SECURITY RISK MITIGATION IN A MULTI-DOMAIN AUDIO VISUAL ENVIRONMENT

September 26, 2013

Submitted by:
Freeport Technologies, Inc.

Point of Contact:
Federal Sales
571-262-0400
Sales@FreeportTech.com

TABLE OF CONTENTS

1. Introduction

Freeport Technologies employs a variety of methods to ensure security requirements are properly defined and addressed throughout the design, configuration, and implementation phases of multi-domain AV systems.

Policy & Procedure Development – A set of policies and procedures is developed in order to classify all audio visual resources and functions of the system.

Source Management, Isolation & Distribution – A system design is created using key hardware components which provide the proper level of isolation and control of all resources and functions.

System Configuration – The system software is configured to enforce the agreed upon policies and procedures developed in the first phase and then deployed in the system design.

Functional Testing & Verification – A test and acceptance document is developed which provides a step by step process of testing and verifying that the system is functioning as intended, with the proper security policies and procedures in place.

In addition, Freeport has developed several AV products that were specifically designed to effectively manage security risks and to reduce overall implementation costs. These products and the risks that they are designed to mitigate are described below.

2. Enterprise Room Control Alleviates Source Management and Environmental Risks

Freeport's AV system software Enterprise Room Control (ERC) was developed using an object-oriented programming language (Microsoft C#). It was designed as a simplified and modern software platform which provides scalability and maintainability in an environment that has been historically limited in both of these areas by proprietary AV programming languages. ERC provides built in security modeling; providing the ability to address specific functional requirements and enforce security policies without custom programming.

The majority of AV room implementations with multi-domain video conferencing requirements require the integration of multiple classifications of AV source inputs (workstations, cameras, media players, TV tuners, streaming devices, external video and audio feeds, etc). These sources are typically utilized to present content (audio and video) locally in the room as well as to the far side participants of a video conference. **Source Management Risks** arise when the AV system has the potential to display or transmit content from *Network A* (highest classification) locally or to far side participants that are cleared or operating on *Network B* (lowest classification). The AV hardware components required to mitigate **Source Management Risks** must be part of detailed system design that provides the ability to enforce a set of policies and procedures which are driven by the AV system software. ERC ensures that these policies and procedures are enforced to protect the security of the information being presented and distributed via the AV system.

AV room systems operating at multiple security classifications generally require the end user to select the desired system classification at which they wish to operate prior to being able to access a specific functionality of the system. **Environmental Risks** can arise when the AV system software is unable to properly address the physical and visual aspect of the space in which it is being operated. End users must be visually aware of the current classification of the system, and all potential information (audio, video) that can be consumed by outside persons and/or participants must be properly secured. ERC provides the ability to display the desired classification of the AV system throughout the interior (touch panels, LED signage) and exterior (LED signage) of the room. It also ensures that the transmissions of video signals to specific display devices have been properly enabled or disabled.

ERC provides **built-in configuration tools** that apply a variety of security related principles in relation to the system design and functional requirements of the AV

system. When applied, these configuration tools have the potential to eliminate **Source Management** and **Environmental Risks**. These configuration tools include:

Access Control – Multiple end user accounts can be created with varying levels of access to specific room sources and functions when logging into the user interface.

Password/PIN Protection – Specific areas and functions of the user interface can be restricted using password/PIN protection.

Mode Selection – The system can be configured around a set of room modes (Presentation Mode, Audio Conference Mode, Video Conference Mode), all of which can be assigned varying levels of classification (Unclassified, Secret, Top Secret, etc).

Source & Destination Classification – All sources (workstations, media players, etc) and destinations (displays, video codecs, recorders, etc) can be assigned a specific classification level in order to provide or restrict access to them.

3. Multi-Domain Video Network Switch Eliminates Data Tunneling Risks

The Freeport Multi-Domain Video Network Switch (MDVNS) permits a single video CODEC to be utilized on up to nine IP networks of varying security classifications. The MDVNS meets all current DISA requirements and future requests as detailed in the STIG dated January 2008. The MDVNS is the only secure VTC switching solution that has been approved by the Defense Intelligence Agency for use on the JWICS top secret network. It has also been approved for operation by DISA for NIPR and SIPR, NRO, NGA, Coalition Forces, and many other classified networks.

Access to multiple video communication networks using the same AV room system provides the ability to maximize building resources (conference rooms) while reducing hardware component costs. A typical AV room system design with a multi-domain VTC requirement revolves around the use of multiple video CODECs (one per network). Since video codecs are actually very fast special purpose computers and the AV system controller is a slower special purpose computer, the AV control system is more than capable of creating **Data Tunneling Risks**. Tunneling provides the means of going "through" existing legitimate equipment and connections in order to make "illegitimate" connections from a lower to a higher network.

In an environment where a single video codec is used to support multiple video communication networks, **Data Tunneling Risks** can be eliminated. A system design based on a single video codec utilizing a multi-domain switching system alleviates most of the security requirements involved with the sharing of AV resources (inputs, outputs, control) as well. It also relieves the high cost associated with purchasing multiple codecs, and if implemented correctly, provides an automated set of procedures to traverse those networks thus eliminating manual errors while maximizing data security.

The MDVNS design approach ensures electrical and data isolation between all networks. Data isolation is achieved through the use of multiple processor and memory units, where each unit is dedicated to a particular network. Data from a particular network is never stored in more than one place and data from different networks is never intermingled into one processor and memory unit. An extensive test program has been constructed to ensure that the security features operate correctly. Electrical conductivity measurements are performed between the different system elements to make sure that all paths between them are "open". A test program that utilizes every codec setting is used to ensure that every single setting is being cleared and managed.

The periods processing procedures that conform to the current DISA STIG, combined with the Freeport MD-VNS hardware, ensure that all security requirements are met during the switching and operational processes. The Freeport approach satisfies all IA requirements with any bending of the rules. The switching process is made as transparent as possible.

4. Room Control Isolator Mitigates Residual Data Risks

Freeport has developed a hardware device that provides the means to program and control AV system components (video codec, displays, etc) without exposing any data that might be contained in them or on the network to which they are connected. Freeport's Room Control Isolator (RCI) prevents the AV control system from permanently inheriting the security classification of the network that specific AV components are connected to. The RCI addresses room control security issues without modification of existing system designs, it is manufacturer neutral, and it can be used with any type of control device.

When the AV control system has unrestricted bi-directional access to the network through which system components are connected, it has the ability to draw data from that connected network and store it. In a multi-domain environment this creates **Residual Data Risks**. Traditional AV system designs provide the AV control system with the ability to retrieve data from one network and pass it over to another network; even if connectivity to both networks is not happening simultaneously. Mitigating **Residual Data Risks** can be accomplished by isolating the connection between the AV control system and any system components that will be connected to active networks. This isolation must ensure that the AV control system can properly communicate with all connected components while restricting the information that flows back.

The Freeport RCI provides the ability to send commands from an AV room controller to an AV component via RS-232 while restricting the information that flows back. It utilizes a two-way serial communication path with the component but only a one-way serial communication path, plus status, back to the AV room controller. The RCI provides optical and relay air gap isolation between the room controller side of the isolator and the codec side of the isolator. It is built as two independent circuits, one circuit communicates with the AV room controller and the other circuit communicates with the specific component. Each circuit has its own power supply and the two circuits are totally isolated.

The result of incorporating a Freeport RCI in a multi-domain system design is that the AV room controller does not have access to sensitive or classified information stored on any connected AV components and therefore does not inherit the security level of any network that those components are connected to. This allows the same AV room controller to be used to control components that are used across multiple networks while conforming to standard IA policy.