Systems and Network Analysis Center
Information Assurance Directorate

Video Teleconferencing

What is Video Teleconferencing?

Video Teleconferencing (VTC) is a communication technology that permits users at two or more different locations to interact by creating a face-to-face meeting environment. VTC systems transmit bi-directional audio, video and data streams during the session. Usage of VTC has expanded beyond corporation boardroom meetings. The demands for collaboration tools and converged infrastructure have boosted VTC usage in recent years. VTC has been gaining popularity in all government sectors including tactical and non-tactical environments.

Type of VTC Systems

The two basic types of VTC systems are the *dedicated* systems and the *desktop* systems. The desktop systems are add-ons to existing PCs. They generally consist of a microphone, speakers, and camera, but may also include a PC add-in card. Dedicated systems have all the necessary components to process the VTC sessions within a single console. This document will focus on these dedicated systems.

The categories of dedicated VTC systems cover different operational environments. A large group system supports large meeting rooms or auditoriums, is fixed to the room, and is non-portable. The second category is the small group system. A small group VTC is designed to support small meeting rooms, is fixed to the room, is non- portable, and is normally more economical to deploy. The third category of dedicated VTC system is the individual system. These individual systems are designed to be portable single user solutions with integrated camera, speakers, and microphone in a compact unit.

Common components in a standard VTC network are *Call Server*, *Video Endpoint*, *Multipoint Conference Unit (MCU)*, *Gateways*, and an Ethernet switch. A *Call Server* performs the registration and call control processing functions. *Video Endpoints* are devices from which users make and receive video calls. The endpoint processes the bi-directional audio, video, and data streams and interfaces to the users. The *Multipoint Conference Unit* and the *Gateways* will be discussed in later sections.

VTC Network Protocols and Architectures

Standard voice and video protocols used on VTC systems today are the Session Initiation Protocol (SIP), H.320, and H.323.

Hardware or software components that execute the compression of signals are called Coder/Decoders or CODECs. A CODEC is also used to convert between analog and digital formats.

Point-to-Point is the most basic architecture configuration for a VTC network. This configuration does not require a Call Server and does not allow conferencing of more than two endpoints, but it does allow for direct video and audio calls between endpoints within a cluster. Figure 1 below depicts a point-to-point network.

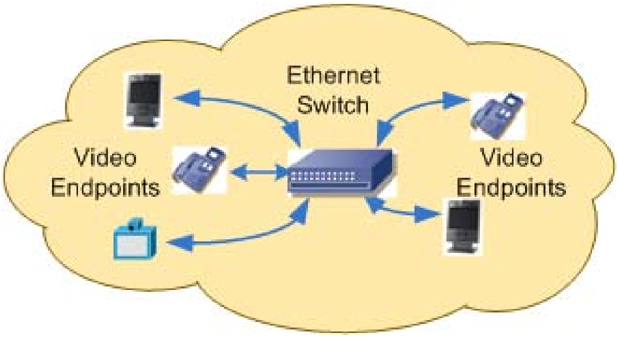

Figure 1: Point-to-Point Conferencing Network

In a Multi-party VTC network architecture, a *Multipoint Conferencing Unit* is required. The MCU makes conferencing possible by acting as a bridge that interconnects calls from three or more *Video Endpoints*. It can be a standalone hardware device, but some dedicated VTCs have embedded MCU functions. Figure 2 illustrates how the MCU facilitates video teleconferencing sessions by processing call control signals and the audio, voice, and data streams to connect the multiple endpoints. It also allows endpoints using different CODECs to participate in the same VTC session.

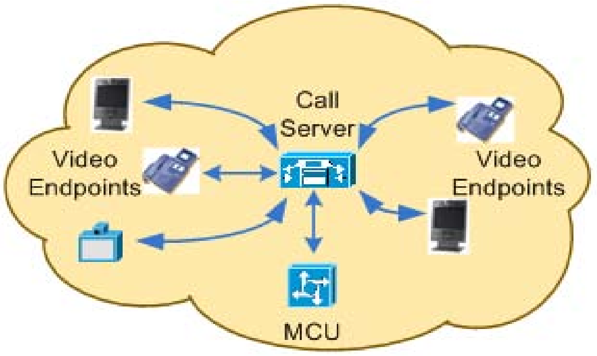

Figure 2: **Multi-party Conferencing Network**

A *Gateway* is required in order for VTC endpoints to communicate with the Public Switched Telephone Network (PSTN) or a legacy network. A Gateway is a standalone hardware device that provides access to other larger IP networks and/or circuit switched telephone networks like the PSTN. Figure 3 shows an IP based VTC network communicating with endpoints on a legacy network. Type 1 external encryption devices like the KIV might be implemented for network link encryption are also shown in Figure 3.

What are the Vulnerabilities?

Due to the valuable benefits and user-friendly set up procedures of VTC systems, many locations have implemented VTCs without applying security best practices. When default settings remain unaltered, unauthorized users can exploit the VTC through the Web interface or other IP management services such as Telnet and File Transfer Protocol (FTP). Unauthorized users can exploit the following security vulnerabilities: participate in VTC sessions, upload malicious code to initiate Denial of Service (DoS) attacks, take control of the far-end camera, record audio and video streams, take snapshots of participants during the session, establish a new session for eavesdropping, use the system as a jumping off point and a hiding place to exploit other systems, and edit configurations to enable additional features (e.g., Microphone, Remote Streaming).

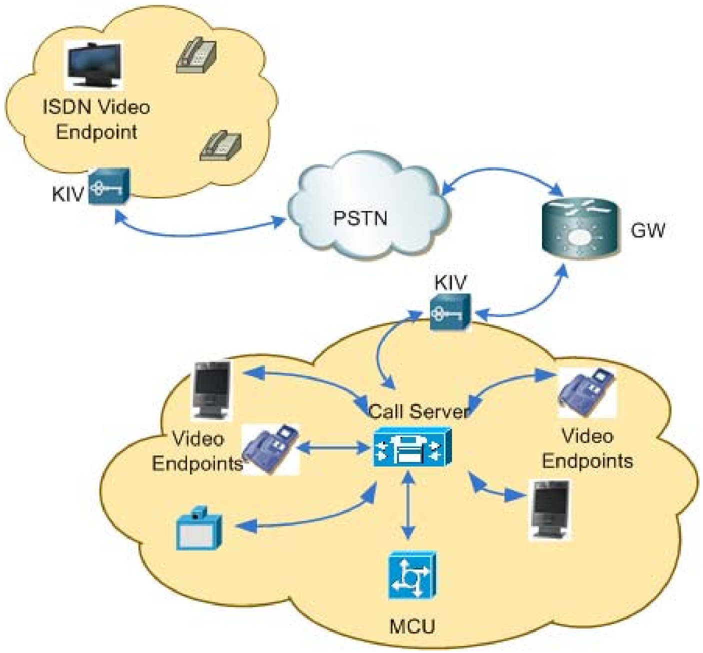

Figure 3: Interoperability with Legacy Network

What Can Be Done?

To mitigate those vulnerabilities, the following actions can be taken:

- Change all default passwords
- Apply best password security practices
- Enable encryption for the VTC sessions
- Disable broadcast streaming
- Disable the far-end camera control feature
- Disable insecure IP services (e.g., Telnet, HTTP)
- Perform initial VTC settings locally using the craft port or the menu on the system
- Regularly update firmware and apply patches
- Practice good physical security (i.e., restrict access, turn off the device, and cover the camera lens when not in use)
- Disable any auto answering feature
- Disable wireless capabilities
- Separate VTCs logically from the rest of the IP network using Virtual Local Area Networks
- When remote access is absolutely required, institute strict access controls (e.g., router access control lists, firewalls rules) to limit privileged access to administrators only