SECURITY OFFICE UPDATE – H.323 and SIP AES Media Encryption –Version 2.0

Security Update Relating to H.323 and SIP AES Media Encryption on Polycom Products

DATE PUBLISHED: February 9st, 2016

Overview

As more video conference calls are conducted over public networks and public environments, the need to deploy security measures to protect the information discussed in the call rises. Conducting video conferences behind firewalls or over ISDN based networks reduce the potential for call tapping, although there is still residual risk. Encryption solutions can assist with call privacy, even when calls are made over the public internet.

This document explains the details of Polycom's implementation of H.323 and SIP Media Encryption using the Advanced Encryption Standard ("AES"), which provides privacy during a video conference call.

Specific details are then also provided for all Polycom® Video endpoint and MCU products.

Standard Encryption

Polycom® products use the Advanced Encryption Standard ("AES") as approved by the National Institute of Standards and Technology ("NIST") for encryption of digital information. When deployed within communication systems, AES ensures that the information discussed within a call is unintelligible to unauthorized parties that may have tapped into the communication system.

AES Media Encryption Technical Notes

- AES media encryption does not change the MTU (Maximum Transmission Unit) size. The endpoint reduces the payload as needed to comply with the configured

MTU. Thus, the media payload within packets in an encrypted call will be smaller than those in an unencrypted call.

- AES media encryption does not introduce any extra latency.
- AES media encryption adds between 0-15 bytes of overhead per media packet.

Polycom® H.323 Media Encryption Implementation

All currently shipping Polycom® H.323 products support media encryption in H.323 calls using the mechanisms defined in H.235v3 (equivalently, per H.235.6), using encrypted RTP with native H.235/H.245 Diffie-Hellman key exchange)[1].

Table 1 shows the specific details of the support by product. All products have "baseline" support; some products have additional support as listed.

Product	AES-128 Support	AES-256 Support
Baseline Support (All Products)	Supported (AES-CBC-128) (DH 1024)	Not Supported
Polycom® HDX® (version 3.1.x or later)	Supported (AES-CBC-128) (DH 1024)	Supported (AES-CBC-256) (DH 2048)
Polycom® RealPresence® Group Series	Supported (AES-CBC-128) (DH 1024)	Supported (AES-CBC-256) (DH 2048)

Table 1 - H.323 Media Encryption Support

See the individual product administrative and user guides for details on how to configure and use H.323 media encryption (administrative and user guides are available at http://support.polycom.com in the "DOCUMENTS & DOWNLOADS" area).

[1] Many Polycom® legacy systems also have the same baseline H.323 media encryption support, including ViewStation EX/FX/VS4000, V500, VSX (all models), MGC (all models).

Verifying secured connections

Polycom® HDX® and Polycom® RealPresence® Group Series endpoints support the display of an “encryption check code”, which can be used to detect whether a Man-In-The-Middle (MITM) attack is underway in an H.323 call. The check code is displayed in the endpoint call statistics in the form of a long hexadecimal number. After an encrypted H.323 call has been established, the user at one end reads the check code out loud while a user on the other end verifies it. If the codes match, the call is secure; if they do not match, the Diffie-Hellman key exchange has been compromised and the call should be considered insecure. See the product user guides for additional details on this mechanism.

Polycom® SIP Media Encryption Implementation

All currently shipping Polycom® SIP products support media encryption in SIP calls per RFCs 3711 (SRTP), 4568 (SDP Security Descriptions for Media Streams) and 6188 (AES-192 and AES-256 usage in SRTP). RFC 4568 key exchange requires the use of TLS as the SIP transport protocol; media encryption is not available when using SIP/UDP or SIP/TCP. Refer to the product administration guides for details on how to ensure that TLS is configured as the SIP transport protocol (configured as part of “Secure Communication Mode” on the RMX; part of the “Local Cluster > Signaling Settings” on DMA; configured as the SIP “Transport Protocol” on Polycom endpoints).

Table 2 shows the specific details of the support by product. All products have “baseline” support; some products have additional support as listed.

Product	AES-128 Support	AES-256 Support
Baseline Support (All Products)	Supported (AES_CM_128_HMAC_SHA1_80)	Not Supported
Polycom® RealPresence® Collaboration Server (RMX®) (version 8.1.4 or later)	Supported (AES_CM_128_HMAC_SHA1_80) (AES_CM_128_HMAC_SHA1_32)	Not Supported
Polycom® HDX® (version 3.1.x or later)	Supported (AES_CM_128_HMAC_SHA1_80)	Supported (AES_CM_256_HMAC_SHA1_80)
Polycom® RealPresence® Group Series (version 4.1 or later)	Supported (AES_CM_128_HMAC_SHA1_80) (AES_CM_128_HMAC_SHA1_32)	Supported (AES_CM_256_HMAC_SHA1_80) (AES_CM_256_HMAC_SHA1_32)

Table 2 - SIP Media Encryption Support

Key exchange is performed in-band over the TLS-secured SIP signaling channel according to RFC 4568[2].

Media Encryption in SIP calls using TIP

Polycom® HDX® endpoints (version 3.0.2 and later) and Polycom® RealPresence® Collaboration Server (RMX®) (version 7.6 and later) also support SIP media encryption in calls using Telepresence Interoperability Protocol (TIP). In addition to the same baseline SRTP media encryption support as documented above, these products include support for the following:

- IMTC TIP version 7.0 (http://www.imtc.org/downloads/IMTC-Members-TIPv7_Implementation_Spec_and_License_2010r00.pdf)
- Cisco TIP Endpoint 1.7 Implementation Profile (http://www.imtc.org/downloads/IMTC-Members-Implementation_License_with_Cisco_1.7_endpoint_profile__2010r00.pdf)
- SRTP-DTLS per RFC 4347, 5764
- Encrypted Key Transport (EKT) per https://tools.ietf.org/html/draft-ietf-avt-srtp-ekt-01

Contact

For additional information regarding Polycom® product security, contact Polycom Technical Support – either call 1-800-POLYCOM or visit:

http://support.polycom.com/PolycomService/support/us/support/documentation/security_center.html

for the latest information. You might also find value in the high-level security guidance and security news located at:

http://www.polycom.com/security

[2] Care must be taken to ensure that TLS signaling is used end-to-end within the SIP infrastructure to protect the key exchange.

Revision History

Revision 1.0 - Original publication

Revision 2.0 – Updated Content and Formatting: February 9th, 2016