Security for Videoconferencing

A guide to understanding, planning, and implementing secure compliant ISDN & IP videoconferencing solutions

Wainhouse Research

Security for Videoconferencing

A guide to understanding, planning, and implementing secure compliant ISDN and IP videoconferencing solutions

January 2004
Revised – February 2004

WR
Wainhouse
Research

CRITICOM
Critical Communications

Contents

List of Figures

Executive Summary

For a variety of reasons, many videoconferences that include classified information are not secure. Reasons for these security violations include a lack of understanding of security procedures, and the high cost and complexity of switching between secure and non-secure conferencing modes.

A secure videoconferencing environment requires three key elements;

1) Physical and electrical isolation between the RS-366 (dialing interface) on the codec and on the IMUX.

2) The use of an approved and certified data encryption device on the RS-449/530 (voice, video, and data) interface between the codec and the IMUX.

3) Physical zone security and power isolation, both of which are typically addressed by the local Designated Approving Authority (or DAA).

In the past, switching between secure and non-secure mode has required the support of a COMSEC-certified engineer to complete the necessary re-cabling and often to dial the call directly from the IMUX. This is both expensive and time consuming. Criticom, a Maryland based firm, recently released a solution to this problem in their ISEC secure videoconferencing product line.

The Security Ebb and Flow

In the years since the cold-war era, public and corporate attitudes toward security have varied from indifference to panic. During times of relative tranquility, most people do not give much attention to their personal security or the security of their information and data. Instead, they focus their time, energy, and money on other areas of their lives.

A similar situation exists for many government agencies. Even though certain security activities are mandated by regulations, the level of compliance with these mandates varies with the perceived threat level, and the cost and ease-of-use of security compliance procedures.

However, during times of war, conflict, or other uncertainty, people become acutely aware of their surroundings and the inherent risks of their daily lives. Recent examples include the Gulf War, the terrorist activities of September 11th, and the recent war with Iraq. These events have led many organizations and government agencies to critically re-examine their existing security procedures and policies. Areas of security risk and concern include the control of access to critical information, physical security issues (locking file cabinets, doors, etc.), and background checks on employees and contractors. In addition, new security mandates have forced government agencies to carefully safeguard their sensitive data transmissions.

One of the most prevalent areas of concern remains the transmission of voice, video, and data during videoconference meetings. Although regulations for securing videoconferences were released some time ago by the NSA, many agencies are not operating in compliance with those guidelines. In many cases, the high cost and complexity of available solutions presents a formidable barrier to compliance. Furthermore, some agencies are simply unaware of the need to secure their meetings.

Understanding Videoconferencing Security

In order to properly secure a videoconference meeting, one must be concerned about three key areas; data storage, data radiation, and data encryption.

Data Storage:

The information that flows through a videoconferencing system may contain classified information. By using existing hardware and software solutions, conference attendees can capture and store data for future access and playback. Such data storage, unless tightly controlled, could give unauthorized personnel access to sensitive information and therefore would represent a significant security violation.

Generally speaking, there are two types of videoconferencing systems, or codecs[1], commercially available today; PC-based and appliance. The PC-based type references videoconferencing systems that run PC operating systems and utilize, at least in part, standard COTS PC hardware. Since these systems include internal hard drives and plug-and-play connectivity for external storage devices, one must take additional steps to secure these systems. Specifically, the system must be equipped with a removable hard-drive setup. In addition, two different hard drives must be used; one for secure calls and one for non-secure calls. Finally, the hard drive used for secure calls must be stored in an approved safe. Because securing a PC-based videoconferencing system requires additional cost and work, these systems are not very well suited for secure videoconferencing.

PC-based videoconferencing systems are not considered ideal
for secure videoconferencing applications.

Appliance videoconferencing systems are not based on a PC platform. These devices have been custom designed and manufactured to provide only specific functionality and typically do not utilize standard PC- based hardware or software. In addition, the storage capabilities of these systems are usually limited to storing address book information, usage data, and configuration settings. Since these devices do not provide data storage capabilities, they are a good choice for secure videoconferencing.

Appliance based videoconferencing systems are better suited than
PC-based systems for secure videoconferencing requirements.

Data Radiation and Encryption:

Another area of concern is that confidential information may be electrically radiated by the conferencing equipment. When this occurs, data is susceptible to monitoring and eavesdropping by unauthorized personnel. For example, studies have shown that signals radiating from a video monitor can be picked up as far as one kilometer away. According to the F.A.S. (Federation of American Scientists), this would allow a person to view all of the contents of

[1] According to www.searchnetworking, com, a codec is "an algorithm, or specialized computer program, that reduces the number of bytes consumed by large files and programs." Since videoconferencing systems utilize codecs to **co**mpress and **dec**ompress the audio and video data, these systems are often referred to as codecs.

another person's computer monitor from over ½ a mile away – without being detected.[2] Therefore, to provide a secure videoconference environment, data radiation must be controlled or eliminated.

The NSA has mandated that environments and technology utilized for secure communications must meet COMSEC / EMSEC criteria, which include TEMPEST emission guidelines. Since the details of TEMPEST are classified, only general information about TEMPEST recommendations can be printed in this document. However, according to one source, TEMPEST refers to "… a classified set of standards for limiting electric or electromagnetic radiation emanations from electronic equipment."[3] Within the TEMPEST guidelines are definitions of red and black equipment or circuits. A RED device is one that handles unencrypted information with national security value. Conversely, equipment that handles unclassified information or classified information protected by approved encryption is called a BLACK device. The primary concern is the isolation of data and signals between RED and BLACK devices and connections.

The NSA has mandated that environments utilized for secure communications must meet COMSEC / EMSEC criteria, including TEMPEST guidelines.

Creating a Secure Videoconferencing Environment

In a non-secure environment, the videoconferencing system and the IMUX[4] are connected using two distinct interfaces, as shown in the following diagram. An RS-366 interface handles dialing commands and an RS-449/530 interface carries compressed voice, video, and data information.

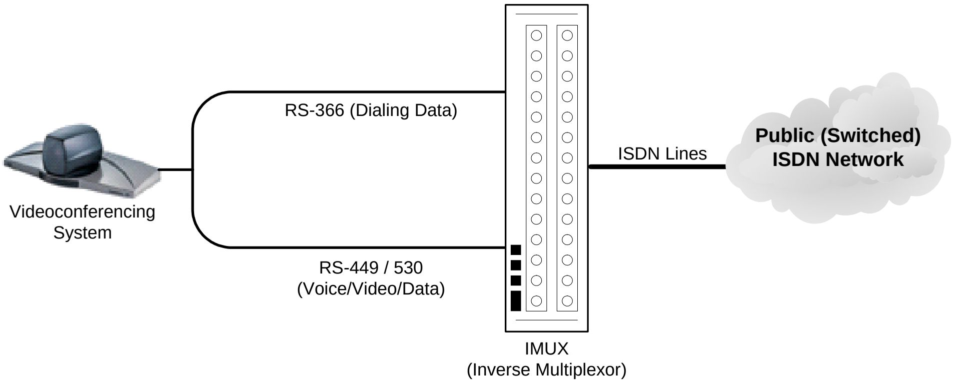
RS-366 (Dialing Data)
Videoconferencing System
RS-449 / 530 (Voice/Video/Data)
ISDN Lines
Public (Switched) ISDN Network
IMUX (Inverse Multiplexor)

Figure 1: A Typical Non-Secure Videoconferencing Setup

The first step toward supporting secure videoconference calls is the installation of an approved encryption device between the codec and the IMUX to encrypt the voice, video, and data information on the RS-449/530 interface. In TEMPEST terms, an encryption device converts RED unprotected signals into BLACK "safe" signals. As illustrated below, in a secure videoconferencing environment, the codec is a RED device, and the IMUX is a BLACK device.

[2] Source: http://www.fas.org/irp/program/security/tempest.htm

[3] Source: http://www.eskimo.com/~joelm/tempestintro.html

[4] In this context, an IMUX, or inverse multiplexer, is the device used to initiate and combine ISDN videoconferencing calls and to combine, or bond, different ISDN data channels.

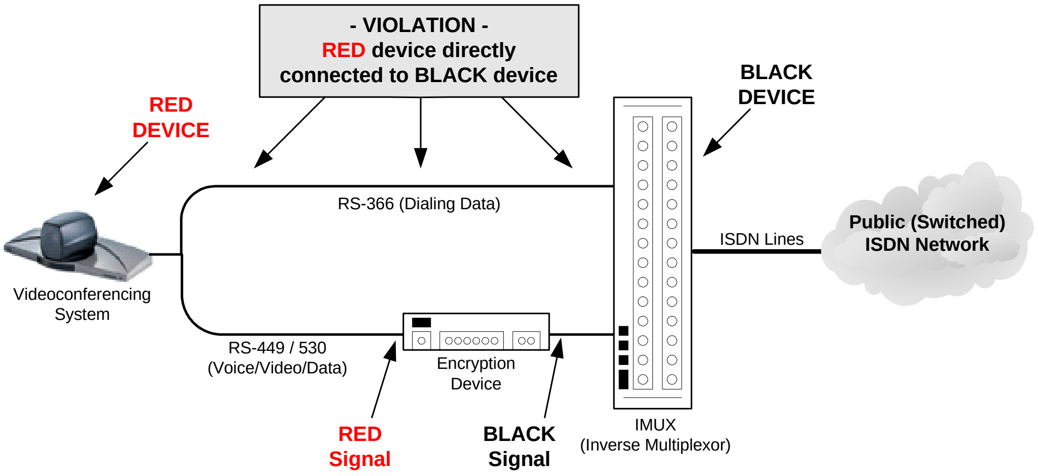
- VIOLATION -
RED device directly connected to BLACK device
RED DEVICE
BLACK DEVICE
RS-366 (Dialing Data)
ISDN Lines
Public (Switched) ISDN Network
Videoconferencing System
RS-449 / 530 (Voice/Video/Data)
Encryption Device
RED Signal
BLACK Signal
IMUX (Inverse Multiplexor)

Figure 2: A Partially Secure Videoconferencing Setup

The problem with the above configuration is that the dialing interface (RS-366) connection between the codec and the IMUX violates COMSEC/TEMPEST guidelines because the copper in that cable may act as an antenna and broadcast or pickup classified information.

Securing the RS-366 Dialing Interface

Typically, videoconferencing users place their calls using the conferencing system's remote control and an "on-screen" menu system. The call request is then sent from the codec to the IMUX through the RS-366 dialing interface. As shown in the prior figure, this is a security violation due to the direct connection between the RED device (codec) and BLACK device (IMUX). There are only two NSA approved solutions for this problem:

Solution 1 - Dialing from the IMUX

With appropriate training, a knowledgeable technician can dial calls directly from the IMUX, thereby negating the need for the RS-366 connection between the two devices. Once the RS-449 connection is eliminated, as illustrated below, this solution meets NSA guidelines. However, this complicates the dialing process, and since IMUXes are often located in remote locations, may involve additional coordination with technical support personnel.

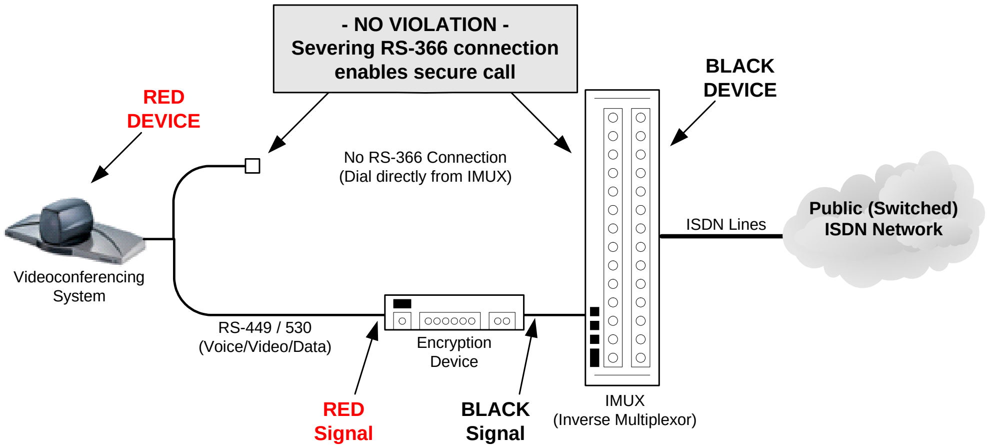
- NO VIOLATION -
Severing RS-366 connection enables secure call
RED DEVICE
BLACK DEVICE
No RS-366 Connection (Dial directly from IMUX)
ISDN Lines
Public (Switched) ISDN Network
Videoconferencing System
RS-449 / 530 (Voice/Video/Data)
Encryption Device
RED Signal
BLACK Signal
IMUX (Inverse Multiplexor)

Figure 3: A Secure Videoconferencing Setup (Dialing From the IMUX)

Solution 2 –Utilizing an Optical Dial Isolator

Optical dial isolators convert RS-366 interfaces into optical light streams that are invulnerable to electronic eavesdropping. Assuming an approved optical dial isolator is used, this solution should meet security guidelines. In addition, this has the added benefit of allowing end-users to place their calls using the on-screen menu systems for both secure and non-secure calls.

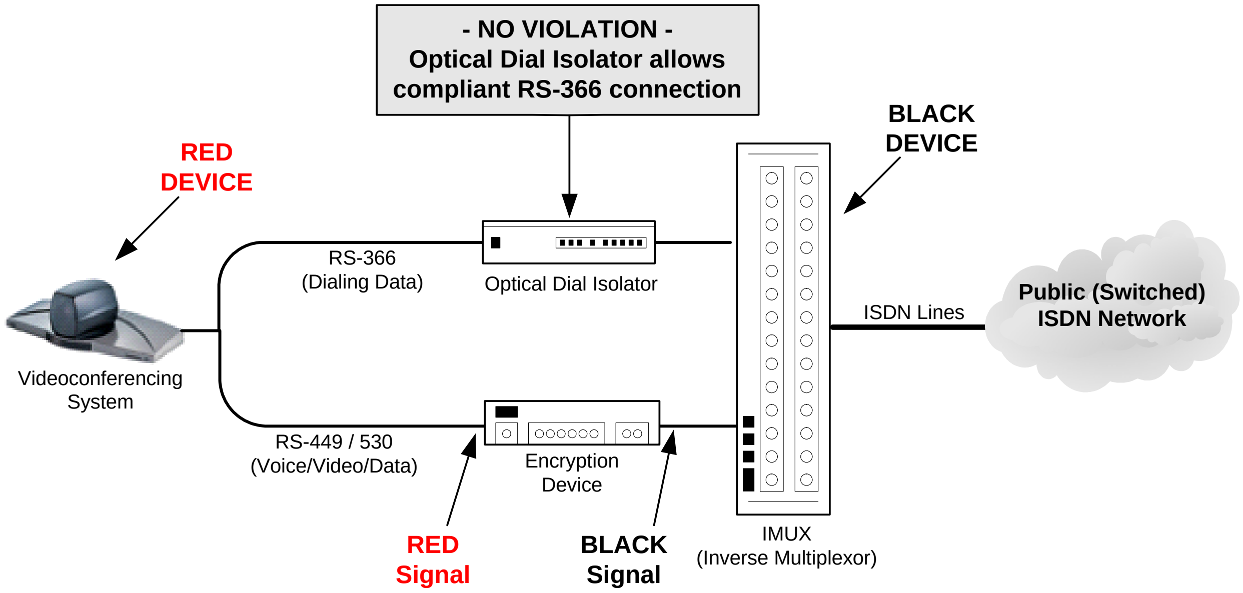

Figure 4: A Secure Videoconferencing Setup (Dialing From the Codec Menu)

The Current State

Many organizations and government agencies need to conduct both secure and non-secure video calls. For example, a government agency may make secure internal (agency to agency) video calls, and non-secure calls to contractors, suppliers, or other government agencies. In addition, after the terrorist activities of September 11th, 2001, many agencies were re-classified to support homeland defense efforts, and as such were mandated to support secure conferencing for classified briefings and situation management. As discussed, switching from secure to non-secure mode requires that a COMSEC certified technician make cabling changes and often dial from the IMUX.

The A/B Printer Switch

In an attempt to avoid frequent re-cabling while switching between non-secure and secure conferences, some organizations have installed inexpensive A/B printer switches. By integrating two A/B switches and an optical dial isolator, organizations can switch between encrypted and de-encrypted modes without the need to disconnect any cables. In addition, this allows all calls to be dialed from the codec's user interface. The illustration below shows a typical A/B switch box solution.

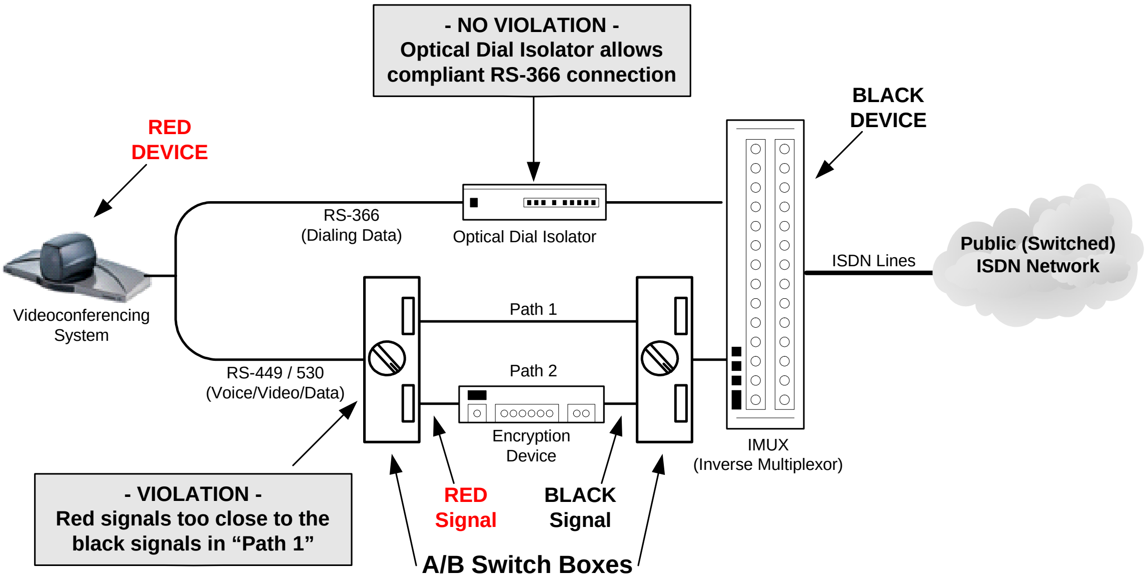

Figure 5: Typical Non-Compliant A/B Switch Box Setup

However, for many reasons including the close proximity of RED and BLACK signals within the device, some A/B switch boxes do not meet signal isolation guidelines. The danger here is that the use of non-certified and untested A/B switches may give users a false sense of security and the inaccurate perception that proper signal separation is in place. Therefore, regardless of the switching device utilized, users should understand that only tested, approved, and certified devices are guaranteed to meet RED/BLACK separation and signal isolation guidelines.

The Criticom Solution

In order to provide failsafe protection, a secure videoconferencing solution must possess the following five key elements; ease of use, optical dialing isolation, successful COMSEC/TEMPEST compliance testing and certification, off-the-shelf functionality, and ease of integration. Criticom, a leading provider of secure videoconferencing solutions, has addressed these issues with the release of the ISEC (Integrated Secure Encryption Console) line of products.

The DI-366 Optical Dialing Isolator

The first piece of the ISEC solution is the DI-366. This TEMPEST Level 1 tested and certified optical dial isolator enables secure endpoint dialing in classified environments. The DI-366 provides the required isolation between the red side (codec) and the black side (IMUX) of the dialing circuit through an optical coupler. By routing the dialing signals through this optical coupler, there is no physical or electrical connection between the codec and the IMUX.

The DI-366 allows end-users to dial both secure and non-secure videoconference calls from the "on-screen" user interface of the videoconferencing system, thereby greatly simplifying the dialing of video calls. To avoid compromising security guidelines, the DI-366 is manufactured in the USA only. The DI-366 can be used independently or in conjunction with other Criticom ISEC products.

The ISEC-320 Videoconferencing Switch

Many seemingly secure meetings are not entirely secure due to the complexities involved in activating the secure conferencing mode. In some cases, activating secure mode requires dialing directly from the IMUX, disconnection of cables and connectors, or a COMSEC certified technician. Alternatively, and quite frequently, non-compliant A/B switch boxes are used to simplify the activation of secure mode. The ISEC-320 is, as of this writing, one of the only approved secure / non-secure videoconferencing switches. The figure below illustrates a typical ISEC-320 videoconferencing setup in secure mode.

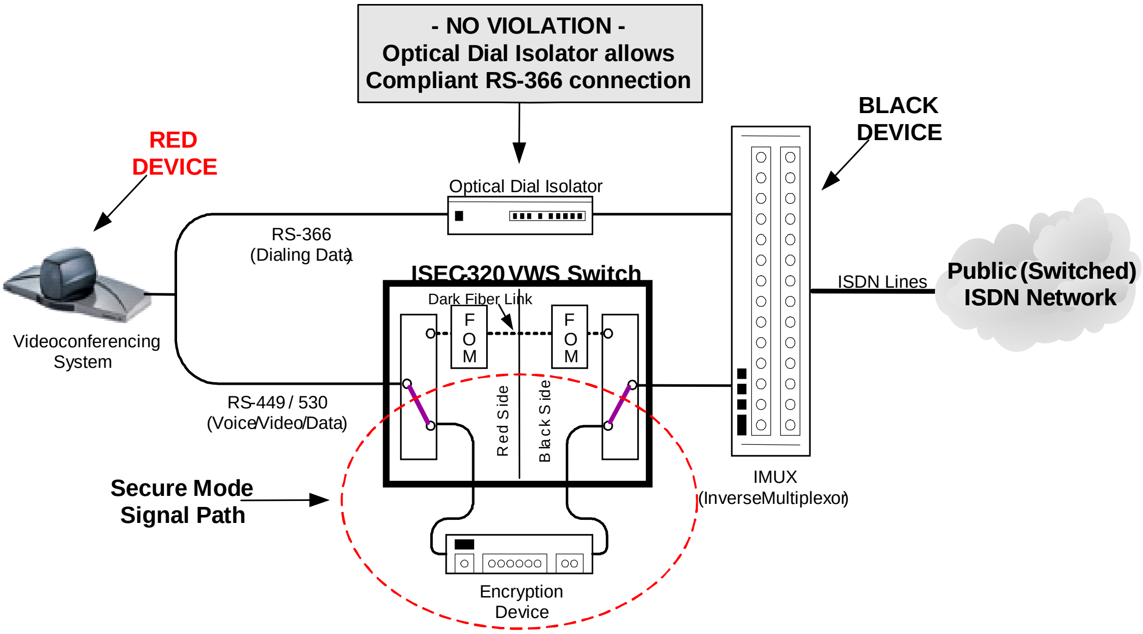

Figure 6: ISEC-320 in Secure Mode

When in secure mode, the ISEC-320 provides two key functions; TEMPEST certified red/black isolation between the codec and the IMUX, and routing of signals through an external encryption device (as shown in the dashed red circle). To ensure appropriate security for classified meetings, the ISEC-320 defaults to secure mode. In fact, while in secure mode, the ISEC-320 switch is actually powered-down, resulting in a total isolation between the red and black sides of the switch box. Conversely, while in non-secure mode, the two optical modems (labeled FOM in the diagrams above and below) in the switch box are powered-up and the fiber-optic link becomes the only path between the red and black sides of the switch box. This fail-safe functionality is a fundamental part of the ISEC-320's COMSEC/TEMPEST compliance.

To switch from secure to non-secure mode, users simply flip the ISEC table-top control switch and dial their call using the videoconferencing system's on-screen dialing menus. Flipping this control switch re-routes the signals as shown in the diagram below:

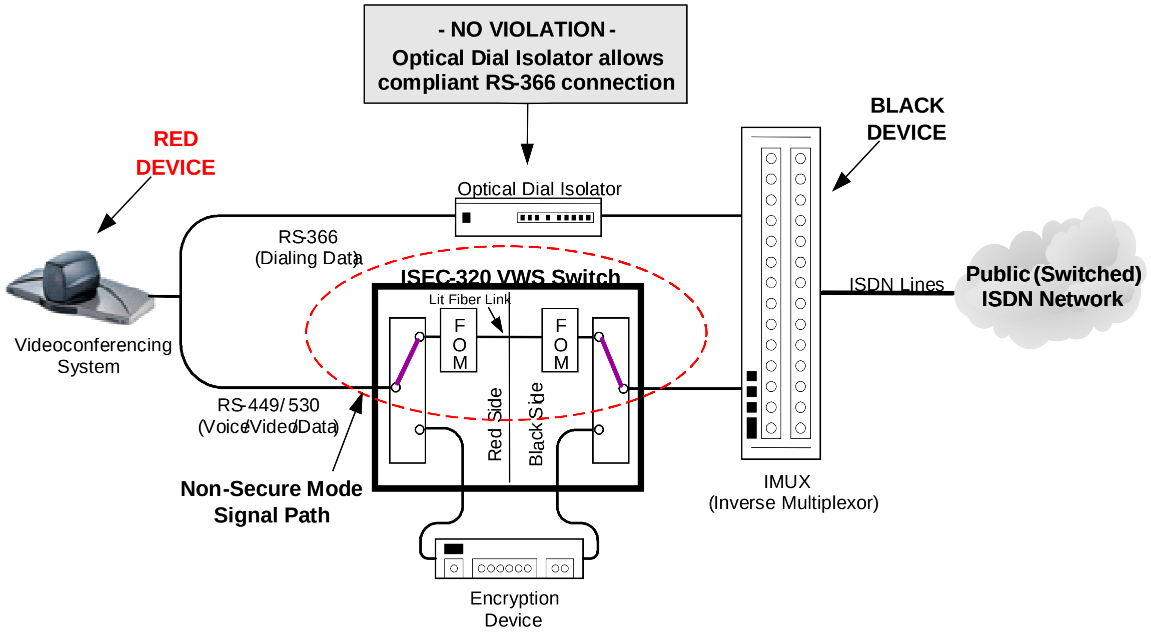

Figure 7: ISEC-320 in Non-Secure Mode

As illustrated in the last two diagrams, the ISEC-320 allows users to easily choose between secure and non-secure conferencing modes – without the need to change cabling or deploy a COMSEC technician. The ISEC-320 has been tested and independently government-certified to TEMPEST-Level 1 for Zones A, B, C, and D[5].

The ISEC-STS Secure Teleconferencing System

The ISEC-STS is the first secure/non-secure RS-530-based videoconferencing solution to be TEMPEST tested and certified. Each ISEC-STS system includes the following items:

- A full-featured TANDBERG videoconferencing codec
- Choice of display devices (up to 60" diagonal)
- Criticom ISEC-320 videoconferencing switch
- Criticom DI-366 optical dialing isolator
- Integrated IMUX (Adtran, Madge/Initia or Ascend)
- Specially designed roll-about furniture housing all equipment

After adding the appropriate encryption device (KIV-7 or KIV-19), ISEC-STS users can enjoy easy to use, secure and non-secure videoconferencing. In addition, the ISEC-STS can also be used with any IP encryptor, such as the KG175 TACLANE, KG235, KIV21 or KG 250 for secure, IP-based videoconferencing.

[5] Based on emissions testing including EMSEC TEMPEST / 1-92 Level 1 in U.S. Air Force Tempest testing labs.

The Next Wave – Secure IP

There are many reasons why organizations are migrating ISDN-based videoconferencing traffic over to IP networks, including:

- Increased reliability
- Enhanced performance
- Easier device and network management
- Potential cost-savings

Military networks, such as DISA's GIG-BE network, will help facilitate the deployment of IP-based videoconferencing throughout the military. Furthermore, although NIPRNET[6] and SIPRNET[7] are not viewed as ready to host videoconferencing today, network upgrades and low-bandwidth videoconferencing protocols promise to resolve this situation in the near future.

The ISEC-VWS-IP Secure IP-Based Teleconferencing System

As the deployment of IP-based video progresses, the need to switch between secure and non-secure IP-based videoconferencing will increase. To that end, Criticom has released the ISEC-VWS-IP switch utilizing the same approved and certified technology as the ISEC-320. As with the ISEC-320, users simply flip the control switch to change from secure to non-secure mode and can dial using the video system's on-screen dialing menu. Through the use of fiber-optic isolation, the ISEC-VWS-IP provides TEMPEST tested red / black signal isolation and is compatible with all Ethernet encryption devices including the KG-175 TACLANE product line.

The ISEC-VSW-IP provides the secure, IP-based videoconferencing demanded by DAAs and COMSEC personnel.

Conclusion

The recent terrorist activities and the global focus on security have increased the interest in secure videoconferencing. While legacy secure videoconferencing solutions were both inconvenient and complex, Criticom's ISEC product line has made switching between secure and non-secure conferencing as simple as flipping a switch. By negating the need for dedicated technical support for secure videoconferences, Criticom has brought secure videoconferencing within the reach of virtually all government agencies.

[6] NIPRNET stands for the Non-Classified Internet Protocol Router Network. Created in 1995, NIPRNET consists of a network of government-owned IP routers used to exchange sensitive information.

[7] According to the FAS (www.fas.org), SIPRNET stands for the Secret Internet Protocol Router Network, a secure network acting as the core of our war fighting command and control capability.

Glossary of Terms

Codec –	Device that compresses and decompresses audio and video data. Videoconferencing systems are often referred to as codecs.
COMSEC –	Communications security
COTS –	Commercial “off-the-shelf”
DAA –	Designated Approving Authority
DISA –	Defense Information Systems Agency
DoD –	Department of Defense
EMSEC –	Emanations security
IMUX –	Inverse multiplexer
NIPRNET –	Non-classified Internet Protocol Router Network
NSA –	National Security Agency
RS-366 –	The dialing interface on a videoconferencing device (codec) or IMUX
RS-449 / 530 –	The voice, video, and data interface on a videoconferencing device (codec) or IMUX
SIPRNET -	Secret Internet Protocol Router Network
TEMPEST –	The widely recognized and classified set of standards for electric or electromagnetic radiation emanations from electronic equipment and other communication devices.

About Wainhouse Research

Wainhouse Research (http://www.wainhouse.com) is an independent market research firm that focuses on critical issues in rich media communications, videoconferencing, teleconferencing, and streaming media. The company conducts multi-client and custom research studies, consults with end users on key implementation issues, publishes white papers and market statistics, and delivers public and private seminars as well as speaker presentations at industry group meetings. Wainhouse Research publishes *Conferencing Markets & Strategies*, a three-volume study that details the current market trends and major vendor strategies in the multimedia networking infrastructure, endpoints, and services markets, as well as the segment report *Video Communications Management Systems,* the free newsletter, *The Wainhouse Research Bulletin,* and free e-zine, *ConferencingBuyer*. To learn more about conferencing, collaboration, and networking, please review other white papers and documents available from Wainhouse Research at http://www.wainhouse.com.

About the Author

Ira M. Weinstein is a Senior Analyst and Consultant at Wainhouse Research, and a 13 year veteran of the conferencing, collaboration and audio-visual industries. Prior to joining Wainhouse Research, Ira was the VP of Marketing and Business Development at IVCi, managed a technology consulting company, and ran the global conferencing department for a Fortune 50 investment bank. Ira's current focus includes IP video conferencing, network service providers, global management systems, scheduling and automation platforms, ROI and technology justification programs, and audio-visual integration. Mr. Weinstein holds a B.S. in Engineering from Lehigh University and is currently pursuing an MBA in Management and Marketing.. He can be reached at iweinstein@wainhouse.com.

About Criticom

Criticom, headquartered in Lanham, Md., is a leading integrator of video and video conferencing equipment for complete video solutions to both government and commercial customers. Founded in 1990 and privately held, the company has earned an outstanding reputation for its video systems and integration expertise — including secure video network design and infrastructure analysis. Criticom has partnerships with the leading manufacturers of video systems and telecommunications equipment, including Tandberg; Polycom; Radvision; VCON; Adtran; VTEL; Cisco Systems, Inc. and General Dynamics. Some of Criticom's many long-standing government customers include the U.S. Central Command, 5th Army, 82nd Airborne, 3rd Army, Army 4th ID, Army National Guard, Air National Guard, Air Reserve Command, Metropolitan DC Police, White House Communication Agency (WHCA), FBI, INS, NSA, Defense Threat Reduction Agency (DTRA), Army Operations Center, Defense Nuclear Agency.   Criticom also serves commercial clients including Titan; Unisys; Lockheed Martin; Northup Grumman; CSC; SAIC; Sony Music Corporation of America; United Way; and the World Bank.

In 2002, Criticom announced the availability of its own-patented product: the ISEC-320, a TEMPEST-tested and certified secure/non-secure switch solution specifically designed for videoconferencing. As of this writing, the CritiCom signature ISEC product is the only secure/non-secure videoconferencing solution utilizing fiber-optic switching technology for conclusive, Type 1 security, enabling classified communications to Top Secret and above. To date, DoD customers have accepted and installed ISEC at more than 35 agencies and locations.

Frequently honored with regional *Washington Technology* "Fast 50" and national *Inc. 500* awards for its fast growth and success, Criticom has achieved consistent financial and employee growth throughout its 14-year history.

Additional information about Criticom can be found on the company's Web site: http://www.criticom.com