Polycom Video Communications

Call Privacy through Polycom Encryption

Author:
Polycom Video Engineering

November 8, 2004
Rev 2.1

POLYCOM

Connect. Any Way You Want.

Call Privacy through Polycom Encryption

As more video conference calls are conducted over public networks and public environments, the need to deploy ample security measures to protect the information discussed in the call rises. In many cases, conducting videoconferences behind firewalls or over ISDN based networks reduce some of the potential for call tapping, although it may not be enough. Encryption solutions can assist with call privacy, even when calls are made over the public internet.

Polycom addresses these issues with the Polycom Encryption Option for the VSX™, iPower™ and ViewStation® EX, ViewStation FX, and VS4000™ products. This application brief explores Polycom's implementation of encryption which offers privacy during a video conference call.

What is AES?

Polycom's Encryption uses AES (Advanced Encryption Standard), which is a set of mathematical algorithms approved by NIST (National Institute of Standards and Technology) for encryption of digital information. When deployed within communication systems, AES ensures that the information discussed within a call is unintelligible to intruders that may have "hacked" or tapped into the communication system.

How does AES work?

When information is encrypted, the sender and receiver exchange a "key" that locks the information. AES currently specifies 3 key sizes, 128, 192, and 256 bits. So if a message is encrypted using an AES key length of 128 bits, this means that there are 2^{128} possible keys that could have been used to code the message, leaving a very large guessing game for any intruder to guess the right key.

How does AES work within a video conference call?

In June 2003, The International Telecommunications Union (ITU) approved H.235 v3, which describes how videoconference systems should incorporate security services for authentication and call privacy using AES.

ITU-T H.235 v3 provides several improvements such as security profiles (simple password-based and sophisticated digital signature), new security countermeasures, support for backend services, but most importantly, support for AES.

Polycom Encryption Implementation:

Polycom encryption is a software add-on option available for older ViewStation EX/FX and VS4000 systems. As of March 2004, all ViewStation EX/FX and VS4000 systems ship with AES software installed. Likewise, all V500, VSX 3000, VSX 7000 and VSX 8000 systems ship with AES software installed. The end user has the option to activate the encryption feature. Polycom encryption fully conforms to both the AES and the ITU-T H.235 v3 standard.

Polycom's encryption is managed through the administration functions of the Polycom V500™, VSX 3000, VSX 7000 and VSX 8000, ViewStation EX, ViewStationFX, VS4000 and iPower systems. A user of an encrypted call will see a small lock icon on their screen showing that the call is encrypted. Both endpoints must have the encryption option selected to activate encrypted operation on calls.

Polycom's encryption can be used in a point to point call, over ISDN or IP based networks. Keys are automatically generated using the Diffie-Hellman algorithm.

Summary

Video conference calls are vulnerable to uninvited intruders as computer networks are to virus attacks and hackers. To ensure that video conference calls are secure, safeguards such as deploying caller password authentication, firewall solutions, and standards based encryption products should be deployed. Illicit monitoring of important meetings can result in exposure of strategic or competitive information and the creation of liability through loss of privacy. Since eavesdropping is difficult to detect, the damage to an organization can continue for long periods of time. A simple and practical method to reduce these risks is to use encryption technology, such as Polycom's Encryption Option.

The Polycom Office™

With integrated video, audio, data, and Web capabilities, The Polycom Office is the only solution that offers an easy way to connect, conference, and collaborate any way you want. Work faster, smarter, and better with The Polycom Office.

Polycom, Inc. develops, manufactures and markets a full range of high-quality, easy-to-use and affordable voice and video communication endpoints, video management software, web collaboration software, multi-network gateways, and multi-point conferencing and network access solutions. Its fully integrated end-to-end solution, The Polycom Office, is supported by the Polycom accelerated communications architecture and enables business users to immediately realize the benefits of integrated video, voice data and web collaboration over rapidly growing converged networks.