



Videoconferencing Security Vulnerabilities

A Discussion of Videoconferencing Security Vulnerabilities

Technical Services Reference

Abstract

This reference discusses the reasons why an organization should use encryption to protect their videoconferencing sessions.

Why Security?

Security is becoming a growing concern for companies as they increase their adoption of videoconferencing. Much of this concern stems from unauthorized people "listening in to private, often confidential business meetings," said Andrew W. Davis, senior analyst and managing partner at Wainhouse Research. Security consists of two basic components: protection of the videoconference system with a firewall or packet filtering device, and protection of the video streams with encryption.

Currently, most government agencies secure their videoconferences – either with commercial-grade encryption, firewalls or their own military-grade encryption depending upon the level of information classification. Many Fortune 500 companies deploy videoconferencing security to every endpoint and at their bridge locations. The major vertical markets using videoconferencing security techniques today are defense and aerospace, automotive, energy, mining and crude oil production, diversified financials, commercial banks, telecommunications, semiconductors, healthcare, pharmaceuticals and consumer food products.

Insecure Infrastructures

Videoconferencing sessions are primarily transmitted using ISDN and IP signaling standards. Each signaling standard has its own set of security weaknesses. The brand and model of videoconferencing equipment used also contributes in a major way to the vulnerability of videoconferencing in general.

Videoconferencing over IP utilizes the TCP/IP protocol—often the Internet as a transmission medium—and can be easily monitored or recorded using any off the shelf packet sniffing tool installed on a computer in the LAN or at a switch. The inherent vulnerability of IP video transmissions traveling over the Internet or a private IP network is linked to the features of the Internet Protocol. There is no other solution than strong encryption for all video transmissions that are proprietary in nature.

To understand some of the vulnerabilities of an ISDN video call, it is helpful to look at the path of an ISDN call. Although the ISDN signal is originally digital, it is soon converted at the phone company's switch. There, it may be converted to analogue for routing over conventional phone lines (pstn) or satellite, where it may be reconverted and sent over a fiber optic network. Once near its destination, it is converted back to digital at a local switch location, where it can be routinely monitored by the owner of the switch. Since ISDN is switched to a variety of formats, it is not inherently safer than any other broadband communications. The path of the information is uncertain, which also is not conducive to maximum privacy. ISDN video calls can also be monitored and recorded with a simple and inexpensive device called an ISDN line tester, like those manufactured by Acterna and Anixter.

Both IP and ISDN video systems are vulnerable to attacks that can give attackers remote control of the videoconferencing device. There have been numerous articles written recently that discuss specific vulnerabilities in the remote management features of the Polycom ViewStation product line, and these vulnerabilities affect many video systems on the market today. Through dial-up management hackers can gain access to the listen command and monitor calls. This type of remote control can also allow unauthorized individuals to gather information about the device, retrieve files, crash the device, or stream the video session to another domain on the Internet.

Service Providers

The fundamental issues that make International communications less secure are the ownership of the telecommunications infrastructure, and the relationship between the telecommunications provider and the government. In many nations, the telecommunications providers are run with a heavy government hand, and are incentivized to route calls through tapped switches and bridges.

Additionally, it is not unheard of for the telecommunications company to operate as a free agent, offering information to the highest bidder. Deutsche Telekom, one of several telecommunications companies providing bridging and telecommunications services for the German government, was responsible for routing a German videoconference via satellite through a major U.S. intelligence center in Denver, Colorado. The German foreign office has meanwhile put plans for videoconferences with overseas embassies on hold. Under investigation by German Secretary of State, Gunter Pleuger, it has been discovered that "for technical reasons" the satellite service was routed via Denver, Colorado. According to a colleague of Pleuger's as quoted in Der Spiegel the German foreign services "might as well hold [their] conferences directly in Langley."

U.S Companies Making International Calls

The majority of commercial enterprises using encryption are U.S. organizations with overseas operations in many countries around the world. Although the security of intra-U.S. conferences is highly questionable, especially since the Patriot Act was passed, the likelihood that an international call will be intercepted by a foreign agency is more likely and potentially more devastating. "If you're with Boeing and you're in France working on a contract against Airbus, you might be concerned about French intelligence listening in [...because] these conversations can be easily monitored, said Bruce Schneier, an encryption specialist.

Concerns over the security of videoconferences are not limited to companies in the aerospace and defense industry. Many of Navastream's customers, previous to their installation of encryption also voiced anxieties regarding the security of their conferencing: An American automobile manufacturer was concerned that the Mexican government was listening to their video conferences into Mexico to learn about plant closings that could injure the Mexican economy; an American photography corporation was concerned that the Japanese government was listening to their conferences into Japan, in order to provide the competition with bid information; an American financial services company was concerned that foreign governments were trying to gain information discussed in video conferences about their clients; an American pharmaceutical company was concerned with the sensitivity of high level meetings conducted via videoconference and the potential for information interception by their competitors.

Conclusion:

Navastream recommends protecting videoconferencing systems connected to the Internet with a gateway product that can provide packet filtering. Encryption and certificate based authentication are also fundamental parts of an overall security policy that protects access to information traveling over public networks. Finally, network administrators should be sensitive to protecting remote management access with the latest security patches available from their videoconferencing manufacturers', while ensuring that all remote administrative functions are protected with either the security of encryption or packet filtering.

About NAVASTREAM:

Navastream is a provider of Managed Security Services (MSS) that develops, markets and supports a comprehensive family of telecommunications security solutions that protect and manage the access, privacy and integrity of information transmitted over local-area networks (LANs), wide-area networks (WANs) and public packet-switched networks such as the Internet.