Global Information Assurance Certification Paper

ANALYZING POLYCOM®

VIDEOCONFERENCE TRAFFIC

GIAC (GCIA) Gold Certification

Chris Cain, BS, GCIH, GCIA, GSFW

Advisor, Rob Vandenbrink

cicain08@gmail.com

ABSTRACT

Using H.323 with videoconferencing (VC) has been the method of choice for conducting remote meetings and presentations for many private and public sector organizations. Polycom, a popular vendor for videoconference products, provides hardware and software solutions for these purposes. Securing these products can be an afterthought because of the complex technologies involved as well as physical requirements for setup. There are many protocols that can be used in videoconferencing using Polycom equipment and many of these have been covered extensively. With the use of H.323 in most Polycom VC calls, it seems this protocol should be covered in more detail and the security considerations when implementing it within a network. Included with this review will be some IDS signatures that can be used to secure a Polycom videoconferencing system. Descriptions of some open source telephony tools will also be tested against these systems.

1.0 INTRODUCTION

Most businesses and hospitals have relied on videoconferencing (VC) hardware to perform meetings, interviews, presentations or even tele-medicine procedures for many years. With the capabilities it provides more applications including instant messaging, telephony, and e-mail are becoming more unified allowing cloud-based technologies to integrate these without the use of costly equipment. This adds more complexity to configuring and securing these applications. Finding ways to connect videoconferencing is becoming more of a requirement and an increased security threat. Support contracts for this equipment can be costly leading some organizations to use internal support staff for setup, support and configuration of the VC systems and may lack understanding of the protocols involved. This lack of understanding can create a security risk if proper configuration is not applied.

Polycom has been a major vendor in providing videoconference equipment and software. Much of the technology Polycom uses is implemented with other major vendors. Research into its products has been lacking in documentation from outside sources other than what they have provided. Focusing on the vulnerabilities within a Polycom system should be understood, as any videoconference system should be considered a networking device much like a switch, router or PC, but with the additional protocols and services, which can be very complex. Recommendations on securing Polycom equipment is important if outside consultants will be implementing it as well, as many times outside vendors don't typically know the security policies that are in place. Many times it is rare to find an external vendor implementing a network device on most medium to large networks, but due to the complexity of videoconferencing many companies will hire externally for implementation. It is this reason that working with vendors during implementation and ensuring they follow best practices is important to avoid costly support costs later.

Chris Cain - cicain08@gmail.com

2.0 MAIN SECTION

The H.323 protocol has been used extensively with videoconference systems for some time and is still the protocol of choice for many companies because of its reliability and quality it ensures. Looking at the technology that make up the H.323 protocol suite is important to understand the security threats that it can create within a network as well. The protocol does have security mechanisms in place such as using H.235 for authentication, integrity, nonrepudiation, and encryption; however, this is very limited and is rarely used due to concerns of performance issues (Porter, Thomas PhD, 2010). Creating proper IDS signatures is another option that can be used against known Polycom vulnerabilities, a few examples are provided in this document. These are just a few of the mechanisms that can be used to properly secure the H.323 framework.

Overall security is many times an afterthought when using multimedia technology due to the importance that it performs efficiently. Thus, more research needs to be around the security threats that using VC protocols such as H.323 can add. Following vendor recommendations is important whenever implementing videoconferencing on a network.

For many years the suite of protocols that have been used for the majority of voice and video traffic have been placed within a framework known as H.323. The H.323 protocol as it has been referred to is actually a suite of protocols that provide multimedia conferencing over a packet switched network. In recent years the Session Initiation Protocol (SIP) has become a popular alternative to H.323 when it comes to Voice over IP (VoIP) applications because of how easily it integrates within an IP network and traverses firewall and NAT devices. Recent changes, however, to the H.323 framework have improved its functionality within these operations. H.323 has been used exclusively within phone companies for some time because of its packet-switching combined with circuit-switching capabilities. It is the reason many have delayed the move to SIP as their framework of choice as research continues to develop in this field. However, SIP will

soon become the main protocol used throughout most audio and video traffic because of its security capabilities, features and open standards. Due to this, focus will be on the vulnerabilities and description of the H.323 protocol and how to mitigate the risks involved when it is used with VC.

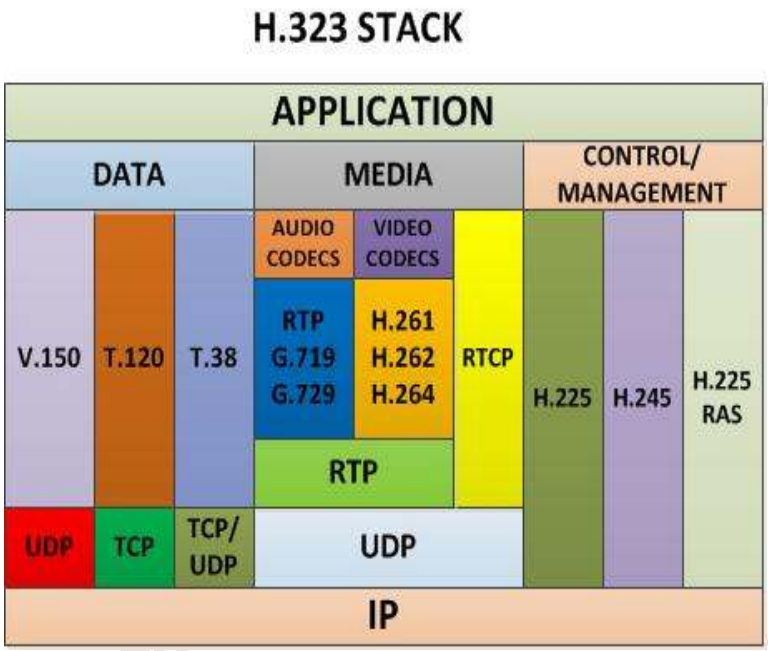
There are many considerations and risks when using H.323 with videoconferencing. One of the main security threats with videoconferencing is Denial of Service (DoS) attacks. Due to the importance of a quality connection for streaming traffic, many times a DoS attack can cause a videoconference system to crash or not allow a proper connection. Another risk is that H.323 does not work well with NAT. Many firewall rules will allow access to a videoconference unit using 1 to 1 NAT, which allows access to multiple protocols and ports to achieve successful connection. These protocols could allow more services to be exploited than would normally be allowed behind a firewall.

Due to the complex technologies and cost of using H.323 in VC, integrating open source technologies has been somewhat of a challenge. The H.323 Plus open source project formerly the OpenH323 Project is focused on implementing open source technologies for systems to connect to H.323 systems. Polycom offers software solutions, such as Polycom PVX for its VC line that allow this, but it comes at a cost. Using open source tools it can be possible to test connectivity and verify if the connection has been secured. Though, setting them up requires sufficient knowledge in their usage.

H.323 was a standard or recommendation created by the International Telecommunications Union Telecommunications Sector (ITU-T)[1]. H.323 is able to be updated and refined to fit these new improvements and has the ability to include additional features and functions as well. The H.323 stack, which is shown below,

[1] The ITU-T is similar to the Internet Engineering Task Force (IETF) in that it provides documentation of implementing each of the protocols used in H.323. The H.323 Recommendation also includes Annexes and Appendices to stay current with technology. Annexes are typically what make up the H.323 standard. Appendices are informational documents that go along with the H.323 standard.

contains protocols that first control and maintain the call when the connection is made between systems. Once that connection is established then Media Control Protocols are used to maintain the quality of the video and audio using various codecs. The Data stack protocols are then used to control the data that is passed between systems. The following is what a typical H.323 stack looks like.



(Rodman, J. 2008)

The H.323 suite of protocols contains strong support of audio and video, which is the main reason it is used so extensively in VC product lines. When explaining H.323, many would describe it as "multimedia over IP". What this means is that the underlying technology carries typical IP traffic but also carries additional traffic on top that handles all the encoding and signaling that need to take place during a typical videoconference call.

Videoconferencing technology in recent years has been moving towards the Next Generation Network (NGN)[2]. Polycom VC systems are able to handle IP traffic and act as Multipoint Control Units (MCU's) or as endpoints avoiding the use of Gateways and Gatekeepers[3], which would normally handle video and audio traffic conversion on an IP network. Many third parties are coming out with cloud-based services that will enable this Multipoint Control without the use of additional equipment. Many of these services come with high usage fees however. As more cloud based provider's come along these prices may be reduced and this may be the future of videoconferencing systems.

Polycom implements H.323 within its systems similar to other product lines, but also includes additional features and technologies that other manufacturers may lack. We will cover these features briefly as they will be seen in the packet captures that are analyzed.

Polycom systems also utilize Quality of Service (QoS). QoS types include IP Precedence and DiffServ. IP Precedence can be set from 0 to 5 representing the priority of IP packets. DiffServ QoS uses DiffServ Code Point (DSCP) one being Expedited Forwarding (EF) and the other being Assured Forwarding (AF). EF is used mostly for VoIP applications because of how it keeps the high priority queue very small, which could cause loss of packets if the queue is full. AF provides four classes, each with three drop precedence levels. (Perumal, M. A. M, 2009)

If video becomes blocky or network errors occur, packets may be too large, so decreasing Maximum Transmission Unit (MTU) size may alleviate the problem. If the network is burdened with unnecessary overhead the packets may be too small which requires

[2] A packet-based network that provides telecommunication services and is able to make use of multiple broadband and Quality of Service (QoS) transport technologies.(16)

[3] Gatekeepers are used to interface telecommunication devices to an IP network and handle admission control and address resolution for media devices. As Gatekeepers handle the call traffic, they will typically use Peer and Border Elements as a way to handle the addressing required between endpoints and authentication and authorization. It should be noted that Gatekeepers do not support IPv6 traffic. (Jones, P. 2007)

increasing the MTU size. Videoconferencing tends to have a higher and much variable MTU size compared to other network traffic. (Perumal, M. A. M, 2009)

Polycom systems allow advanced configuration of their API using telnet communications to enable or disable certain functions and to automate certain functions. Connections can be made over RS-232 or telnet over a LAN. Using various commands everything within the videoconference system can be set remotely, including camera position, directory, QoS and even to make or disconnect calls. There is quite a bit that can be done with this interface. A few commands are listed below:

*get = returns current setting

- farcontrolnearcamera <get|yes|no>
- dial auto|manual “speed” “dialstr” <h323|ip|sip>
  ex. dial manual 64 5551212 h323
- dns set [id=1:4] “ip”
- whoami = returns all system info
- recentcalls = retrieves all recent calls
- muteautoanswer <get|yes|no>
- ldapusername <get|set>
- ldapserveraddress <get|set>
- ldappassword set <ntlm|basic> “password”
- ldapntlmdomain <get|set>
- ldapbinddn <get|set>

These are just a few of the commands that you can use on Polycom videoconference systems. (Jones, P. 2007)

Polycom VC systems will typically use the following service ports:

23 – Telnet

24 – Polycom API (Telnet)

80 – HTTP Software upgrades, HTTP interface, system information

123 – Network Time Protocol (NTP)

161-162 – Simple Network Management Protocol (SNMP)

389 – LDAP and ILS registration

443 – TCP HTTPS

514 – UDP Syslog

636 – LDAP secure communications

1503 – TCP T.120

1718 – TCP Gatekeeper discovery

1719 – TCP Gatekeeper Registration, Admission, and Status (RAS)

1720 – TCP H.323 call setup

1731 – TCP Audio call control

3601 – Polycom proprietary Global directory data

5001 – Polycom People+Content

5060 – TCP/UDP SIP call setup

8080 – TCP HTTP Server Push

1024:65535 – Dynamic H.245 can be fixed, RTP audio and video, RTCP all can be fix.

2.1 VIDEOCONFERENCE COMMUNICATIONS

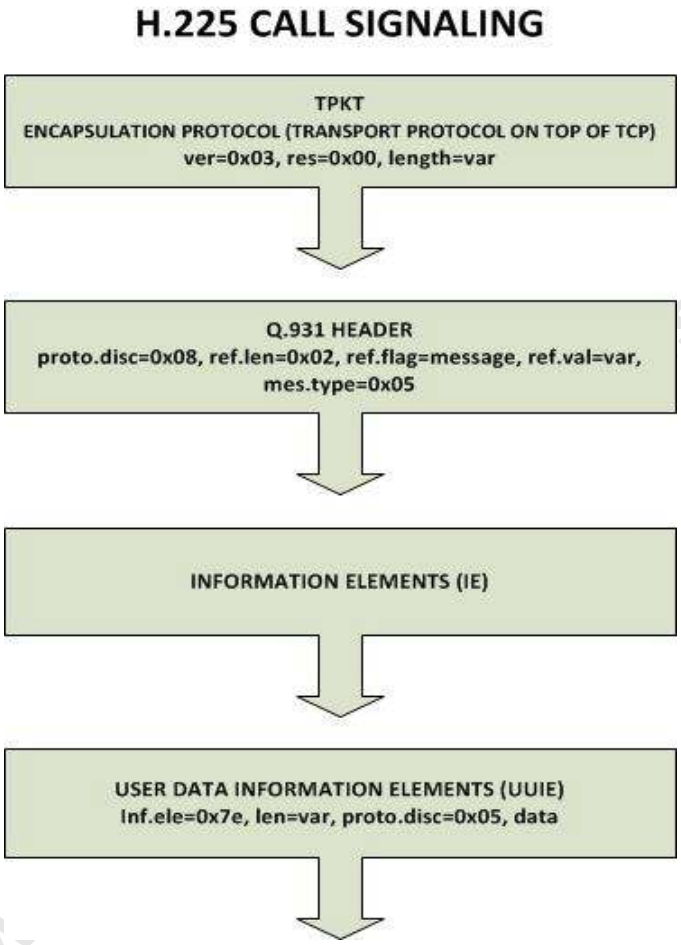
2.1.2 H.225/Q.931 CALL SETUP & CONTROL

The following protocols are typically used during a videoconference call.

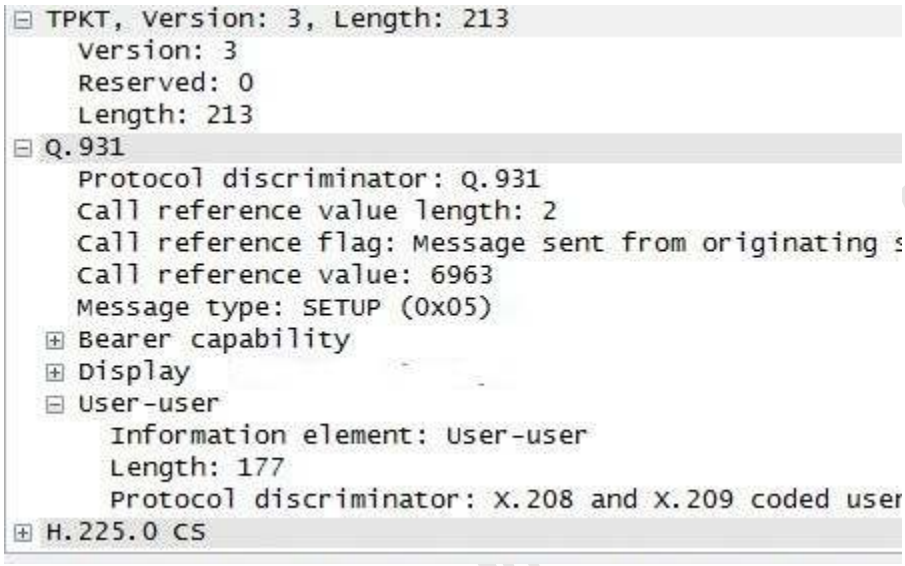
- H.225/Q.931
- H.245
- RTP
- RTCP

When a call is first placed between videoconference systems there are a few setup procedures that take place using the H.225 protocol. The H.225 protocol establishes call signaling between systems or endpoints. The diagram below gives a graphical view of how traffic is processed using the H.225 protocol within Q.931.

Q.931 is an older connection control protocol that was used for ISDN calls and is now used by H.225 as a way to handle call connection setup and teardown, but has been modified to support traffic on an IP network. The format of a Q.931 message and an H.225 message are similar and include a single byte protocol discriminator which is assigned the 8th bit, a call reference value to distinguish between different calls being managed, a message type, and various information elements as required by the message type. Below is a diagram of an H.225 Call Signaling packet.



Here is a sample packet capture of an H.225 initial Call Setup:



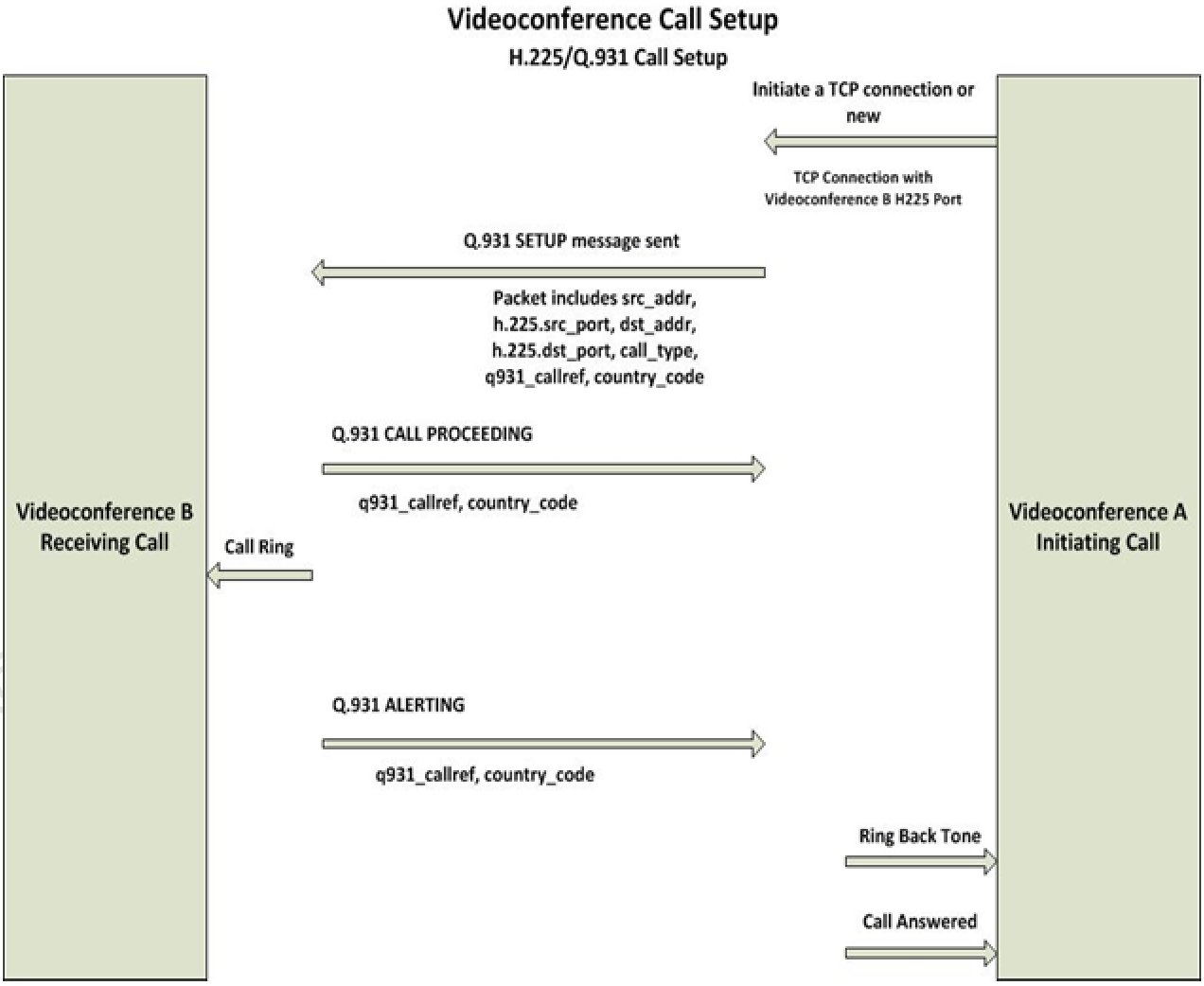
During an initial call a user will hear a tone that a connection is being requested or received such as a ringing or an inband tone. If the connection fails than an announcement is made on the screen as to why the call failed.

Some H.225/Q.931 messages that are typically seen in a packet include:

- CALL PROCEEDING
- CONNECT
- CONNECT ACKNOWLEDGE
- SETUP
- SETUP ACKNOWLEDGE
- SUSPEND
- SUSPEND ACKNOWLEDGE
- SUSPEND REJECT
- RESUME
- RESUME ACKNOWLEDGE
- RESUME REJECT

- DISCONNECT RELEASE
- RELEASE COMPLETE
- STATUS INQUIRY
- STATUS
- ALERTING

Below is a diagram showing how traffic will typically flow during a call using H.225/Q.931 signaling.



2.1.3 H.245 SIGNALING

The H.245 protocol is part of the H.323 framework and offers many multimedia signaling options during an initial VC call setup. The signaling and connection of H.245 occurs in parallel with an H.225 call setup.
H.245 provides control to the multimedia session that has been established and handles the following services:

- Terminal Capability Exchange
- Master/Slave Determination
- Logical Channel Signaling
- Conference Control

H.245 is typically run over a separate TCP connection than H.225, but can be tunneled within H.225 if needed. When using UDP tunneling through H.225 is required. H.245 messages are carried via a special channel called a Control Channel. Typically, you will find that many H.245 connections are now tunneled within the H.225 signaling messages.

The H.245 Fast Connect option does not use all available options and connects in the quickest manner possible with just a SETUP and a CONNECT message.

There are four different message types used within H.245 and include the following:

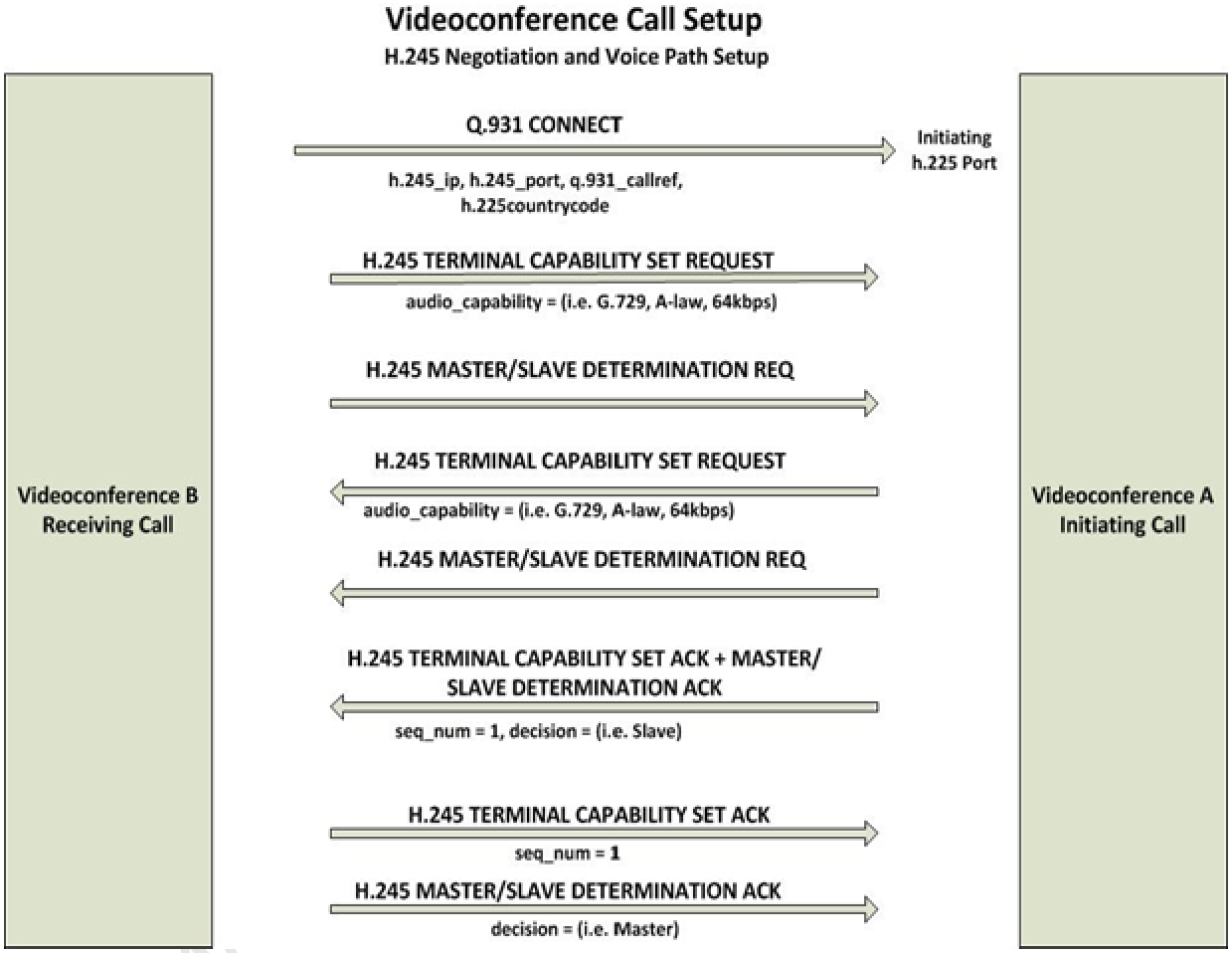
- **REQUEST**
    - Ex. MasterSlaveDetermination
    - Ex. TerminalCapabilitySet
- **RESPONSE**
    - Ex. MasterSlaveDeterminationACK
    - Ex. TerminalCapabilitySET

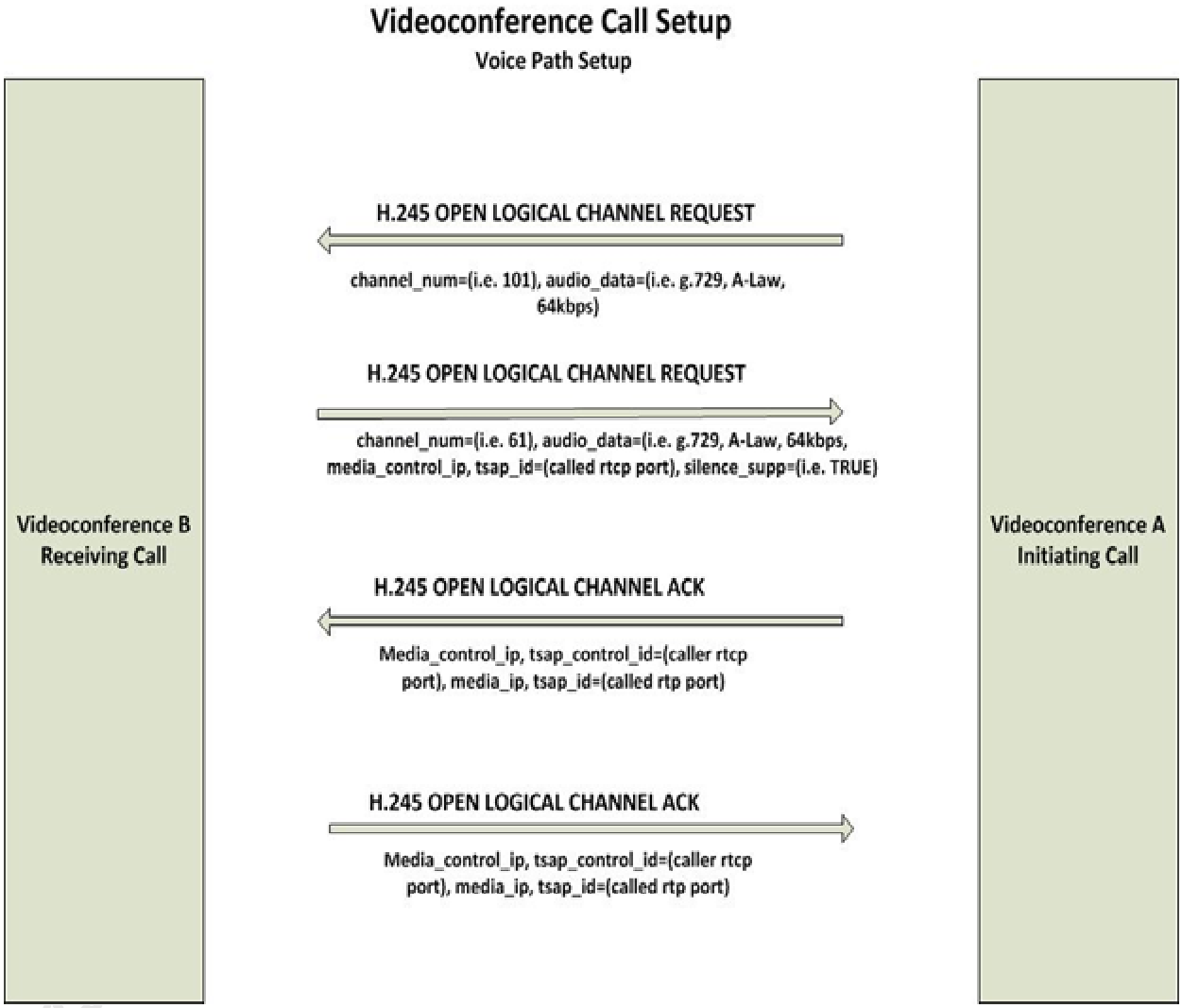
- **COMMAND**
    - Ex. SendTerminalCapabilitySet
- **INDICATION**
    - Ex. UserInput

The first exchange is to determine capabilities of each system and what type of media each system can handle such as codecs and streaming. This is similar to a stranger walking up to on a street and speaking to you in a different language. Once you both realize you can't communicate you then switch to a language you both can speak. The TerminalCapabilitySet (TCS) must be the first message transmitted on the H.245 channel. The capabilities are numbered and include the following examples of capabilities: **1- G.723.1, 2 – G.711, 3 – H.261, 4 - H.264, 5 – T.38** to name a few.

The Master/Slave determination process of the H.245 signaling protocol is used to determine which system is allowed to make decisions on call control issues that can arise during the duration of a call. During an initial videoconference session the H.245 signaling protocol will take a series of steps to make sure no conflicts occur. To avoid attempts to retrieve resources simultaneously such as opening logical channels a determination is made to set which terminal or endpoint system is master and which is slave so that these conflicts can be remedied properly. The system with the larger terminal type number is chosen as the Master. If the terminal type numbers are the same then they are compared using modulo arithmetic to determine the Master and the Slave. An indeterminate result can occur if both terminals have equal type field numbers.

The following is a diagram of a typical H.245 negotiation and setup during a VC call.


Videoconference Call Setup
H.245 Negotiation and Voice Path Setup
Videoconference B
Receiving Call
Videoconference A
Initiating Call
Q.931 CONNECT
Initiating
h.225 Port
h.245_ip, h.245_port, q.931_callref,
h.225countrycode
H.245 TERMINAL CAPABILITY SET REQUEST
audio_capability = (i.e. G.729, A-law, 64kbps)
H.245 MASTER/SLAVE DETERMINATION REQ
H.245 TERMINAL CAPABILITY SET REQUEST
audio_capability = (i.e. G.729, A-law, 64kbps)
H.245 MASTER/SLAVE DETERMINATION REQ
H.245 TERMINAL CAPABILITY SET ACK + MASTER/
SLAVE DETERMINATION ACK
seq_num = 1, decision = (i.e. Slave)
H.245 TERMINAL CAPABILITY SET ACK
seq_num = 1
H.245 MASTER/SLAVE DETERMINATION ACK
decision = (i.e. Master)



2.1.4 AUDIO CODECS BRIEF OVERVIEW

Audio codecs are an important part of VC and are used to determine the rate to which the audio can traverse. When comparing different codecs there can be quite a bit of confusion as to which ones are the best and what each of features are, such as comparing G.711 to G.729. Below are some things that should be considered when evaluating an audio codec.

- Audio bandwidth (higher is better)

- Data rate or bit rate (how many bits per second, fewer is better)
- Audio quality loss (how much does audio degrade, lower is better)
- Kind of audio (does it only work with speech?)
- Processing power required (less is better)
- Processor memory required (less is better)
- Openly available to vendors? (Yes is essential)
- Inserted delay (audio latency, less is better)
- Resilience (amount of lost or corrupted packets, more is better)
- ITU standards based (yes is better)

Here are a few descriptions of popular codecs used today in VC systems:

- G.719 is the best match among requirements for many communication systems at 20 kHz and combines excellent quality for music and voice with low latency, modest processor power and network friendly bit rates.
- G.722 is the grandfather of 7 kHz wideband codecs, and is the most widely deployed codec so far.
- G.722.1 is also known as Siren 7 and is a modern 7 kHz audio codec used in almost every videoconferencing system and is gaining traction within the VoIP field because of its high efficiency and lower bit rate.
- G.722.1 Annex C also known as Siren 14 runs at 14 kHz and is an extension of the G.722.1 codec and is popular because of its wider bandwidth, efficiency, and availability of being free.
- MP3 is the popular format used within the music industry and uses a form of transform encoding.
- Free Lossless Audio Codec (FLAC) produces much higher bit rates, but compensates by preserving the audio quality
- The Adaptive Multi-Rate Codec (AMR) encodes narrowband (200-3400Hz) signals at variable rates ranging from 4.75 to 12.2kbps with toll

quality speech starting at 7.4kbps. AMR is the standard codec for 2.5/3G wireless networks based on GSM (WDMA, EDGE, GPRS).

- G.729 is an audio codec that compresses voice audio in chunks of 10 milliseconds and is used mostly in VoIP applications. The standard version operates at 8 kbit/. G.729a is an extension to the standard that allows the same rates but with less computation.
- G.729.1 is a recent upgrade to G.729 that allows wideband speech and audio encoding.

2.1.5 REAL TIME PROTOCOL (RTP)

The Real Time Protocol (RTP) provides end-to-end network transport functions for audio and video over multicast or unicast network. It is typically run over the UDP protocol.

Below is what an RTP packet contains:

MAC Header	IP Header	UDP Header	RTP Message

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Ver			P	X	CC				M	PT							Sequence Number														
Timestamp																															
SSRC																															
CSRC [0:15]																															

Ver = Version (2 bits)

P = Padding (1 bit)

X = Extension (1 bit)

CC = CSRC Count (4 bits)

M = Marker (1 bit)

PT = Payload Type (7 bits)

Below is a sample RTP packet captured during a typical call.

```
Real-Time Transport Protocol
  [Stream setup by H245 (frame 46)]
      [Setup frame: 46]
      [Setup Method: H245]
    10.. .... = Version: RFC 1889 Version (2)
    ..0. .... = Padding: False
    ...0 .... = Extension: False
    .... 0000 = Contributing source identifiers count: 0
    0... .... = Marker: False
    Payload type: DynamicRTP-Type-115 (115)
    Sequence number: 0
    [Extended sequence number: 65536]
    Timestamp: 0
    Synchronization Source identifier: 0x5f22a801 (1596106753)
    Payload: 0b13300d4c8854606aa9885440f98a63f3ac104374b01203...
```

RTP Events that occur with DTMF Event ID'S set are typically tones that are expressed within the videoconference system, such as changing the volume or setting a parameter.

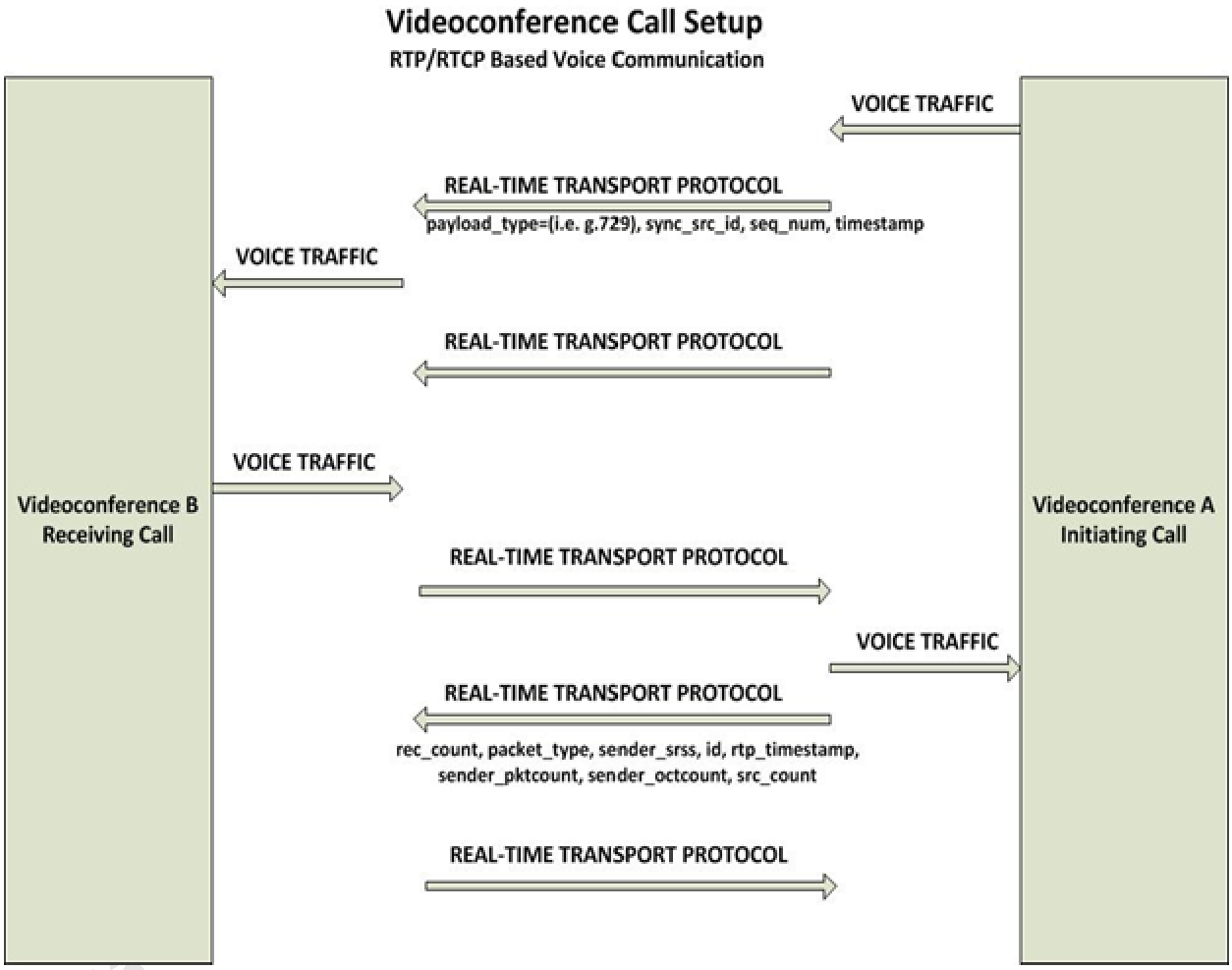
Synchronization Source Identifier (SSRC) is a randomly chosen 32-bit identifier carried in the RTP header, which starts from the source. It is randomly chosen to avoid having the same SSRC chosen within the same RTP packet. If multiple streams are created such as from multiple cameras, then an additional SSRC is required. If a source changes its transport address then a new SSRC is also required.

Contributing Source Identifier (CSRC) is the source of stream packets that carries a list of up to 15 elements containing SSRC's that contributed to the packet. These could be separate cameras or microphones that were involved in the RTP packet or were in the same mixer.

RTP will send audio data in small chunks across a conference in 20ms durations, which is then preceded by the RTP Header. The header and data are contained within the UDP packet. The RTP Header contains information about the type of audio encoding used (i.e. PCM, ADPCM, or LPC). The RTP Header also contains a sequence number and timing info to reconstruct fragmented packets.

When using both audio and video in a conference both media are transmitted using separate RTP sessions. That is separate RTP and RTCP UDP port pairs and/or multicast addresses. The only association that needs to be made is the distinguished name or canonical name in the RTCP packet to associate the sessions. This association allows one party to receive only audio and video if they so choose. Synchronized playback of these sessions is possible using the timing information carried within the RTCP packets.

Below is a diagram explaining the process involved in an RTP/RTCP based call.



2.1.5 REAL TIME CONTROL PROTOCOL (RTCP)

The Real Time Control Protocol (RTCP) is used to monitor Quality of Service (QoS) and to convey information about the participants in an on-going session and monitors the control packets of a VC call. The control packet consists of a fixed header part similar to that of an RTP data packet.

RTCP packets contain information about the participants of a conference using what are called reception reports, which are multicast periodically to verify if anyone has left the conference. The reception report indicates how well a current speaker is being received and can be used to control adaptive encodings. Once the conference is ended an RTCP BYE packet is sent from the site. The following is the format that an RTCP packet contains.

SR – Sender Report, which shows transmission and reception statistics from participants that are active senders.
RR – Receiver Report, which shows transmission and reception statistics from participants that are **NOT** active senders.
SDES – Source Description Items, including CNAME.
BYE – This indicates the end of participation in the call.
APP – are related to application specific functions.

2.1.6 ADDITIONAL POLYCOM PROTOCOLS

The H.235 protocol is the security recommendation for the H.323 framework. It provides authentication, privacy and integrity. Traffic can be secured using TLS or an IPSEC tunnel across a VPN. H.235 can also secure a call using Digital Certificates on the H.245 tunnel. Implementing this can sometimes cause performance degradation so proper QoS configurations need to be configured. (Rodman, J 2008)

The H.226 protocol is a channel aggregation protocol intended for multilink operation. This allows Multipoint Control Units (MCUs) to handle multiple channels of data throughout a call.

An MCU is a system that can handle multi calls at the same time. The MCU provides central access for multiple calling parties. The maximum number of members allowed to call in is based on the system that is used.

The H.239 protocol is used by Polycom specifically to stream content across VC systems. The streaming can be enabled via the videoconference unit itself on a MCU or via the proprietary software from Polycom called People+Content. Both sides must support H.239 for content sharing to take place.

The H.264 Content protocol streams data across VC systems. If this protocol is enabled this will be used first if both sides are able to support it.

2.1.8 SECURITY RECOMMENDATIONS

When using H.225 for control messaging there are some things to consider in regards to threats. H.225 has a weakness in allowing execution of code and DoS attacks against it. Many of the security failures of H.225 result in that there are insufficient bounds checking in H.225 messages as they are parsed and processed. These errors are primarily due to problems in low-level byte operations with vendor ASN.1 PER/BER PDU decoders. These attacks can result in system crashes and reload (DoS), or in execution of code. Flooding multiple malformed Gatekeeper Request (GRQ) packets to the Gatekeeper, (If there is one), can disconnect the VC call. (Porter, Thomas PhD, 2010)

Another issue with H.323 is the complexity of how it handles firewall rules. Due to the way it handles NAT and the many port options, it can difficult to limit the ports at the firewall due to the range that need to be available.

Recently, the University of Oulu Secure Programming Group (OUSPG) tested the effects of sending modified Setup-PDU's to a number of H.323 implementations. Modified Setup-PDU's are TCP/IP packets that carry the H.225/Q.931 initial signaling information (protocol identifier, source address, called number, etc.) encoded according to ASN.1 PER (Packed Encoding Rules). The H.225 Setup-PDU is an excellent test candidate for several reasons: The Setup-PDU contains many information elements, whose length and type are variable; The Setup PDU is normally the first packet exchanged during H.323 communication; and affected systems can be quickly rebooted for additional testing. OUSPG prepared a test suite containing approximately 4,500 modified Setup-PDUs, and fed these to each tested H.323 device. They found that many systems that implement H.323 are vulnerable to one or more of these malformed PDUs -- affected devices typically crashed or experienced 100% CPU utilization. Another candidate for vulnerability testing is the first of the many H.245 messages - the Terminal Capability Set (TCS) message. The TCS message occurs early in the H.245 exchange so that the calling party can determine the version and capabilities of the corresponding H.245 endpoint. Work is in progress in this area. Vulnerabilities to H.245 have not been announced yet but are anticipated. (Porter, Thomas PhD, 2010)

There are some specific recommendations for securing a VC in an environment. Some of these recommendations are well-known and some maybe difficult to implement, but should be considered. (Porter, Thomas PhD, 2010)

- Keep VC traffic off the network. Segregation is the best option for many reasons, but isn't possible for some networks.
- Use encryption if possible. Sometimes this can be a problem if performance issues are a concern.
- Use VPN's to avoid any packet captures and rebuilding of traffic, or use separate subnets.

- Integrate IDS/IPS signatures for VC traffic. A few have been included below for Polycom system vulnerabilities.
- Use proxy servers in front of firewalls to process incoming and outgoing VC traffic. Performance could be a concern here as well.
- Harden authentications mechanisms with secure passwords.
- Patch VC systems just as any regular device on the network.
- Integrate VC systems as part of the security policy and ensure it follows the same standards as other devices.

3.0 IDS SIGNATURES

Below are a few IDS/IPS signatures that can be used when using Polycom VC systems within a network. These vulnerabilities were published from the Polycom vulnerability list from their website.

Polycom Web Management Interface Directory Traversal

The path traversal vulnerability occurs due to lack of proper input validation on user supplied data. It's possible for an attacker to download "/etc/passwd" using this technique.

*alert tcp $EXTERNAL_NET $POLYCOM_PORTS -> $HOME_NET any *
*(msg: "Possible Exploit of web interface directory traversal"; *
content: "/etc/passwd"; nocase; |
sid:1000007; rev:1;)

Polycom Web Management Interface Command Injection

The command injection vulnerability occurs due to lack of proper input validation on user supplied data.

*alert tcp $EXTERNAL_NET $POLYCOM_PORTS -> $HOME_NET any *
*(msg: "Possible Exploit of web interface command injection"; *

content: |
sid:10000008;rev:1;)

TELNET_POLYCOM_DoS Denial of Service Vulnerability

Key terms to look for in this vulnerability include "password failed, retry"
75 login attempts in 1 minute.

*alert tcp $EXTERNAL_NET $POLYCOM_PORTS -> $HOME_NET any *
*(msg: "Possible EXPLOIT of Polycom Telnet service Denial of Service"; *
content: "password failed, retry"; no case; |
sid:1000001; rev:1;)

TELNET_POLYCOM_BLANK_PASSWORD Vulnerability

Detect when a Telnet session is established that has a blank password. If the Telnet service responds with a, "Hi: My name is".

*alert tcp $EXTERNAL_NET $POLYCOM_PORTS -> $HOME_NET any *
*(msg: "Possible EXPLOIT of Polycom Telnet Blank Password"; *
*content: "Hi: My name is"; no case; *
sid:1000002; rev:1;) (Hass, 2013)

POLYCOM_VIAVIDEO_WEB_SERVER_GET_REQUEST_BUFFER_OVERFLOW Vulnerability (HTTP_VIAVIDEO_OVERFLOW)

Check for an HTTP GET Request which contains an overflow of 4000 or more characters.

Check for an HTTP GET Request which contains an overflow of 256 or more characters.

*alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORT *
*(msg: "Possible EXPLOIT of Polycom VIAVIDEO GET Request Buffer Overflow"; *

*content: ; *
sid:1000003; rev:1;) (Hass, 2013)

The next series of signatures include a way to log any VC calls that may appear unusual but don't warrant an alert and are for more troubleshooting purposes. This will include signatures for H.225, H.245, H.239, and the H.264 protocols.

This alert is to notify that someone is connecting to the Polycom Telnet service.

*alert tcp $EXTERNAL_NET any -> $HOME_NET 24 *
*(msg: "Possible Exploit of the Telnet service"; *
(content: msg:"Someone is logging onto the Videoconference Telnet session";
sid:1000004; rev:1;)

CONCLUSION

Videoconferencing is a very complex technology to implement in your network. Due to the many firewall rules needed, bandwidth availability and QoS requirements, it can also be missed in many security audits. Approaching it from a security standpoint and ensuring any vendors that implement it use the proper recommendations and security policy are crucial to avoiding issues in the future. Using H.323 it is important to understand the protocols involved and how they are used within a Polycom VC system. Understanding their security weaknesses is also important to implement the proper security mechanisms to handle these threats as H.323 continues to be the framework of choice in VC.

When implementing security mechanisms it is important to decide the level of security needed for conference systems. Understanding if the conferences need to be private, then it may be a good idea to use encryption in the H.225 messages. If performance is more important than the privacy of the meeting, then consider using proper firewall and IDS signatures for control. On the basic level though every VC system should use the same security principles as any other network devices since it should be considered a network device as well. Things such as strong password authentication, scheduled patching, restricting management controls from the external interface, restricting telnet access and IDS/IPS signatures are all recommendations for every videoconference system that is in place. Working with ISP's may also help to prevent any possible DoS attacks against your system and restricting who can connect to it via firewall rules is another important element.

In further review, there seems to be quite a few options in penetrating a Polycom VC system. Out of the box, Polycom systems come with external interfaces enabled for management including Telnet and FTP. Locking these services down is essential for creating a first line of defense. Developing policies around securing the protocols used

and the ports needed to make successful connections should also be considered. Determining the privacy of the meetings taking place and what technologies to implement the correct security are also essential in following any security guidelines that are documented. Blocking external interfaces for management and allowing only brokered access for external vendors when they need to login and resolve issues should be also included as part of that. Another consideration is to properly update firmware as schedules such as Firewalls, switches and routers.

REFERENCES

Indiana University Knowledgebase, April 2 2012, http://kb.iu.edu/data/aurw.html

Jones P.E. (2007, April). *Overview of H.323.* Retrieved from http://hive2.hive.packetizer.com/users/packetizer/papers/h323/overview_of_h323.pdf

Schlatter, C. Basic Architecture of H.323, 2003. Retrieved from http://hive1.hive.packetizer.com/users/packetizer/papers/h323/h323_basics_handout.pdf

Polycom (2009, April) *G.719 The first ITU-T Standard for Full Band Audio*, Retrieved from http://www.polycom.com/global/documents/whitepapers/g719-the-first-itut-standard-for-full-band-audio.pdf

Telecommunication Standardization Sector (ITU-T), H.226, 1998, http://www.itu.int/rec/T-REC-H.226-199809-I/en

K20 Education Network, H.239 Protocol and Content Sharing Challenges and Considerations, 10/11/2011 http://www.wa-k20.net/docs/h.239k20infov3.doc

Perumal Mozhi Arul Muthu (2009, Nov) *Call Signaling and Media Stream Packetization for Packet-Based Multimedia Communication Systems*

Rodman, Jeffrey (2008, July) *VoIP to 20kHz: kHz: Codec Choices for High Definition Voice Telephony,*

Retrieved from http://docs.polycom.com/global/documents/whitepapers/codecs_white_paper.pdf

Hass, Paul (2013, Feb) *Polycom HDX Telnet Authorization Bypass,* Retrieved from http://packetstormsecurity.org/search/?q=polycom&s=files

Porter, Thomas PhD (2010, Nov), *H.323 Mediate Voice over IP: Protocols, Vulnerabilities & Remediation*, Retrieved from http://www.symantec.com/connect/articles/h323-mediated-voice-over-ip-protocols-vulnerabilities-amp-remediation

Last Updated: April 26th, 2018

Upcoming Training

SANS vLive - SEC503: Intrusion Detection In-Depth	SEC503 - 201805,	May 02, 2018 - Jun 14, 2018	vLive
Community SANS Virginia Beach SEC503	Virginia Beach, VA	May 07, 2018 - May 12, 2018	Community SANS
SANS Security West 2018	San Diego, CA	May 11, 2018 - May 18, 2018	Live Event
SANS Oslo June 2018	Oslo, Norway	Jun 18, 2018 - Jun 23, 2018	Live Event
Mentor Session - SEC503	Houston, TX	Jun 18, 2018 - Jul 18, 2018	Mentor
Minneapolis 2018 - SEC503: Intrusion Detection In-Depth	Minneapolis, MN	Jun 25, 2018 - Jun 30, 2018	vLive
SANS Minneapolis 2018	Minneapolis, MN	Jun 25, 2018 - Jun 30, 2018	Live Event
SANS London July 2018	London, United Kingdom	Jul 02, 2018 - Jul 07, 2018	Live Event
SANSFIRE 2018	Washington, DC	Jul 14, 2018 - Jul 21, 2018	Live Event
Security Operations Summit & Training 2018	New Orleans, LA	Jul 30, 2018 - Aug 06, 2018	Live Event
SANS San Antonio 2018	San Antonio, TX	Aug 06, 2018 - Aug 11, 2018	Live Event
San Antonio 2018 - SEC503: Intrusion Detection In-Depth	San Antonio, TX	Aug 06, 2018 - Aug 11, 2018	vLive
Community SANS Columbia SEC503	Columbia, MD	Aug 13, 2018 - Aug 18, 2018	Community SANS
SANS Virginia Beach 2018	Virginia Beach, VA	Aug 20, 2018 - Aug 31, 2018	Live Event
SANS Tokyo Autumn 2018	Tokyo, Japan	Sep 03, 2018 - Sep 15, 2018	Live Event
SANS Amsterdam September 2018	Amsterdam, Netherlands	Sep 03, 2018 - Sep 08, 2018	Live Event
SANS London September 2018	London, United Kingdom	Sep 17, 2018 - Sep 22, 2018	Live Event
SANS Network Security 2018	Las Vegas, NV	Sep 23, 2018 - Sep 30, 2018	Live Event
SANS Brussels October 2018	Brussels, Belgium	Oct 08, 2018 - Oct 13, 2018	Live Event
SANS Northern VA Fall- Tysons 2018	Tysons, VA	Oct 13, 2018 - Oct 20, 2018	Live Event
SANS Denver 2018	Denver, CO	Oct 15, 2018 - Oct 20, 2018	Live Event
SANS October Singapore 2018	Singapore, Singapore	Oct 15, 2018 - Oct 28, 2018	Live Event
Mentor Session - SEC503	Ballston, VA	Nov 01, 2018 - Dec 06, 2018	Mentor
SANS Dallas Fall 2018	Dallas, TX	Nov 05, 2018 - Nov 10, 2018	Live Event
SANS San Diego Fall 2018	San Diego, CA	Nov 12, 2018 - Nov 17, 2018	Live Event
SANS Stockholm 2018	Stockholm, Sweden	Nov 26, 2018 - Dec 01, 2018	Live Event
SANS OnDemand	Online	Anytime	Self Paced
SANS SelfStudy	Books & MP3s Only	Anytime	Self Paced