. Rouiller
  - "VLAN Security in the LAN and MAN Environment"
    - Chris Hoffmann (April, 2003)

VoIP Hopping

- Definition
  - Unauthorized VLAN access within a VoIP infrastructure, that was not intended by the system design
- Business Risk increases in areas with:
  - Inherent right to privacy (hotel guest rooms)
  - Poor physical security (public access)



VoIP Hopping: A Method of Testing VoIP security or Voice VLANs

Updated: 02 Nov 2010

0
0 Votes

by Jason Ostrom, John Kindervag

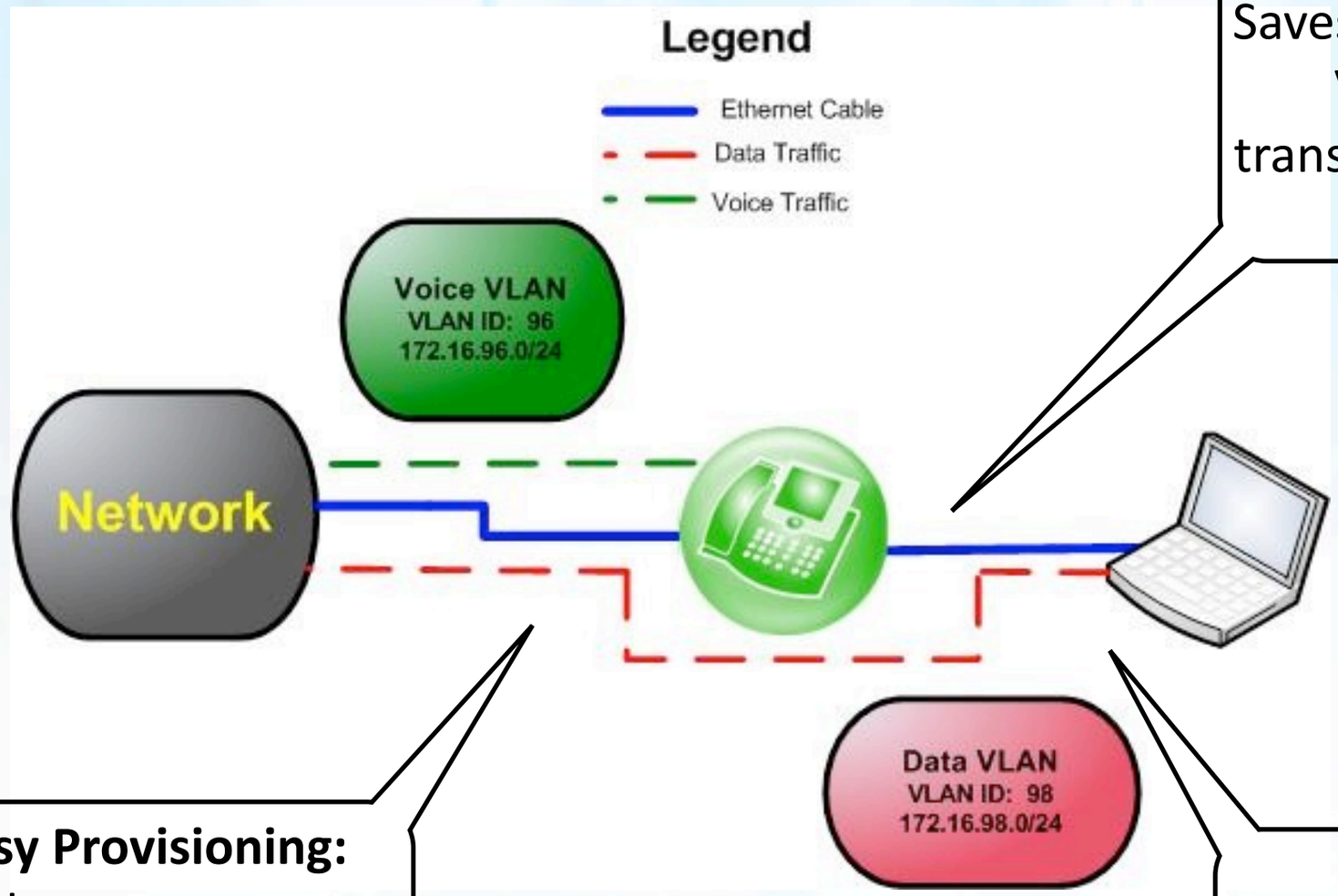
"You can't access our corporate data network from the IP Phones."

Testing Protection Controls on a VoIP Network – A Case Study and Method

VoIP Hopping

- All Best Practices recommend disabling trunk ports for user access networks
- With VoIP to work, some form of trunk ports (usually) must be used
  - Trunk ports in traditional sense
  - Multi-access VLANS with auxiliary ports
    - The Cisco “Voice VLAN”

Overview



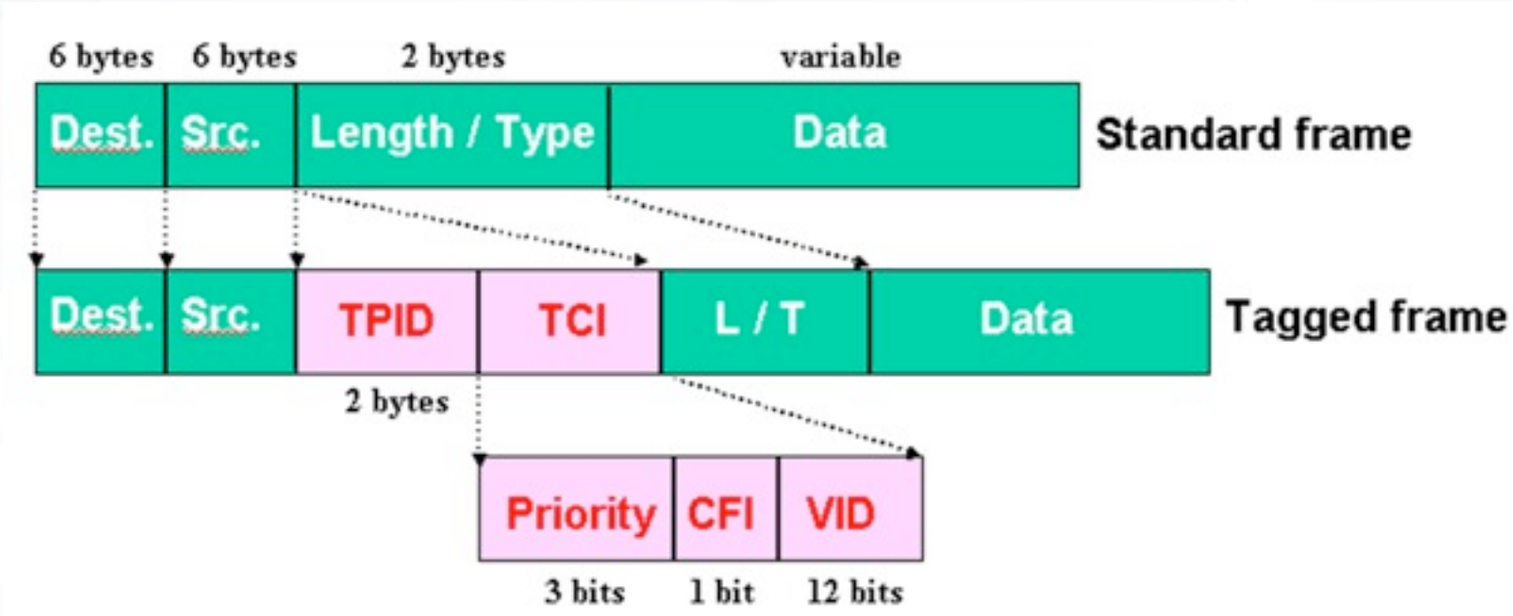
Benefit of VoIP:
Saves on Cabling Costs: VoIP and Data transmitted over single cable

Easy Provisioning:
IP Phones can auto-discover and provision into the VoIP network

Easy QoS:
QoS can ensure that VoIP and Video traffic has highest priority through network

802.1q Frame Tagging Attack: Step 1

- Learn the VLAN ID
  - Need to learn the VLAN ID to tag traffic, or the ethernet frames will be dropped
  - Usually this is the Voice VLAN ID (VVID)
- Can be learned through CDP, LLDP-MED, DHCP



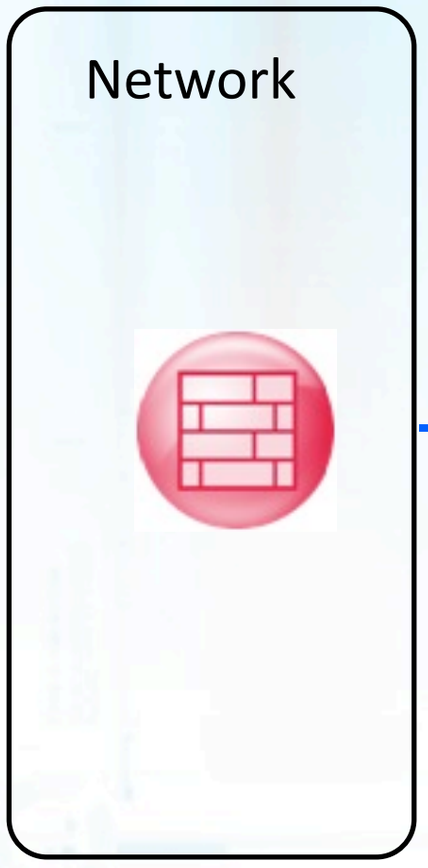
802.1q Frame Tagging Attack: Step 2

- Spoof tagged ethernet frames
  - Spoof ethernet frames with VLAN ID learned in Step #1
  - Trivial to do, using special software on your PC
  - Create a virtual interface (eth0.xxx)
  - Send DHCP with eth0.xxx (& tag subsequent frames)

```
bt voiphopper # ifconfig
eth0      Link encap:Ethernet  HWaddr 00:12:3F:0F:33:F3
          inet addr:172.16.100.3  Bcast:172.16.100.255  Mask:255.255.255.0
          inet6 addr: fe80::212:3fff:fe0f:33f3/64 Scope:Link
          UP BROADCAST NOTRAILERS RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:749 errors:0 dropped:0 overruns:0 frame:0
          TX packets:401 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:76441 (74.6 KiB)  TX bytes:54121 (52.8 KiB)
          Interrupt:11

eth0.200  Link encap:Ethernet  HWaddr 00:12:3F:0F:33:F3
          inet addr:172.16.200.3  Bcast:172.16.200.255  Mask:255.255.255.0
          inet6 addr: fe80::212:3fff:fe0f:33f3/64 Scope:Link
          UP BROADCAST NOTRAILERS RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:3 errors:0 dropped:0 overruns:0 frame:0
          TX packets:10 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:984 (984.0 b)  TX bytes:2298 (2.2 KiB)
```

Overview



Legend

- Ethernet cable
- VoIP network traffic
- Data network traffic

Networks

VoIP VLAN: VLAN_200
IP Subnet: 172.16.200.0/24

Guest Data VLAN: VLAN_100
IP Subnet: 172.16.100.0/24

Call Control Servers VLAN_67

172.16.67.0/24

Overview

Network

Legend

- Ethernet cable
- VoIP network traffic
- Data network traffic

Networks

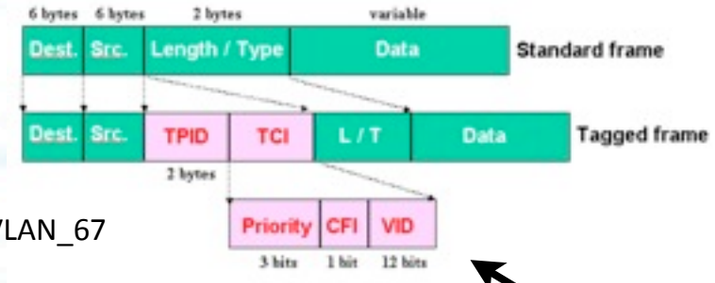
VoIP VLAN: VLAN_200
IP Subnet: 172.16.200.0/24

Guest Data VLAN: VLAN_100
IP Subnet: 172.16.100.0/24

Learn VLAN ID: 200

eth0.200

Create eth0.200 Voice interface



Call Control Servers

VLAN_67

172.16.67.0/24

Tag with VID: 200

VoIP Hopping

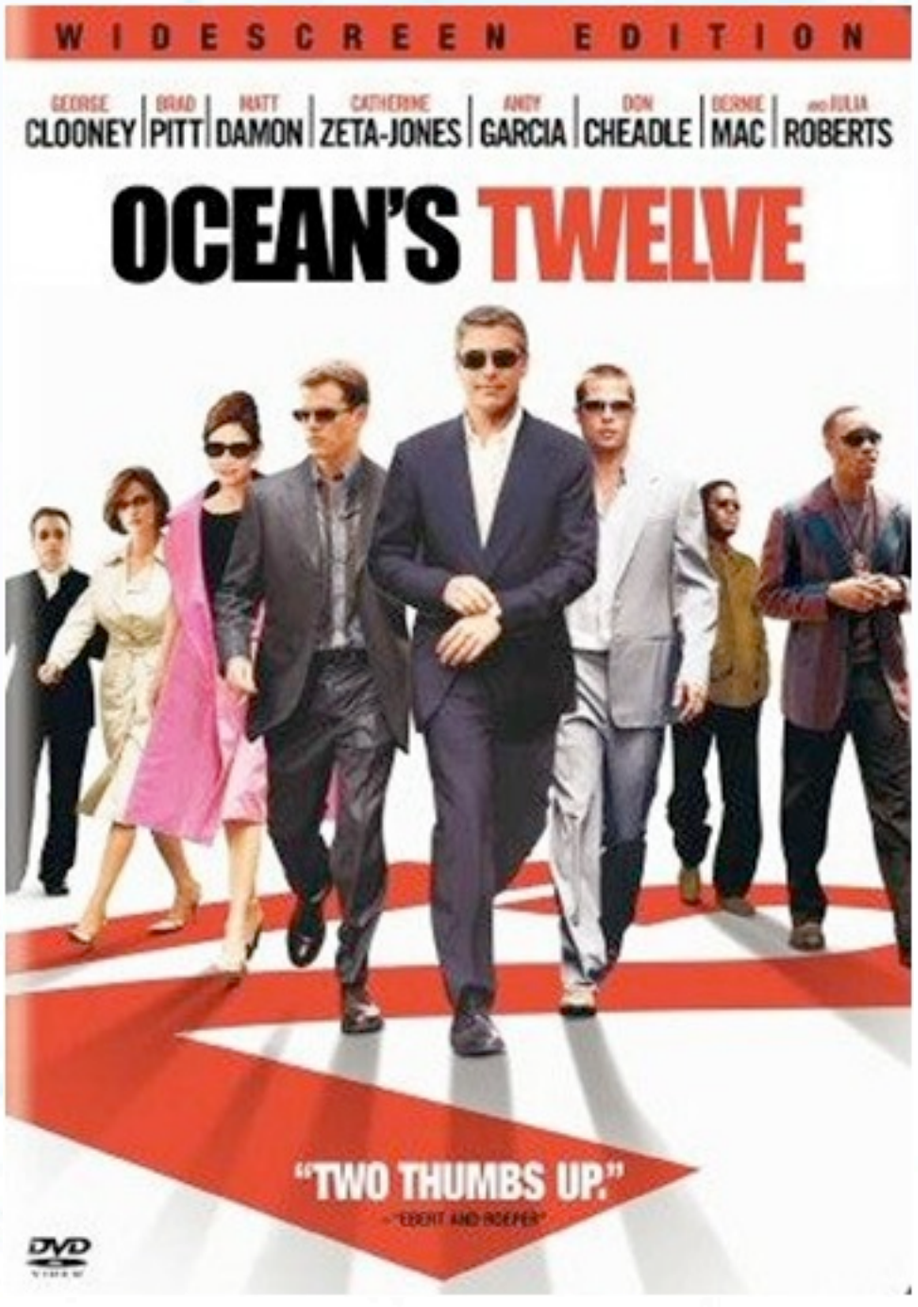
- How to reconcile this security problem
  - Current best practices recommend disabling trunk ports in user access networks
  - Yet, VoIP configuration requires 802.1q trunking in these user access networks

> Additional Information
> ==========
>
> Cisco is aware of VLAN spoofing attacks and recommends that customers apply best practices where possible to reduce the impact of such attacks on their networks. Many best practices are discussed in Cisco's SAFE Blueprint for Layer 2 security:

Best Practices need to be updated to include security configuration in UC networks with Voice VLANS and/or Trunk port requirements for QoS

> The recommended configuration is to disable 802.1q trunking everywhere it is not required so that tagged frames are discarded on ports not configured for trunking.

Case Study: Hotel Vulnerability



Credit: Michelle Ahmadian

Case Study: My Story of a Hotel

- Story Intro
  - Sitting in a luxury hotel with IP Phones in guest rooms
- Summary of Configuration
  - What security controls were in place
  - Detailed description of methods and how they can be defeated

Observation 1: MAC Address Hiding

- MAC Address label removed from IP Phone
  - Increasingly common knowledge that MAC Address spoofing defeats Port Security (MAC Address filtering)
  - Infers that they knew about this
  - Infers that they were trying to prevent VLAN Hop and MAC Address spoofing by removing ability of attacker to use MAC address of IP Phone
  - This infers that Port Security could have also been enabled
    - Why else would they hide the MAC Address of IP Phone?

Observation 2: DHCP Disabled

- DHCP was disabled
  - Sending a tagged DHCP request was ineffective
  - You would have to configure a static IP address
  - Defeats casual or unsophisticated attackers
- How to know the right IP address to use?

Issue #1: Trunk ports leaking VLAN ID

- Plugged laptop with sniffer directly into wall port
- Passively observed ~ sniffed tagged ethernet frames
  - Observed ARP traffic from IP Phones
  - 802.1q tagged ARP frames contained VLAN ID
  - Now we have the VLAN ID (for spoofing 802.1q!)
- Trunk ports mis-configured, or shouldn't be used at all?

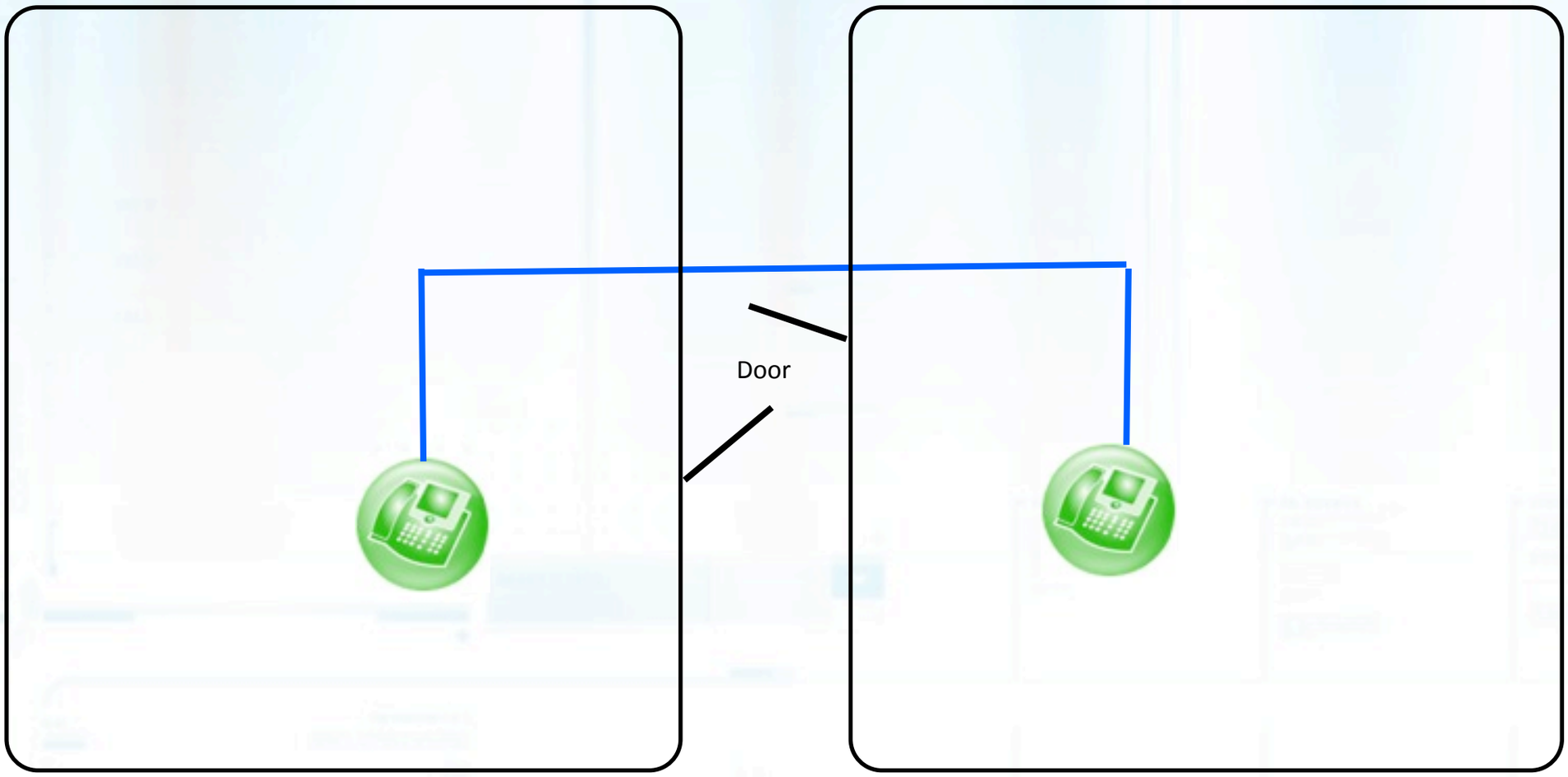
Issue #2: Control two IP Phones in adjoining guest rooms

- I can check into two adjoining guest rooms
  - Coordinated, physical attack with multiple colluders
  - Physical control of at least two IP Phones
- Method
  - Room 1: Replace IP phone with sniffing laptop
  - Room 2: Reboot IP Phone multiple times
  - Room 1: Sniff and verify MAC address and static IP address of phone in room 1 (rebooted multiple times)
  - Room 1: Plug IP Phone back into wall port

Issue #2: Control two IP Phones in adjoining guest rooms

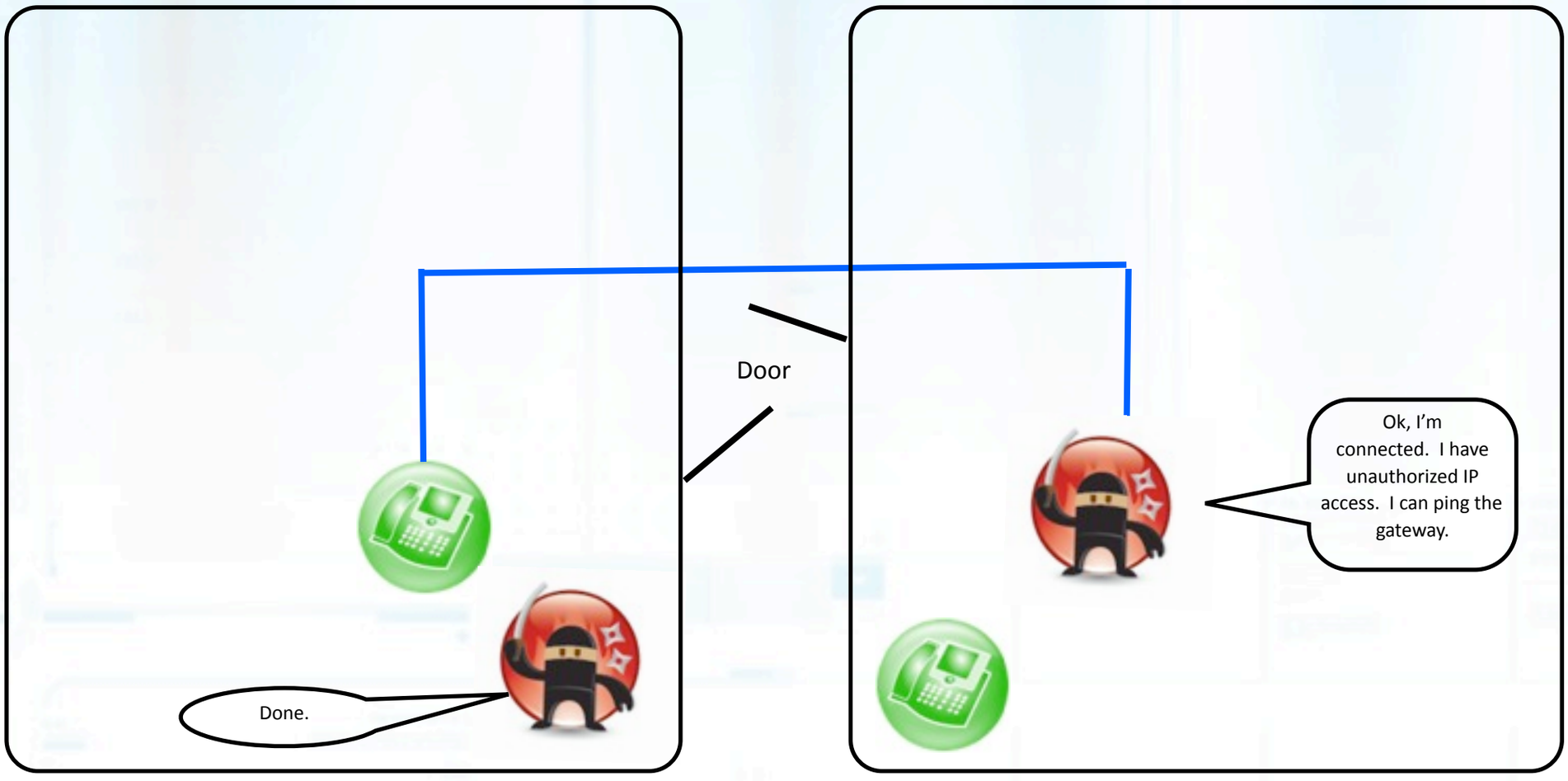
- Method (Continued)
  - Room 2: Move sniffing laptop into Room 2
  - Room 2: Unplug IP Phone
  - Room 2: Offline, manually spoof MAC address, create virtual interface, configure static IP address
  - Room 2: Connect laptop to wall port
  - Room 2: Ping IP Gateway
    - If successful, unauthorized IP network access

Overview



Overview

Keeping in mind
-Phones in adjoining rooms are normally going to be members of the same VLAN (broadcast domain)
-All ethernet broadcasts (ARP) are forwarded out all ethernet switch ports of broadcast domain hosts
-In hotels normally all phones on same floor are terminated into same switch closet
-There is a high degree of probability that phones in adjoining rooms are in the same VLAN



VoIP Hopper 2.0 Release

VoIP Hopper 2.0 will be released soon!

- Summary of new features
  - Assessment Mode
  - Interactive, CLI
  - LLDP-MED support (spoof, sniff)
  - ARP and 802.1q dissector
  - Automatically learns IP and MAC of phones
  - Automatic VLAN Hop based on first learned VVID (CDP, LLDP-MED, ARP)
  - Can set IP and MAC statically from learned phones when DHCP is disabled
  - Fixed many issues with integrated DHCP code

VoIP Hopper 2.0 Release

- New Assessment mode
  - CLI interface
  - Pass individual commands, easily creating new features

```
VoIP Hopper assessment mode ~ Select 'q' to quit and 'h' for help menu.
Main Sniffer:  capturing packets on eth0
h
Please select from one of the following options:
************************************************
a   <------>   Toggle recording ARP packets on default interface ~ (Disabled by default)
b   <------>   Toggle recording ARP packets on new VoIP VLAN interface ~ (Enabled by default)
c   <------>   Spoof 1 CDP packet ~ Quickly discover VVID
d   <------>   Toggle CDP packet analysis ~ (Enabled by default)
f   <------>   Toggle 802.1q analysis ~ (Enabled by default)
h   <------>   Print help menu
i   <------>   Toggle automatic VLAN Hop ~ (Enabled by default)
l   <------>   Toggle analysis of LLDP-MED ~ (Enabled by default)
m   <------>   Spoof 1 LLDP-MED packet ~ Quickly learn VVID
q   <------>   Safely quit VoIP Hopper
s   <------>   Spoof my IP and MAC address
v   <------>   Toggle verbose mode on and off
z   <------>   About VoIP Hopper
************************************************
```

VoIP Hopper 2.0 Release

- LLDP-MED spoofing support
  - Shows spoofing LLDP-MED in assessment mode

```
File  Edit  View  Search  Terminal  Help
root@      ·laptop:/home/viper/Desktop/voiphopper-demo#
root@      ·laptop:/home/viper/Desktop/voiphopper-demo#
root@      ·laptop:/home/viper/Desktop/voiphopper-demo#
root@      ·laptop:/home/viper/Desktop/voiphopper-demo# voiphopper -i eth0 -z
VoIP Hopper assessment mode ~ Select 'q' to quit and 'h' for help menu.
Main Sniffer:  capturing packets on eth0
m
Made LLDP packet of 270 bytes - Sent LLDP packet of 270 bytes
Discovered VoIP VLAN through LLDP-MED: 200
dhcpTimedOut():  VoIP dhcp client:  Elapsed time is 0 (Time out is 20).
dhcpTimedOut():  VoIP dhcp client:  Elapsed time is 2 (Time out is 20).
VoIP Hopper dhcp client:  received IP address for eth0.200: 172.16.200.7
Decoded VLAN ID through 802.1q VLAN Header:  200
Capturing ARP packets on eth0.200
New host #1 learned on eth0.200: (MAC): 00:1e:f7:28:9c:8e      (IP): 172.16.200.10
```

VoIP Hopper 2.0 Release

- Automatically VLAN Hops based on first discovered VVID
  - New support for decoding 802.1q tagged ARP traffic
  - In the screen shot, automatic VLAN Hop is disabled
  - The first protocol method discovery (CDP, LLDP-MED, ARP) is used

```
i
Disabling automatic VLAN Hop
Discovered VoIP VLAN through LLDP-MED: 200
Decoded VLAN ID through 802.1q VLAN Header:  200
Discovered VoIP VLAN through CDP: 200
```

VoIP Hopper 2.0 Release

- Passive ARP sniffer automatically launches after VLAN Hop
- Silently logs / records Phone MAC and IP from ARP traffic
- Logs the phones to a text file, voip-hosts.txt

```
VoIP Hopper dhcp client:  received IP address for eth0.200: 172.16.200.7
Capturing ARP packets on eth0.200
New host #1 learned on eth0.200: (MAC): 00:19:e8:af:a9:47       (IP): 172.16.200.2
New host #2 learned on eth0.200: (MAC): e8:40:40:a5:73:c2       (IP): 172.16.200.1
Discovered VoIP VLAN through CDP: 200
New host #3 learned on eth0.200: (MAC): 00:1e:f7:28:9c:8e       (IP): 172.16.200.10
New host #4 learned on eth0.200: (MAC): 64:16:8d:51:13:6c       (IP): 172.16.200.11
New host #5 learned on eth0.200: (MAC): 64:16:8d:51:10:ac       (IP): 172.16.200.12
```

```
root@              :/home/viper/Desktop/voiphopper-demo# cat voip-hosts.txt
00:19:e8:af:a9:47,172.16.200.2
e8:40:40:a5:73:c2,172.16.200.1
00:1e:f7:28:9c:8e,172.16.200.10
64:16:8d:51:13:6c,172.16.200.11
64:16:8d:51:10:ac,172.16.200.12
root@              :/home/viper/Desktop/voiphopper-demo#
```

VoIP Hopper 2.0 Release

- If DHCP is disabled, VoIP Hopper automatically sets a static IP address (after DHCP timeout)
- Also, starts sniffing and recording IP Phones via ARP

```
dhcpTimedOut():  VoIP dhcp client:  Elapsed time is 0 (Time out is 20).
dhcpTimedOut():  VoIP dhcp client:  Elapsed time is 4 (Time out is 20).
dhcpTimedOut():  VoIP dhcp client:  Elapsed time is 12 (Time out is 20).
dhcpTimedOut():  VoIP dhcp client:  Elapsed time is 28 (Time out is 20).  We have timed out
VoIP Hopper dhcp client has timed out after 28 seconds
IP address of 'eth0.200' set to '9.9.9.9'
Capturing ARP packets on eth0.200
```

VoIP Hopper 2.0 Release

- An attacker can then spoof a previously learned Phone's IP and MAC address, from a menu

```
s
Spoof IP and MAC address ~ Become an IP Phone
(1)     IP:   172.16.200.2,     MAC:   00:19:e8:af:a9:47
(2)     IP:   172.16.200.1,     MAC:   e8:40:40:a5:73:c2

Select an IP Phone index (1 - 2) to spoof the MAC and IP Address of, 'q' to Quit, or 'r' to repeat Phone list
1
IP address of 'eth0.200' set to '172.16.200.2'
eth0.200 Current MAC:  00:1e:c9:05:da:3c
eth0.200 Faked MAC:    00:19:e8:af:a9:47
```

VoIP Hopper 2.0 Release

- Automatically learns and records all IP Phone endpoints that support LLDP-MED
- Saves endpoints to a text file, 'myass.txt'
- Useful feature from a previous VoIP Pentest

```
root@                /home/viper/Desktop/voiphopper-demo# cat myass.txt
Discovered new LLDP-MED endpoint (# 1)
System Name:  SEP64168D5110AC.viperlab.net
System Description:  Cisco IP Phone 9971, V1, sip9971.9-0-2
IP Address:  172.16.200.3
Discovered new LLDP-MED endpoint (# 2)
System Name:  SEP64168D51136C.viperlab.net
System Description:  Cisco IP Phone 9971, V1, sip9971.9-0-2
IP Address:  172.16.200.4
Discovered new LLDP-MED endpoint (# 3)
System Name:  SEP001EF7289C8E.cisco.com
System Description:  Cisco IP Phone CP-7971G-GE,V3, SCCP70.8-3-3SR2S
IP Address:  172.16.200.5
Discovered new LLDP-MED endpoint (# 4)
System Name:  SEP0019E8AFA947.cisco.com
System Description:  Cisco IP Phone CP-7931G,V, SCCP31.8-3-3SR2S
IP Address:  172.16.200.2
root@          .  . /home/viper/Desktop/voiphopper-demo#
```

Live Demo: VoIP Hopper

Thanks to Tom Mostyn, for low level debugging help

```
// Now start ARP Sniffer on new VoIP interface
// Create new thread
pthread_t new_arp_threads;
int rc;
int arg;
rc = pthread_create(&new_arp_threads,NULL,sniff_arp_new,(void *)arg);
if(rc) {
        printf("Error:  pthread_create error %d\n",rc);
        exit(-1);
}
```

Live Demo: VoIP Hopper vs. Hotel

VoIP Hopper

vs

The Hotel

Summary

- What happens when you physically control two or more IP Phones?
  - Are people really thinking about this?
  - A potential coordinated attack from trusted ports
  - Key Assumptions
    - Phones members of same VLAN, broadcast domain
    - An ethernet broadcast (ARP) will forward to all broadcast domain member switch ports
    - Hotels usually would terminate all IP Phones into same wiring closet on a given floor
    - Very likely that phones in adjoining rooms are in same VLAN

Using the IP Phone reboot as a tool or method to learn information about the network.

802.1q tagged ARP traffic is another way of learning the VLAN ID. We don't absolutely need CDP, DHCP, or LLDP.

Summary

- The point is that for VoIP, QoS, and "convergence" to work, you (usually) need both VLANs allowed
  - Risk of VLAN Hop known for a long time
  - This is about the risk of VLAN Hop in environments that require trunk ports in user access networks

Summary

- Impact in this Case Study
  - Unauthorized IP network access to VoIP network
    - Enables UC specific attacks against VoIP network
    - Could allow access to corporate data (servers)
    - Could represent critical business impact
    - Attacker sitting in privacy of guest room could spend all the time he or she desires penetrating further
- These Hotels deploying UC in guest rooms should be aware and apply required security controls

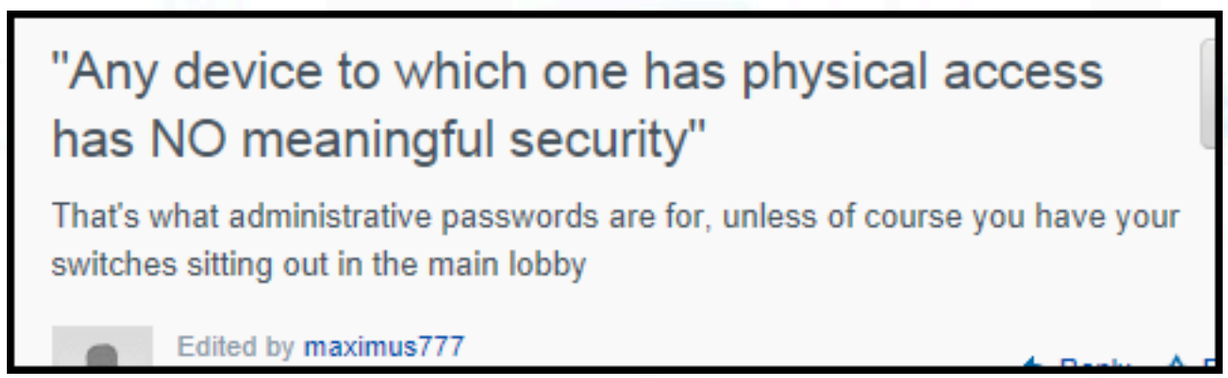
Mitigation covered at end of slides

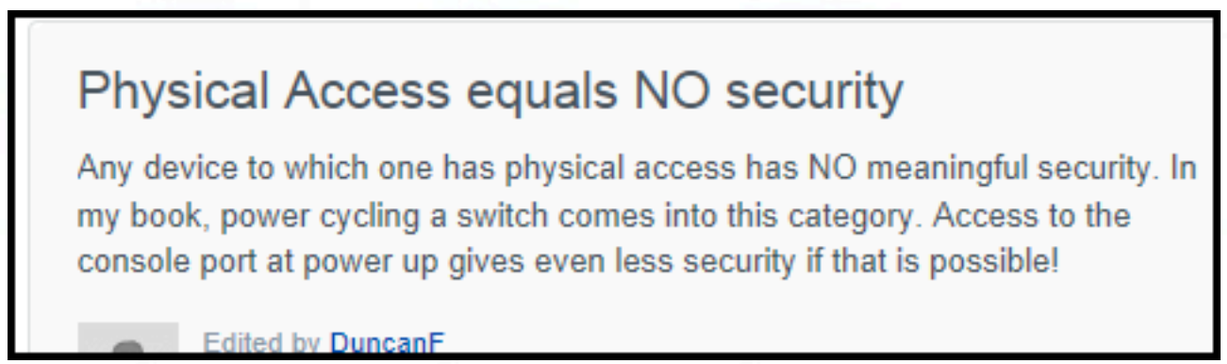
Summary

- Authorized VoIP Pentest in 2007
  - Gained unauthorized access to Hotel's servers through IP Phone in hotel guest room
  - Potential back door into internal systems could represent critical impact to business in hospitality industries
  - Businesses deploying UC to private areas must understand the risk ~ it can be properly mitigated
  - Could represent another method of data breach (credit card data)

Summary

- Physical Security is compromised here
  - It's a unique situation for hotel rooms
  - Guests have right to privacy
  - Security controls need to compensate for this
  - Solutions such as 802.1x provide equivalent physical security





Valcros and Percipia

VALCROS, INC. SELECTED TO PROVIDE VOICE, DATA AND VIDEO NETWORK FOR HI-TECH HOTEL

VALCROS, INC. SELECTED TO PROVIDE VOICE, DATA AND VIDEO NETWORK FOR HI-TECH HOTEL

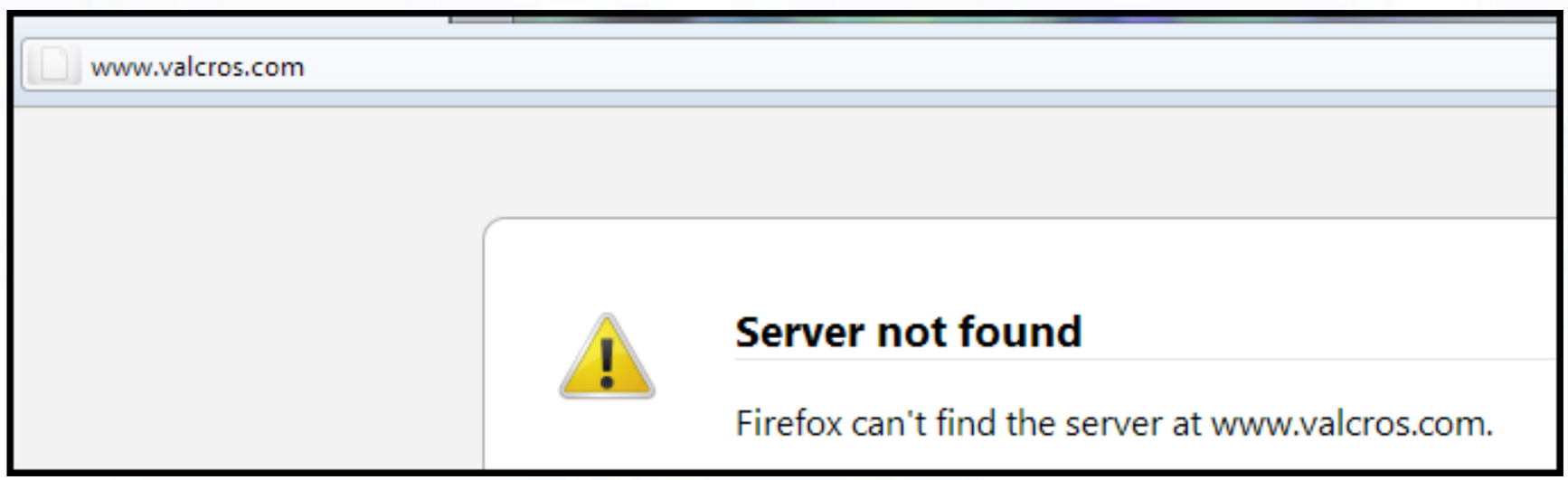
Cutting Edge Technology for Superior Customer Service

SAN DIEGO, May 9, 2006 – Hotel 1000 has chosen San Diego-based Valcros, Inc. to design and integrate its voice, data, and video network into a fully converged infrastructure for a unique condo hotel, opening in downtown Seattle June 26, 2006. This hotel features 120 guest rooms, a restaurant and bar, the Hotel 1000 Country Club and Spa (with virtual golf from the world's top courses), and a dog-walking park on the roof.

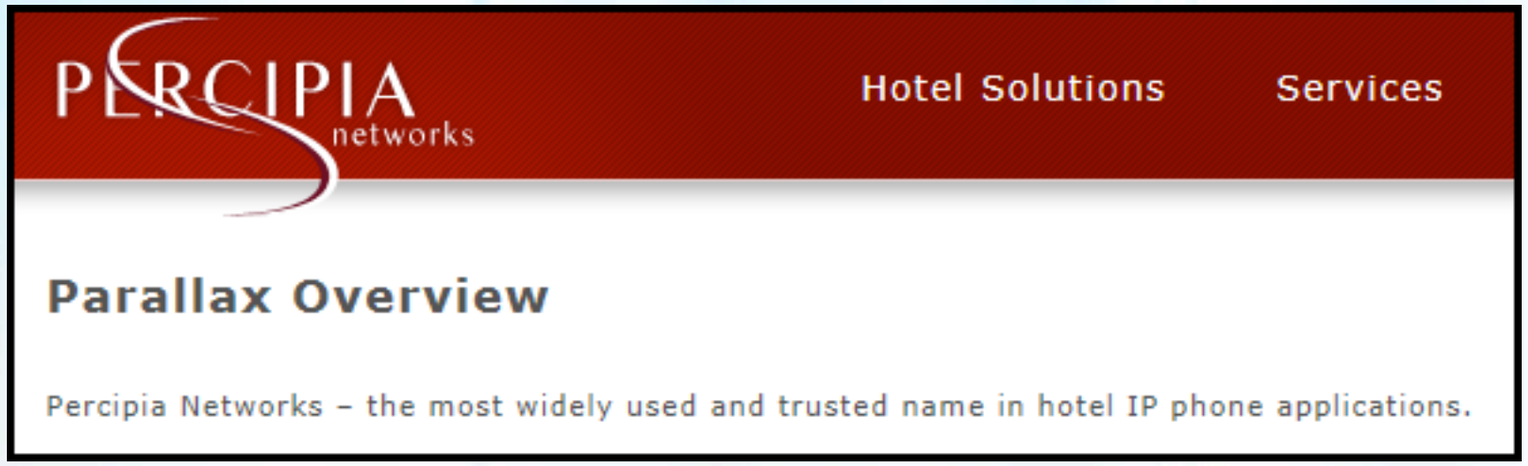
About Valcros

Since 1998, Valcros has provided consultation, design, and implementation of converged voi
data networks and applications. Recently awarded by Cisco for "Best in Engineering" for the
region, Valcros strives to provide customers with easy-to-deploy, easy-to-use, and easy-to-m
that address their immediate and long-term business goals. Valcros is a partner of Cisco Sys
Cisco equipment to provide Voice, Video, and Data integrated networks to hospitality and co
businesses. Valcros also partners with Sony to deliver video conferencing and video surveilla
AT&T to provide telecom and transportation services. Headquartered in San Diego, Valcros
nationwide and internationally. You can find out more about Valcros at www.valcros.com.

I wanted to ask: how do you recommend best practices in these hotel infrastructures?



Valcros and Percipia



From: Jason Ostrom
Sent: Mon 7/11/2011 8:20 AM
To: info@percipianetworks.com
Cc: sales@percipianetworks.com
Subject: Inquiry: Hotel security solution in guest rooms

Hello,

I was wondering if Percipia has a solution / product / service that can help provide security in hotel guest rooms, when customers have deployed IP Phones in the guest rooms. Do you have a security solution that can help prevent unauthorized access from "hackers" breaking into the internal IP network of a Hotel guest room, by unplugging the phone and plugging in their laptop? I would be very interested to know more about your solution that can mitigate this real threat to hotel networks.

Thank you!

No response

Hotel Survey

- Idea to conduct a survey of hotels
  - Objective:
    - To find percentage of hotels using VoIP and price, from a sampling of 100 luxury hotels
    - To record calls and see how the reservation specialist answers questions of IP Phones in guest rooms
  - Used research assistant, recorded all phone calls
  - Hotels included 20% international and 80% US
    - Included Paris, London, NYC, Tokyo, Monte Carlo
    - Most US were Las Vegas and other casino resort hotels

Hotel Survey

- Script
  - "My boss has a strong preference for hotels with VoIP, as he really likes the service and convenience of these IP Phones"
  - Interesting from a social engineering aspect
  - If an attacker wanted to find potential VoIP Hopping targets
- Result
  - Of 100 luxury hotels, 8 out of 100 (8%) confirmed to have IP phones in guest rooms
  - Average room price per night: $655.32 USD

Hotel Survey

- Sample audio clip 1
  - For hotels that do, reservation specialist doesn't know what VoIP is and has to check
  - "Ooohhh....not quite sure if our phones do that"

Hotel Survey

- Sample audio clip 2
  - She checked with her IT Director and they do have IP Phones

Voice VLANs as Trunk Ports

- Went back through all internal VoIP Pentests, researched packet captures from Voice VLAN port
- In 6 customer cases, tagged frames revealed:
  - 5 deployments revealed VVID through ARP to switch access ports
  - 1 deployment didn't tag ARP packets
- Summary
  - Cisco Voice VLANs appear to behave as trunk ports
  - Advertise VVID to access ports through 802.1q tagged ARP

Voice VLANs as Trunk Ports

- Sent notification to Cisco PSIRT

```
Cat3560G-4#sh int gigabitEthernet 0/1 switchport
Name: Gi0/1
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 100 (VLAN0100)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: 200 (VLAN0200)
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
```

From: Jason Ostrom
To: 'psirt@cisco.com'
Cc: [redacted]
Subject: Cisco IOS advertises VVID by sending tagged frames to switch access ports

* PGP Signed: 7/10/2011 at 12:33:35 PM

Cisco PSIRT,

We recently discovered a generic information disclosure vulnerability, in both
DEFCON 19 conference [1], in a vendor agnostic way (not discussing any partic
educate Cisco customers, or a true vulnerability in Cisco IOS, then we urge a jo
back. Thank you.

OVERVIEW
Cisco IOS Ethernet switches advertise the Voice VLAN ID through tagged Ethe
the Voice VLAN ID through tagged ARP packets received on switch access por
VLAN ID in ARP and other miscellaneous network traffic. It was also our unde

IMPACT
Disclosure of Voice VLAN ID, which can lead to unauthorized access through V

Voice VLANs as Trunk Ports

http://cciepursuit.wordpress.com/2009/01/01/group-study-good-explanation-of-the-voice-vlan/

The official Cisco stance is that this is not a trunk:

> Cisco calls this a Multi-Vlan access port, and NOT a trunk port. if it were a trunk port, according to Cisco, it would flood all vlans configured on the switch out to the phone. As you probably know already, a port configured for voice Vlan does not flood out all Vlans to the phone, just the voice vlan frames (tagged) and the data frames (untagged).
>
> *Multiservice switches supports a new parameter for IP Telephony support that makes **the access port a multi-VLAN access port**. The new parameter is called an auxiliary VLAN. Every Ethernet 10/100/1000 port in the switch is associated with two VLANs*
>
> *- **A Native VLAN for data service** that is identified by the port VLAN identifier or **PVID***
>
> *- **An Auxiliary VLAN for voice service** that is identified by the voice VLAN identified or **VVID**.*
>
> *- During the initial CDP exchange with the access switch, the IP phone is configured with a VVID.*
>
> *- The IP phone also supplied with a QoS configuration using Cisco Discovery Protocol. Voice traffic is separated from data, and supports a different trust boundary.*
>
> ***Data packets between the multiservice access switch and the PC or workstation will be on the native VLAN**. All packets going out on the native VLAN of a 802.1q port are sent untagged by the access switch. The PC or workstation connected to the IP phone usually sends untagged packets.*
>
> ***Voice packets will be tagged by the IP phone based on the Cisco Discovery Protocol information from the access switch**.*
>
> ***The multi-VLAN access ports are not trunk ports**, even though the hardware is set to dot1q trunk*. **The hardware setting is used to carry more than two VLANs, but the port is still considered an access port that is able to carry one native VLAN and the Auxiliary VLAN. The 'switchport host' command can be applied to a multi-VLAN access port on the access switch.***

If I understand this correctly, although the switchport is configured to use two different VLANs, only the voice VLAN traffic is actually tagged by the IP Phone. The data VLAN is sent untagged (making use of the native VLAN dot1q feature). This STILL sounds like trunking to me though. 😀 This gives me high school Physics flashbacks about photons ("Is it a wave or a particle?" "It's both...and neither." <head explodes>). Scott Morris agrees:

> That's a fancy name for a small trunk. I agree. **If you have tagged frames, it's a trunk.**
>
> If it has two wheels and pedals, it's a bicycle. They have some weird looking ones these days, but they're still bicycles. Call it a multi-unicycled transportation device if you want, but it's still a bicycle.

LLDP-MED

ether proto 0x88cc

```
Ethernet II, Src: ExtremeN_f9:ad:a0 (00:01:30:f9:ad:a0), Dst: LLDP_Multicast (01:80:c2:00:00:0e)
  Destination: LLDP_Multicast (01:80:c2:00:00:0e)
  Source: ExtremeN_f9:ad:a0 (00:01:30:f9:ad:a0)
  Type: 802.1 Link Layer Discovery Protocol (LLDP) (0x88cc)
Link Layer Discovery Protocol
  Chassis Subtype = MAC address
  Port Subtype = Interface name
  Time To Live = 120 sec
  Port Description = Summit300-48-Port 1001
  System Name = Summit300-48
  System Description = Summit300-48 - Version 7.4e.1 (Build 5) by Release_Master 05/27/05 04:53:11
  Capabilities
  Management Address
  IEEE 802.3 - Power Via MDI
  IEEE 802.3 - MAC/PHY Configuration/Status
  IEEE 802.3 - Link Aggregation
  IEEE 802.3 - Maximum Frame Size
  IEEE 802.1 - Port VLAN ID
  IEEE 802.1 - Port and Protocol VLAN ID
  IEEE 802.1 - VLAN Name
  IEEE 802.1 - Protocol Identity
  End of LLDPDU
```

Intro to LLDP-MED

- LLDP
  - Link Layer Discovery Protocol ~ 802.1A
  - New standardized Discovery Protocol
  - IEEE multi-vendor support ~ provides standards-based discovery for vendor interop (May 2005)
- LLDP-MED
  - Link Layer Discovery Protocol - Media Endpoint Discovery
  - An extension to LLDP to address voice applications

Intro to LLDP-MED

- Uses TLV messages to communicate to neighboring devices
  - Very similar to CDP, IP Phones can learn VoIP VLAN and negotiate power with PoE Switch (but it's IEEE multi-vendor interop!)
- Summarized features
  - Inventory control (Serial number, model numbers, firmware)
  - Network Topology with an NMS (Aid in troubleshooting)
  - Power Negotiation and priority
  - Network Policy Discovery (VoIP VLAN)
  - Capabilities Discovery
  - Automatic Location Identification (E911)
    - Media endpoint location in emergency situations

e911 Emergency Services

- Corporations challenged by obligation to support Emergency Calling Services (ECS) that include E911
  - Difficult due to lack of standards
  - LLDP-MED provides e911 in enterprises
  - When an endpoint receives a TLV with ECS location data, stores it and can communicate with public safety answering point
  - Appears more useful for telling IP Phone its location

e911 Emergency Services

- Location information
  - Normally sent from switch to phone
  - For phones that can't determine their own location
  - Can be useful for location based applications on phone
- Scenarios where an IP Phone needs to send its location information to switch
  - Any security risk
  - Spoofing LLDP-MED messages

Comparison: LLDP-MED vs CDP

	LLDP-MED	CDP
Spoofing	Cisco IOS switch accepts spoofed LLDP. Can spoof capabilities, fill LLDP table.	Cisco IOS switch accepts spoofed CDP.
Sniffing	Can sniff LLDP advertisements, but by default don't receive Network Policy (VVID) TLV	Can easily sniff CDP and learn VVVID by default
802.1x Bypass	Spoofing LLDP doesn't bypass 802.1x. LLDP messages can't be prior to 802.1x port up.	Spoofing CDP can bypass 802.1x with Voice VLANs. Can be mitigated with 802.1x.
Automatically learning VVID	LLDP-MED must be spoofed. Harder.	Spoofed or sniffed. Easier.

Case Study: Pentest with LLDP-MED

- Plugged into Ethernet port
  - Received LLDP-MED multicast messages from other IP Phones on VLAN

Filter: lldp — Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Length	Info
1019	135.159301	Cisco_6c:2d:8e	LLDP_Multicast	LLDP	326	Chassis Id = [redacted] Port Id = 001E136C2D8E:P1 TTL = 180 System Name = SEP0
1048	139.293380	Cisco_0b:de:01	LLDP_Multicast	LLDP	326	Chassis Id = [redacted] Port Id = 001E4A0BDE01:P1 TTL = 180 System Name = SEP0
1053	139.671774	Cisco_6c:30:92	LLDP_Multicast	LLDP	326	Chassis Id = [redacted] Port Id = 001E136C3092:P1 TTL = 180 System Name = SEP0
1055	140.032799	Cisco_af:fa:6b	LLDP_Multicast	LLDP	326	Chassis Id = [redacted] Port Id = 001E13AFFA6B:P1 TTL = 180 System Name = SEP0
1058	141.175508	Cisco_0c:4c:4e	LLDP_Multicast	LLDP	326	Chassis Id = [redacted] Port Id = 001E4A0C4C4E:P1 TTL = 180 System Name = SEP0
1079	143.827798	Cisco_af:f1:da	LLDP_Multicast	LLDP	326	Chassis Id = [redacted] Port Id = 001E13AFF1DA:P1 TTL = 180 System Name = SEP00
1094	145.336899	Cisco_b0:00:09	LLDP_Multicast	LLDP	326	Chassis Id = [redacted] Port Id = 001E13B00009:P1 TTL = 180 System Name = SEP0
1118	148.598159	Cisco_56:e8:a4	LLDP_Multicast	LLDP	326	Chassis Id = [redacted] Port Id = 00070E56E8A4:P1 TTL = 180 System Name = SEP0
1122	149.005687	Cisco_0c:43:e5	LLDP_Multicast	LLDP	326	Chassis Id = [redacted] Port Id = 001E4A0C43E5:P1 TTL = 180 System Name = SEP0
1126	149.587599	Cisco_a8:3c:39	LLDP_Multicast	LLDP	316	Chassis Id = [redacted] Port Id = 0018B9A83C39:P1 TTL = 180 System Name = SEP0
1129	149.723511	Cisco_0b:e1:2e	LLDP_Multicast	LLDP	326	Chassis Id = [redacted] Port Id = 001E4A0BE12E:P1 TTL = 180 System Name = SEP0
1131	149.828075	Cisco_5d:14:2d	LLDP_Multicast	LLDP	326	Chassis Id = [redacted] Port Id = 001E135D142D:P1 TTL = 180 System Name = SEP0
1133	150.020025	Cisco_6c:26:ed	LLDP_Multicast	LLDP	326	Chassis Id = [redacted] Port Id = 001E136C26ED:P1 TTL = 180 System Name = SEP0
1145	151.523618	Cisco_8c:52:f2	LLDP_Multicast	LLDP	326	Chassis Id = [redacted] Port Id = 001E138C52F2:P1 TTL = 180 System Name = SEP0
1152	151.841112	Cisco_8d:0f:81	LLDP_Multicast	LLDP	326	Chassis Id = [redacted] Port Id = 001E138D0F81:P1 TTL = 180 System Name = SEP0
1153	151.884078	Cisco_af:ea:bc	LLDP_Multicast	LLDP	326	Chassis Id = [redacted] Port Id = 001E13AFEABC:P1 TTL = 180 System Name = SEP0

Mitigations

- Voice 1: VoIP is totally insecure! Be scared!
- Voice 2: Don't worry, VoIP is safe, you don't have to do anything! It's secure out of the box!
- Truth rests somewhere in between
  - As any TCP/IP client/server application, VoIP can most definitely be properly secured to match your environment's security requirements
  - It should be

Mitigations: Don't do this

- Port Security
- MAC Address filtering

Port Security

Table Of Contents

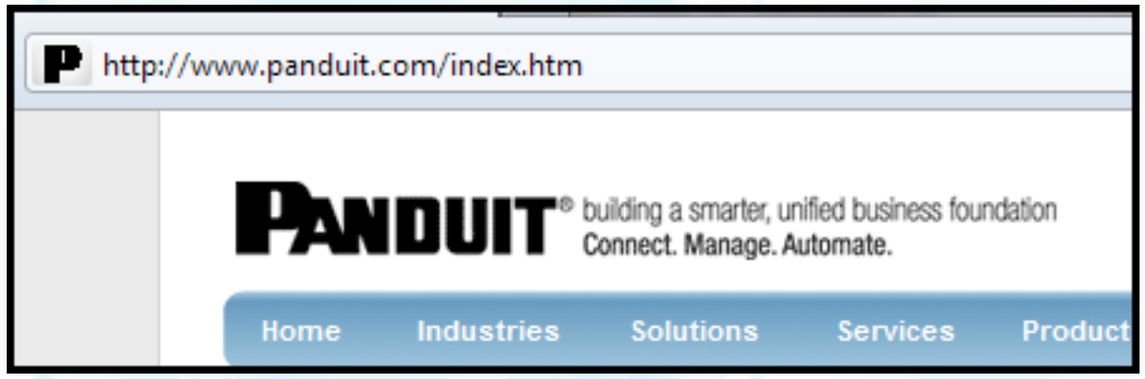
Configuring Port Security

This chapter describes how to configure the port security feature.

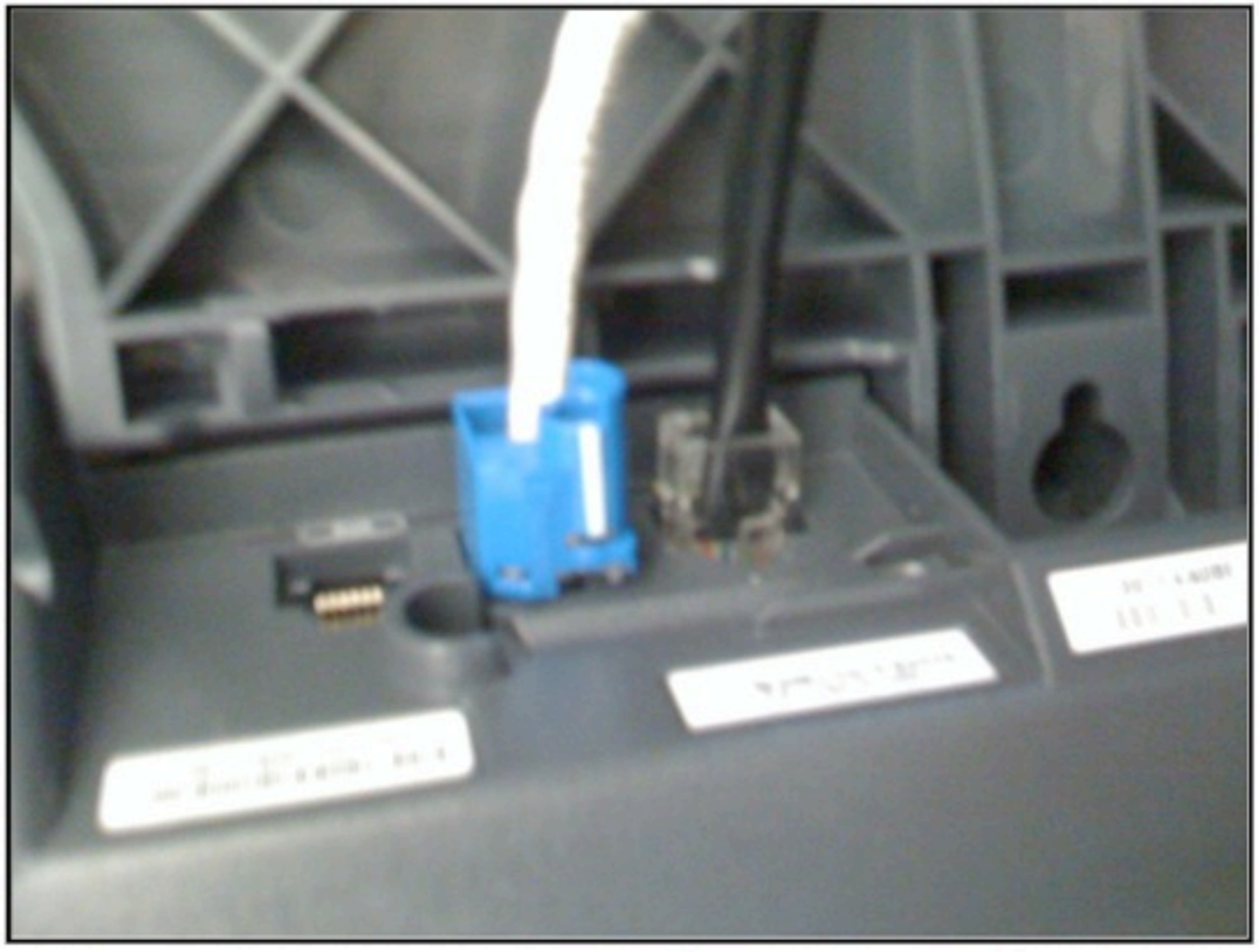
Mitigations: Don't do this

- Including "hiding" the MAC Address
- Hiding the MAC Address isn't a security feature

Mitigations



- Locking phones to wall



Mitigations

- Can be broken with this

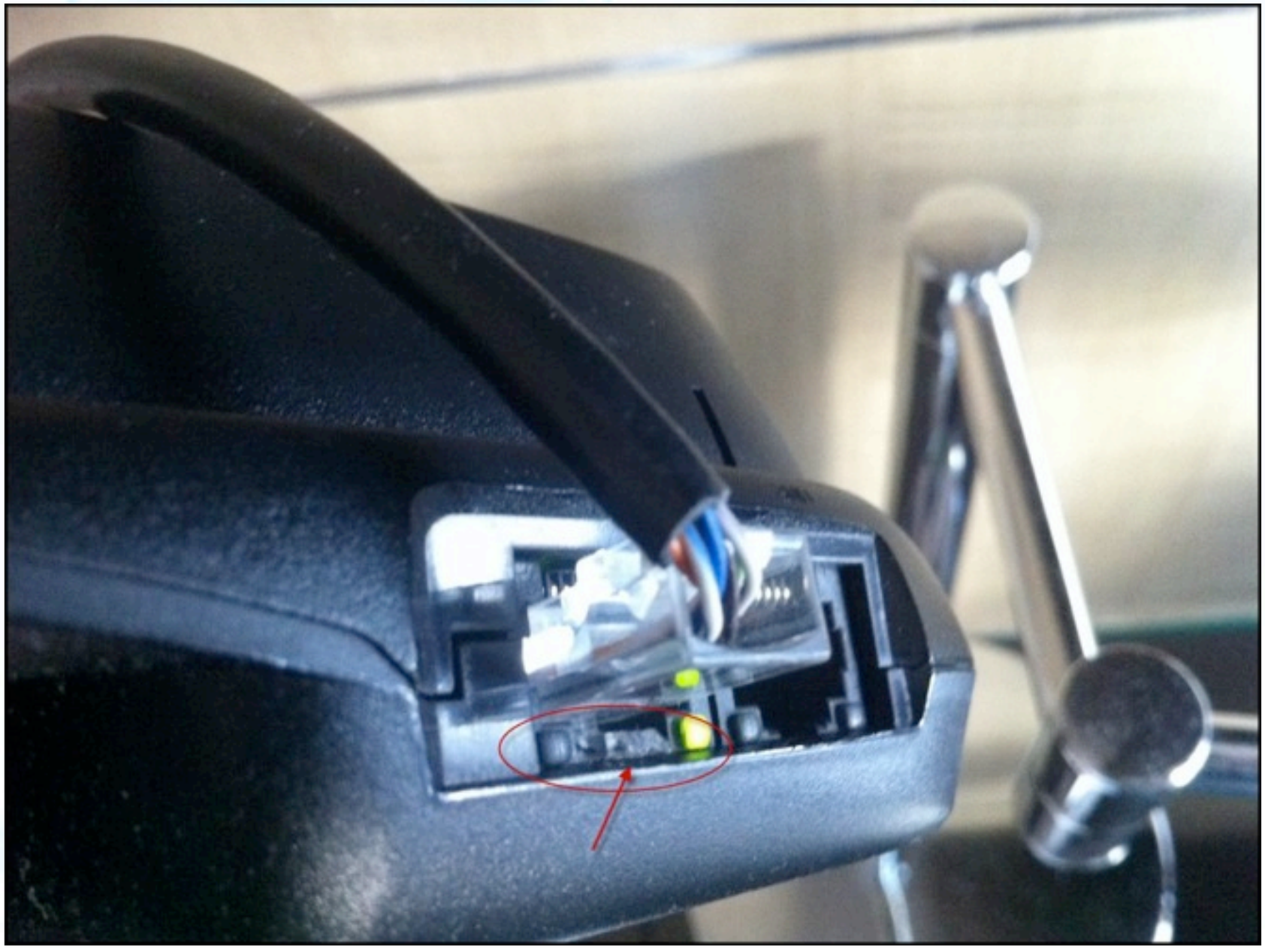
Mitigations

Fascinating, found another hotel this week using IP Phones in guest rooms. Vendor is specialized for VoIP in hospitality industry: www.teledex.com

Mitigations

Fascinating, look at what they did. They stripped the RJ-45 plug where a human would easily unplug the cable.

Almost a poor man's physical security solution. It looked like you could still use a tool to pry off the ethernet plug.



Part II

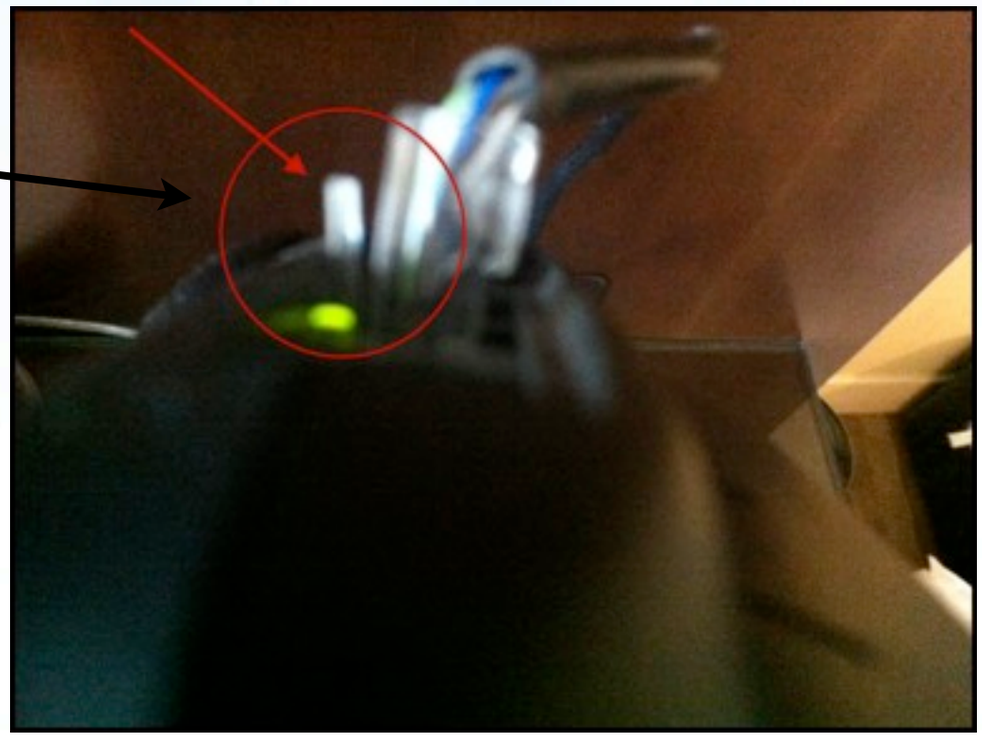
As circumstance would have it, I changed rooms (yesterday) in this hotel. Found the following in comparing new room to prior:

* In my new room, IP phone didn't have same physical security control applied.

* The RJ-45 connector plug was intact, and one could easily disconnect the phone from the wall and connect their laptop.

* Fascinating: Physical security controls not applied consistently across hotel guest rooms.

* Human error always the weakest link in a security system and can lead to breach, in the right scenarios.



Mitigations

- Great Mitigation Idea, not using dot1x
  - Lock phones to wall using Panduit or equivalent
  - If IP Phones are disconnected from wall
    - Err-disable the port ~ port goes down and needs Administrator intervention to enable
    - Issue a high priority snmp trap or syslog of suspicious activity
      - With either method, if the attacker has physically broken through the security locks, this is highly suspicious activity in a hotel room
        - » Either scenario should require NetOps or SecOps notification

Great security mitigation idea from Chris and Zack with Cisco Systems

Mitigations

- 802.1x with multi-domain authentication

LAN Security

IEEE 802.1x Multi-Domain Authentication on Cisco Catalyst Layer 3 Fixed Configuration Switches Configuration Example

HOME
SUPPORT

Document ID: 98523

- Make sure you don't configure single VLAN
  - With Cisco Voice VLANs, 802.1x can be bypassed via spoofing CDP

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

HOME
SUPPORT

Document ID: 65152

Downloads

Dotx1 limitations

- Be careful with 802.1x with VoIP wired deployments
  - Uses RFC 3847 EAP-MD5 authentication
  - Vulnerable to 2 security issues
    - Vulnerable to offline pcap dictionary attack
      - » EAP-MD5 vulnerable to offline dictionary attack
    - Vulnerable to MiTM attack
      - » 802.1x EAP authentication only required in wired deployments when port comes up
      - » Attacker can piggyback on successful Auth of an IP Phone, sharing a hub with IP Phone for unauthorized access

Major props to Josh Wright for his research.

Discovered by Steve Riley and Svyatoslav Pidgorny with Microsoft (2005)

Dotx1 limitations

- In 2008, VIPER published open source security assessment tool to highlight both of these issues in wired 802.1x deployments
  - XTest (ToorCon X, 2008)
- Talk advancing this forward

A Bridge Too Far: Defeating Wired 802.1x with a Transparent Bridge Using Linux

ALVA 'SKIP' DUCKWALL NORTHROP GRUMMAN, SR. CYBER SOMETHING OR OTHER

Using Linux and a device with 2 network cards, I will demonstrate how to configure an undetectable transparent bridge to inject a rogue device onto a wired network that is secured via 802.1x using an existing authorized connection. I will then demonstrate how to set up the bridge to allow remote interaction and how the entire process can be automated, creating the ultimate drop and walk away device for physical penetration testers and remote testers alike.

Alva 'Skip' Duckwall has been using Linux back before there was a 1.0 kernel and has since moved into the information security arena doing anything from computer/network auditing, to vulnerability assessments and penetration testing. Skip currently holds the following certs: CISSP, CISA, GCIH, GCIA, GCFW, GPEN, GWPT, GCFA, GSEC, RHCE, and SCSA and is working on getting his GSE. Skip currently works for Northrop Grumman as a Sr. Cyber Something or other.

Mitigations

- MACSec
  - IEEE 802.1AE
  - Provides hop-by-hop layer 2 encryption
  - Doesn’t appear to be widespread support yet, at least in Edge network ethernet switch products, or IP Phones

Conclusion - Thank you for listening!

- Why I did this

Someone is going to get caught with their pants down

Conclusion

- Why I did this
  - This talk is a culmination of my research on hotel VoIP VLAN & Infrastructure security (since 2007)
  - Share something I'm passionate about (interests me)

Attacking the Crown Jewels through VoIP

May 18th, 2010 by Jason Ostrom

The security weaknesses of VLANs have been known for years. Recent case studies have highlighted the potential risk of using Voice VLANs together with VoIP in an infrastructure absent of properly configured security controls. While visiting Europe just recently, I was reminded of this issue for a couple of reasons.

The British Crown Jewels

Voice of VOIPSA

Collective thoughts and musings on the state of VoIP security today.

Conclusion

- Why I did this (continued)
  - To create education and awareness
  - To publish a new version of the free security tool, “VoIP Hopper”, so that people can test their own network
    - Understand the vulnerability and risk for yourself (hotels, integrators)
    - Showing is believing
    - Seeing the vulnerability is believing (VoIP Hopper)
    - Sometimes people have to see a vulnerability with their own eyes before they can start to mitigate it

Conclusion

- Why I did this (continued)
  - It's my hope this information will get into the proper hands
    - Hotel Net and Sec Ops
    - System integrators and VARs who implement these Hospitality VoIP solutions
  - Before a real security breach happens in a hotel
  - See, if I'm showing this today, and it is news to a hotel
    - How many people already know, and were silent?
    - How many hotels have already been breached?

Conclusion

- Why I did this (continued)
  - Publishing updated best practices around UC security in these deployments would be a good first step
    - UC Security where 802.1q trunking is required ~ to protect customers
  - SANS mentions this in their Top 20 (2007)

> • Ensure that the VoIP VLAN can not be used as a way to gain access to other core services, usually this is a propagated VLAN over different locations with some machines such as the Call Manager dual homed.

Contact Information

- Jason Ostrom, CCIE #15239 (Security)
  - Director, VIPER (Voice over IP Exploit Research)
  - jostrom@viperlab.net; iknowjason@pobox.com
- For more information about us, visit us online:
  - VIPER Lab: http://www.viperlab.net
  - Sipera Systems: http://www.sipera.com