Polycom Videoconferencing Endpoint Security and Configuration

Scott Christianson

Polycom Videoconferencing Endpoint Security and Configuration

J Scott Christianson
GSEC Candidate, Practical Version 1.4

Abstract

This paper focuses on the security of videoconferencing endpoints made by Polycom Corporation—currently the leader in the videoconferencing market. The paper begins by discussing the recent growth in videoconferencing and introducing the International Telecommunication Union (ITU) system of videoconferencing standards. Videoconferencing components are briefly reviewed, including H.323 Terminals, MCUs, and Gatekeepers. The paper then provides an overview of the videoconferencing endpoints offered by Polycom. Next, the paper reviews some motivations for attacking videoconferencing endpoints. Then a number of vulnerabilities and related security measures are discussed, including: theft of endpoints, eavesdropping on videoconferencing calls, administrative security, ISDN and perimeter security, SNMP access threats, FTP access threats, and denial of service attacks. The paper describes how vulnerability scanners can misreport videoconferencing endpoints as Trojan horse programs and concludes with a checklist for Polycom endpoint security.

Introduction

Growth of IP-Based Videoconferencing

Videoconferencing over IP-based networks has grown at a dramatic pace in the last four years, and is poised to undergo another growth spurt due to a number of factors[1]:

1. Tighter budgets are pressuring companies to limit travel.
2. Security concerns are making travel less desirable, especially in certain countries.
3. Expenses for high quality ISDN-based videoconferencing can't be justified by some organizations when an existing IP infrastructure can be used instead.

An enterprise-wide IP-based videoconferencing system involves multiple components, including endpoints, gateways, gatekeepers, multipoint conferencing units (MCUs), desktop units, and other components[2]. Each part of a videoconferencing network has its own unique set of security concerns. These concerns may be compounded by the fact that the personnel who are assigned to manage videoconferencing within an organization often are not information technology personnel. Managers often decide that—since it involves cameras and TVs—audiovisual departments should handle videoconferencing for the organization. As a result, people who are not familiar with information security issues often administrate videoconferencing systems.

Videoconferencing Standards

The standards for videoconferencing are developed and approved by committees of the International Telecommunication Union (ITU), which is part of the United Nations[3]. There are standards for video compression and communications, audio transmission, call setup and termination, data collaboration, and others aspects of video communications. These standards are grouped together in "families" that include all the necessary standards for a particular type of videoconferencing transmission medium. For example, the standards for videoconferencing over TCP/IP networks are grouped together in the H.323 standard. The H.323 standard is one of sets of standards known as "H.32X" standards. There are currently four well-known H.32X standards[3]:

- **H.320** is for transmission over ISDN and dedicated T1 lines.
- **H.321** uses MPEG2 Compression for transmission over broadband ATM networks
- **H.323** is for transmission of videoconferencing over traditional TCP/IP networks. The formal name of this standard is "Visual Telephone Terminals over Non-Guaranteed Quality of Service LANs"
- **H.324** is for transmission of videoconferencing over analog telephone service (POTS or Plain Old Telephone Service). This type of videoconferencing has been used a lot recently by news reporters in Afghanistan. It offers the lowest quality of all the families of standards.

H.323 Videoconferencing Components

The main components of a H.323 videoconferencing system are terminals (endpoints), MCUs, and Gatekeepers. Each of these is described in more detail below.

H.323 Terminals

These are the actual endpoints of a videoconferencing system. H.323 endpoints include televisions, cameras, microphones, speakers, and an H.323 CODEC (Coder Decoder). It is the CODEC that encodes the analog video and audio signals into the digital protocols for transmission over the IP network and decodes the incoming data to analog video and audio. H.323 uses TCP for call setup, conference control and signaling. UDP is used for transmission of the video, audio and some control information. The table below lists the TCP and UDP ports that are commonly used by H.323 terminals[4&5].

Port	Protocol	Description/Function
389	Static TCP	Registration with ILS (Internet Locator Server) directories, which provides a real-time directory service for videoconferencing users.
1503	Static TCP	Transmission of T.120 data. T.120 is the ITU standard for data collaboration (shared whiteboard, application sharing, etc.)
1720	Static TCP	H.323 Call Setup

1731	Static TCP	Audio Call Control
1024-65535	Dynamic TCP	H.245 Call Parameter
1024-65535	Dynamic UDP	RTP (Video Data Streams)
1024-65535	Dynamic UDP	RTP (Audio Data Streams)
1024-65535	Dynamic UDP	RTCP (Status and Control Information)

H.323 Multipoint Conferencing Units (MCUs)
When more than two endpoints are involved in a conference, the conference must involve an MCU to bring the endpoints together. For additional information on MCU security, see H.323 MCU Security by T. Chown and B. Juby (Available from: http://www.ja.net/development/video/vip/reports/south5.pdf).

Gatekeepers
Gatekeepers assist endpoints and MCUs with call management. They can translate H.323 "aliases" or common names such as "Room 220" into IP addresses in much the same way that DNS servers resolve names to IP addresses on the web. For more information on Gatekeeper security, see H.323 Gatekeeper Security Issues, by T. Chown and B. Juby (Available from: http://www.ja.net/development/video/vip/reports/south4.pdf).

Polycom

Polycom is currently the world leader in the videoconferencing market, in terms of both units shipped and gross sales[6]. Polycom Endpoints come in three basic forms: the desktop ViaVideo, the set-top Viewstation models, and the rack-mounted VS4000. Figure 1 shows examples of these units.

Figure1: Form factors for Polycom endpoints.

There are four basic "lines" of Polycom videoconferencing endpoints, each with it's own version of Polycom software:

- Viewstation SP 128 and SP 384: These non-expandable units have limited camera inputs, monitors outputs and ISDN bandwidth capabilities. The SP line is the lowest priced of the set-top units (Approximate price: $4000-$6000).
- Viewstation 512,V.35, MP, and DCP: These units represent the most popular Polycom line and are very flexible and expandable (Approximate price: $6000-$12000).
- Viewstation FX and VS4000: These are the top of the list units and feature built-in four site MCUs and 60 frames per second video (Approximate price: $15000-$19000).
- ViaVideo: The ViaVideo is Polycom's desktop unit and will support H.323 calls up to 384kbps (Approximate price: $600).

All of these units support H.323 videoconferencing. For more information on these products, see www.polycom.com.

Videoconferencing Security Concerns

A wide range of security concerns must be addressed when working with videoconferencing technologies. These include: physical security of the endpoints, eavesdropping on the video or audio portions of a connection (meeting security), denial of service attacks, administrative security, and malicious "monkey-wrenching" of the endpoints. There are also auxiliary concerns, such as false alarms raised by vulnerability scanners.

There are several obvious reasons why an attacker might be motivated to attack a videoconferencing system:

1. A business competitor or someone within your company might want to listen into an important meeting.
2. A competitor might want to launch a denial of service attack, so that an important videoconference never takes place.
3. A student that uses videoconferencing to received instruction at a distance might want to make the system inoperable in order to avoid having class or having to take a test.
4. A thief might want to steal an endpoint in order to sell it.

Polycom Endpoint Security

Physical Security

Physical security can be a concern for a Polycom endpoint, since the units are very expensive (up to $18,000 for the set-top Viewstation FX), small, easy to carry, and easy to sell via online auction services like eBay. There are several means of physically securing Polycom units. The VS4000 is the easiest to deal with, since it is rack mountable and can be secured within a locked cabinet. There are two means of securing a set-top Viewstation.

- The back of the Viewstation has a place for a standard "Kensington" style lock. A cable lock (approximately $35) can be secured to the wall or nearby furniture and then secured to the Polycom.
- The Viewstation can be mounted using a set-top shelf, such as the one from Videolabs pictured in Figure 2. The Viewstation can be screwed or even lightly glued to the mounting shelf, which can in-turn can be secured to the television or the wall.

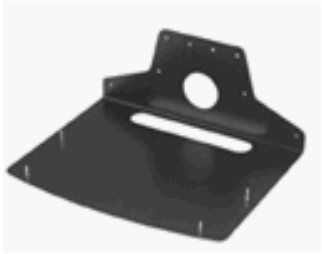

Figure 2: Videolabs Set-top Shelf Kit (List Price: $149).

These solutions would not stop a determined thief, but they would slow down a thief; in addition, the unit might be damaged if removed quickly. In order to maintain physical security, the rooms in which any Polycom units are kept must be secured. The desktop ViaVideo is the most vulnerable, since it is very small and cannot be connected to a Kensington style lock. Again, room security is a must for this type of unit.

Meeting Security

There are a number of important issues relating to the topic of meeting security—preventing someone from eavesdropping on a videoconference. The first step to increase meeting security is to make sure that endpoints are not set to automatically receive incoming calls. When the auto-answer feature is turned off, a recipient must actively accept any in-coming calls. This is also important for videoconference-capable rooms that are used for non-videoconferenced meetings to prevent someone from dialing into the room, muting their audio and video, and then listening into conversations in the room.

Another basic way to prevent eavesdropping is to define a meeting password that everyone must know in order to join the conference. This feature is available when using an MCU to connect your calls. Meeting passwords are defined in the ITU standards and are supported on most ITU-compliant endpoints. Meeting passwords are a good security measure that should be taken for any sensitive videoconferences, but will not stop a more technologically sophisticated attacker who knows how to sniff meeting passwords from the network. However, doing this type of sniffing is often very difficult or impossible, since video endpoints are often placed on entirely switched networks in order to avoid packet latency and jitter.

Another threat to meeting security is the capture and reconstruction of the audio and video, whereby an attacker can listen to the conversations. There is an open source tool that will allow for capture of the audio portion of a H.323 call (either from a videoconference or a VoIP phone) via TCPdump and reassembly of the data into WAV files for playback[7]. The tool is called Voice Over Misconfigured Internet Telephones or "vomit" and is available from http://vomit.xtdnet.nl/.

There is no way to easily encrypt videoconferencing calls using Polycom endpoints. There are no provisions for encryption built into the endpoints, so an external device must be used. External encryption devices are available for videoconferencing via V.35 (dedicated T1 and ISDN) and have been used for years, especially by the military (For an example of this type of device, see http://www.lysisit.gr/brochures/Biodata_Babylon_VC.pdf). For H.323 videoconferencing, the easiest way to create a secure conference is to create a VPN between the two networks in the conference, and then videoconference through that VPN[8&9]. The VPN must be created with a hardware device, since there is no provision for installing a VPN client on Polycom endpoints (with the exception of the ViaVideo desktop unit). This is a good solution for transport across a firewall as well, since ports do not need to be opened to the outside.

Administrative Security

All Polycom endpoints allow for administration of the endpoint via a web interface and/or a telnet session. The username for remote administration is always "Admin" and can't be changed. An administrator password may be used but is not required. However, if an administrator password is to be used, it must be set initially at the unit. This prevents an attacker from finding a system that doesn't have a password and setting up their own administrator password on that unit. On the Viewstation FX and VS4000 models, once an administrator password has been set, the password can be changed via the web interface or a telnet session after an administrator is logged into the unit. The other Viewstation models do not allow the password to be changed remotely. In addition, the administrator password is required on all Viewstation models for web access, but only the Viewstation FX and VS4000 require it for telnet access. This is a major security hole that Polycom should close in a future release of the Viewstation software.

When remotely accessing an endpoint via the web interface, the administrator password is encoded using a java applet that relies on the "Authorization: Basic" class. This password is encoded and is not easily sniffed in a form that is useable[10]. However, this login is subject to a replay attack, since the username/password hash will be the same for each login. Also, a program similar to L0phtcrack for NT, would be able to do a dictionary or brute force attack on this hash, especially since the username is always "Admin". Below is an example of the capture of an administrator login to the web interface of a Polycom unit captured with Ethereal and reconstructed using the "Follow TCP Stream" tool (Username/Password Hash is highlighted in yellow).

```
GET /a_admininindex.htm HTTP/1.1
Accept: application/vnd.ms-powerpoint, application/vnd.ms-excel,
application/msword, image/gif, image/x-xbitmap, image/jpeg,
image/pjpeg, */*
Referer: http://10.185.111.120/
Accept-Language: en-us
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0;
Q312461)
Host: 10.185.111.120
Connection: Keep-Alive
Authorization: Basic YWRtaW46U2NvdHQ
```

When an administrator remotely logins into a Viewstation FX or VS 4000 via telnet, the administrator password is sent in plaintext and is vulnerable to sniffing. Below is an example of the capture of an administrator telnet login to a Polycom unit captured with Ethereal and reconstructed using the "Follow TCP Stream" tool.

```
Welcome to ViewStation

Password: Scott

Hi, my name is :     Northwest

Here is what I know about myself:
Serial Number:       005BAA
```

```
Brand:                Polycom
Software Version:     Release 7.0.1 - 16 Jun 2001
Model:                VS
Network Interface:    V.35/RS-449
MP Enabled:           No
H323 Enabled:         No
IP Address:           10.185.251.111
Time In Last Call:    6:22:32
Total Time In Calls:  10475:30:15
Total Calls:          1009
Country Code:         1
```

Two TCP port numbers can be used for telnet to a Polycom Viewstation. Telnet access is available via the well-known telnet port of 23 as well as port 24, which is normally used for Private mail system. The reason for having two telnet ports is described in the Polycom software release notes as follows: "You can access the shell via telnet on Port 23 or Port 24. When you use Port 23, the Viewstation provides a shell prompt to the telnet and receives all internal software traces. To avoid the internal software traces, you can also access the command shell on the non-standard telnet Port 24."

SSH is not supported at this time for a secure command line session to the endpoint. There are no "backdoor" passwords that are common to other videoconferencing endpoints. If the password is lost, the Viewstation must be reset locally (it can't be done remotely). This process is described in the Polycom Knowledgebase (Available via http://www.polycom.com):

> If the Administrative Password on a ViewStation is lost, in order to unlock the unit, it must be reset by going to System Info > Diagnostics > Reset System (Version 7.0 and greater of the ViewStation Software.) To keep from inadvertently resetting the system, the short serial number shown on the System Information page is required. The opportunity is given to keep the System Settings and Address Book Entries. Performing the system reset, wipes out the Administrative password.

Once logged in, the administrator can change the configuration of the unit, view call status information, reboot the system, and even move cameras and change video sources. However, one cannot telnet from the Polycom to another device (it is a telnet server only and can't function as a client).

ISDN and Perimeter Security

Since Viewstations will often be connected both to the LAN and to ISDN lines, some network administrators are initially concerned about an attacker calling in on the ISDN lines and accessing the LAN. However the ISDN lines are not used for transport of IP traffic and will not support a PPP or SLIP connection[11].

SNMP Access

Polycom Viewstations support the use of SNMP for management. According to the CERT Vulnerability notes 854306 and 107186, which relate to the widely reported

vulnerabilities with SNMP, Polycom has not yet responded to this vulnerability. Therefore, SNMP should be turned off unless necessary. Organizations that must use SNMP should set access lists on their routers/firewalls to only allow SNMP to and from specified IP addresses.

FTP Access

Polycom endpoints also have an ftp server in the unit for upload of firmware updates (see vulnerability scans below). Besides the "normal" vulnerabilities associated with ftp (lack of encrypted passwords, etc.), this ftp server could be susceptible to common ftp buffer overflow attacks. In fact, a scan with the Retina vulnerability scanner suggested that this might be a problem:

> CHAM-FTP: T:Overflow,C:ALLO,S:5001,P:21
> Risk Level: High
> Description: CHAMFtp has found that the remote system may be vulnerable to one or more remote buffer overflow attacks.

For this reason, it would be a good idea to set access lists on a router/firewall to limit ftp access to only those IP address(s) from which administrators will be doing firmware updates.

Denial of Service (DOS) Attacks

DOS attacks can be launched against Polycom endpoints as well. Dadoun[7], points out that there are several ways that DOS attacks can be made on Voice over IP (VoIP) services, with the two most likely to be bandwidth consumption or resource starvation:

> ***Bandwidth consumption*** attacks attempt to consume all of the network bandwidth available to the victim, either directly by attacking from a network with more bandwidth than the victim or with an amplifying attack in which other sites are enlisted to overwhelm the bandwidth available to the victim.
> ***Resource starvation*** attacks focus on consuming system resources rather than network resources e.g. CPU, memory, disc space etc. This may take the form of making so many spurious processing requests that legitimate requests can no longer be serviced.

These attacks can also be used against H.323 videoconferencing systems as well (the H.323 standards are the basis for VoIP phone service).

Vulnerability Scans

Because of the large number of ports that are used for H.323 conferencing, videoconferencing endpoints will often create false positives when scanned by a vulnerability scanner. I did a scan of a Polycom Viewstation with Retina (available from http://www.eeye.com/), and it reported that it had the following ports open:

Port	Port Name*	Purpose
7	Echo	Ping, connectivity testing
21	ftp	Firmware updates, upload of slides to unit
23	Telnet	Remote command line access
24	Private mail system	Remote command line access
80	HTTP	Remote web access
5001	COMMPLEX-LINK -	H.323- RTP (Video Data Streams)
5003	CLARIS-FMPRO - Claris FileMaker Pro	H.323- RTP (Audio Data Streams)
5004	AVT-PROFILE-1	H.323- RTCP (Status and Control Information)

*From http://www.iana.org/assignments/port-numbers

Retina identified the unit as a "Tekronix Phaser 350 firmware 3.3(printer)", based on the profile of open ports. Because of the open ports at 5001,5003, and 5004, some programs and network administrators will assume that this is a Trojan horse program that waiting for a connection from a master (such as Netbus, or SubSeven).

Polycom Security Checklist

Based on the information presented in this paper, the following checklist can be used to help secure Polycom videoconferencing endpoints.

- ✓ Physically secure all Polycom endpoints and videoconferencing rooms.
- ✓ Turn auto-answer off.
- ✓ Set an Administrator password.
- ✓ Put all videoconferencing units on entirely switched segments, for increased video quality and to prevent password sniffing.
- ✓ Set meeting passwords on your MCU for all sensitive meetings.
- ✓ Turn off SNMP unless used by your organization.
- ✓ Use a VPN connection for secure H.323 videoconferencing.
- ✓ Use access lists to limit Telnet, SNMP and FTP access to only "trusted" IP addresses.

References

1. Wainhouse Research. March 2002. "The Business Case for Videoconferencing." URL: http://www.wainhouse.com/files/papers/WR-bizcase4vc.pdf (3 June 2002).

2. Polycom. 2001. "Video Communications: Building Blocks for a Simpler Deployment." URL: http://www.polycom.com/common/pw_item_show_doc/0,1449,693,00.pdf (3 June 2002).

3. Wilcox, James R. Videoconferencing: The Whole Picture, 3rd Edition. Gilroy, CA: Telecom Books, 2000.

4. Weiner, J. 2001. "Netmeeting Security Concerns" URL: http://rr.sans.org/win/netmeeting.php (3 June 2002).

5. Silbaugh, J. 2000. "It Is Only Dialtone" URL: http://rr.sans.org/wireless/dialtone.php (3 June 2002).

6. Wainhouse Research, 2002. "The Wainhouse Research Bulletin, Volume 3 Issue #22." URL: http://www.wainhouse.com/files/wrb-03/WRB-0322.pdf (3 June 2002).

7. Dadoun, N. 2002. "Security Framework for IP Telephony" URL: http://ftp.tiaonline.org/tr-41/tr4144/Public/2002-02-Vancouver/TR41.4.4-02-02-008SecurityFrameworknd.pdf (3 June 2002).

8. Polycom, 2001. "Deploying Secure Enterprise Wide IP Videoconferencing Across Virtual Private Networks." URL: http://nsd.polycom.com/products/LOOKAND1/New/VPN_sol_guide.pdf (3 June 2002).

9. Polycom, 2002. "Will encryption provide security in your video communications environment?" URL: http://www.skccom.com/1.888.734.4438/polyvideo/PolycomEncyption.pdf (3 June 2002).

10. Zukowski, J. 2002. "Java Tip 47: URL authentication revisited" URL: http://www.javaworld.com/javaworld/javatips/jw-javatip47.html (3 June 2002).

11. Polycom, 2001. "LAN-ISDN Security" URL: http://www.skccom.com/1.888.734.4438/polyvideo/ts-isdn-lansec.htm (3 June 2002).

###

Last Updated: August 25th, 2019

Upcoming SANS Training

Click here to view a list of all SANS Courses

SANS Philippines 2019	Manila, PH	Sep 02, 2019 - Sep 07, 2019	Live Event
SANS Canberra Spring 2019	Canberra, AU	Sep 02, 2019 - Sep 21, 2019	Live Event
SANS Munich September 2019	Munich, DE	Sep 02, 2019 - Sep 07, 2019	Live Event
SANS Brussels September 2019	Brussels, BE	Sep 02, 2019 - Sep 07, 2019	Live Event
SANS Oslo September 2019	Oslo, NO	Sep 09, 2019 - Sep 14, 2019	Live Event
SANS Network Security 2019	Las Vegas, NVUS	Sep 09, 2019 - Sep 16, 2019	Live Event
SANS Dubai September 2019	Dubai, AE	Sep 14, 2019 - Sep 19, 2019	Live Event
SANS Paris September 2019	Paris, FR	Sep 16, 2019 - Sep 21, 2019	Live Event
SANS Rome September 2019	Rome, IT	Sep 16, 2019 - Sep 21, 2019	Live Event
SANS Raleigh 2019	Raleigh, NCUS	Sep 16, 2019 - Sep 21, 2019	Live Event
Oil & Gas Cybersecurity Summit & Training 2019	Houston, TXUS	Sep 16, 2019 - Sep 22, 2019	Live Event
SANS Bahrain September 2019	Manama, BH	Sep 21, 2019 - Sep 26, 2019	Live Event
SANS San Francisco Fall 2019	San Francisco, CAUS	Sep 23, 2019 - Sep 28, 2019	Live Event
SANS London September 2019	London, GB	Sep 23, 2019 - Sep 28, 2019	Live Event
SANS Dallas Fall 2019	Dallas, TXUS	Sep 23, 2019 - Sep 28, 2019	Live Event
SANS Kuwait September 2019	Salmiya, KW	Sep 28, 2019 - Oct 03, 2019	Live Event
SANS Cardiff September 2019	Cardiff, GB	Sep 30, 2019 - Oct 05, 2019	Live Event
SANS DFIR Europe Summit & Training 2019 - Prague Edition	Prague, CZ	Sep 30, 2019 - Oct 06, 2019	Live Event
SANS Tokyo Autumn 2019	Tokyo, JP	Sep 30, 2019 - Oct 12, 2019	Live Event
Threat Hunting & Incident Response Summit & Training 2019	New Orleans, LAUS	Sep 30, 2019 - Oct 07, 2019	Live Event
SANS Northern VA Fall- Reston 2019	Reston, VAUS	Sep 30, 2019 - Oct 05, 2019	Live Event
SANS Riyadh October 2019	Riyadh, SA	Oct 05, 2019 - Oct 10, 2019	Live Event
SANS October Singapore 2019	Singapore, SG	Oct 07, 2019 - Oct 26, 2019	Live Event
SIEM Summit & Training 2019	Chicago, ILUS	Oct 07, 2019 - Oct 14, 2019	Live Event
SANS Lisbon October 2019	Lisbon, PT	Oct 07, 2019 - Oct 12, 2019	Live Event
SANS Baltimore Fall 2019	Baltimore, MDUS	Oct 07, 2019 - Oct 12, 2019	Live Event
SANS San Diego 2019	San Diego, CAUS	Oct 07, 2019 - Oct 12, 2019	Live Event
SANS Doha October 2019	Doha, QA	Oct 12, 2019 - Oct 17, 2019	Live Event
SANS SEC504 Madrid October 2019 (in Spanish)	Madrid, ES	Oct 14, 2019 - Oct 19, 2019	Live Event
SANS London October 2019	London, GB	Oct 14, 2019 - Oct 19, 2019	Live Event
SANS Seattle Fall 2019	Seattle, WAUS	Oct 14, 2019 - Oct 19, 2019	Live Event
SANS Denver 2019	Denver, COUS	Oct 14, 2019 - Oct 19, 2019	Live Event
SANS Copenhagen August 2019	OnlineDK	Aug 26, 2019 - Aug 31, 2019	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced