FREEPORT TECHNOLOGIES

An Overlooked Vulnerability

Security Risk Mitigation in a Multi-Domain Audio Visual Environment

Much attention of late has been given to insider threats and to shoring up network security in the Intelligence Community (IC), yet one of the great vulnerabilities left for America's enemies to exploit is access to classified information via Audio Visual (AV) channels. With current budget cuts and travel restrictions, along with a push to share more information among various agencies, the demand to provide video conferencing access to multiple domains in a single location is rapidly increasing. While video access to both of the primary networks (NIPR, SIPR) has been common for some time, there has been a recent increase in demand to include separate and/or dedicated SCI networks (e.g. JWICS) within the Intelligence Community (IC) and to provide access to traditionally isolated networks dedicated to specific agencies (e.g. FBI).

Most Information Systems Security Managers (ISSM) are familiar with the security risks that exist in deploying and configuring workstations, routers and servers in a secure environment. Security personnel have been trained to properly address and mitigate those risks and have numerous tools to assist them in managing them.

Notably however, the security risks that are associated with AV and video conferencing implementations (control systems, video codecs, digital audio signal processors, etc) have not received the same degree of attention as the comparable IT risks. These AV security risks are not as well understood by ISSM personnel and have not been properly documented and defined. This lack of understanding is compounded by current budget pressures to focus on the tangible cost reductions than it is to evaluate the potential AV security risks. The result is that IC systems remain vulnerable to exploitation via AV channels.

There are several areas of risk that exist in a multi-domain AV environment that are likely being considered by America's most sophisticated adversaries.

These risks include the following:

A. *Source Management Risks*: the potential to display or transmit content from *Network A* (highest classification) to local or remote participants that are cleared/operating on *Network B* (lowest classification)

B. *Data Tunneling Risks*: utilizing an AV system controller to create data connections from one network domain to another via industry standard bi-directional data paths

C. *Residual Data Risks*: 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

D. *Environmental Risks*: broadcasting local material that is not appropriate for the current security level of the meeting or remote participants