Secure KVM Technology for Government and Military Desktops

Introduction

Since the advent of the Internet, "cyber attack" has grown in prominence as a mainstay in the vocabulary of information security experts all over the world. Beyond security professionals, as well as the information technology market, mainstream consumers of all technical skill levels are also dealing with cyber attacks, given the influx of viruses, identity theft, and other online transactions associated with the Internet.

Cyber attacks are constantly monitored and guarded by world governments, armed forces, and specific corporate market segments, such as financial services where data security is paramount. Without question, the presence of domestic or foreign terrorists attempting to breach national infrastructure platforms such as utility grids, the major stock exchanges or other high-level targets is still prevalent. Additionally, there is an emergence and focus toward softer targets, many which are aimed at the private sector.

The proliferation of the Internet into nearly every facet of our daily lives has enabled terrorists and other criminals to harness an all-encompassing medium for cyber attacks. From online gaming, media sharing and banking to companies relying upon it to power their IT infrastructure, the Internet has evolved into the most powerful communications platform in the world. Some security pundits are under the misconception that this behavior must be limited to some political group or faction. In reality, many known cyber attacks were orchestrated by pedestrian attackers with little to gain but the sheer thrill of wreaking havoc.

Many world governments have antiquated computer systems that are prime targets for criminal activity. International agencies such as Interpol act to gather data on possible targets, terrorists, and other information to proactively warn its members of possible threats. In the U.S., the National Infrastructure Protection Center (NIPC) supports information and physical security for law enforcement, national institutions, the military and the corporate sector. However, U.S. government agencies and militaries must do more to protect sensitive data.

Secure KVM Switches to the Rescue

As security threats on government and military continue to rise at an alarming rate, so too, does the need for security-hardened IT environments. Enter Secure KVM solutions. Secure KVM switches are designed specifically for government and military desktops or in environments where security is business-critical, such as financial services and medical/healthcare.

Security-hardened KVM switches provide the means to consolidate multiple workstations of various security classification levels with one keyboard, video monitor and mouse (KVM) console. With hardware and software-based security features built into the units, military, intelligence and federal agency installations can rest assured that their data is being protected on both physical and digital levels.

The Solution - ATEN's Secure KVM Switches

ATEN's **CS1182** and **CS1184** are two- and four-port USB DVI Dual-Link Secure KVM switches that provide safe switching between computers operating on different secure networks. By combining physical security with controlled USB connectivity, the CS1182/CS1184 gives users the means to consolidate multiple workstations of various security classification levels with one keyboard, monitor and mouse (KVM) console.

The CS1182/CS1184 Secure KVM switches, housed in a rugged metal enclosure, ensure data integrity when switching between computers operating on different secure networks.

The secure desktop KVM switches provide users with hardware security features such as tamper-evident tape, providing a visual indication of any attempted access to the switch's internal components, and chassis intrusion detection, which disables the unit if only one of the screws is removed. In accordance with the NIAP requirements, all integrated circuits are soldered directly onto the circuit board to prevent component tampering.

From a firmware point of view, secure KVMs offer restricted USB connectivity whereby non-HID devices are ignored if connected. Isolated channel per port and automatic keyboard buffer clearing prevent any cross-computer communication. Additionally, non-reprogrammable ROM fully protects the unit's firmware from tampering and reprogramming.

Secure KVM Certification

The National Institute of Standards and Technology (NIST) and National Security Agency (NSA) have established a program under the National Information Assurance Partnership (NIAP) to evaluate IT product conformance to international standards. The program, known as the NIAP Common Criteria Evaluation and Validation Scheme for IT Security (CCEVS), was implemented to help consumers and government agencies select commercial off-the-shelf IT products that meet their security requirements.

Thus, the CS1182/CS1184 Secure KVM switches are NIAP-certified which complies with the Common Criteria EAL2+ for Peripheral Sharing Switch (PSS) Human Interface Devices Protection Profile v2.1, satisfying the latest security requisites set by the U.S. Department of Defense for peripheral switches. Compliance ensures maximum information security while sharing a single set of HIDs (keyboards, mouse, speakers, etc.) between multiple computers. Conformity with Protection Profile v2.1 certifies that other USB peripherals cannot be connected to the console ports of the secure KVM switch, and that only a keyboard and mouse are accommodated, therefore providing high-level security, protection and safekeeping of data.

Security Benefits of ATEN Secure KVM Switches

- ***Chassis Intrusion Detection*** – renders the secure KVM switch inoperable when malicious tampering is detected
- ***Tamper-proof Hardware*** – all integrated circuits are soldered directly to the circuit board to prevent tampering with the components
- ***Tamper-Evident Tape*** – monitors any attempt to physically access the switch's internal components
- ***Non-Reprogrammable ROM*** – prevents reprogramming the switch's firmware
- ***Restricted USB Connectivity*** – non-HIDs (Human Interface Devices) are ignored when switching
- ***Port Selection Via Pushbutton Only*** – selecting ports via OSD and hotkey methods are disabled to enhance security
- ***Cleared Keyboard Buffer*** - Switch's keyboard data is automatically deleted after it has been transmitted
- ***Channel Isolation*** - Isolated channel per port makes it impossible for data to be transferred between secure and unsecure computers.

Conclusion

While security has markedly improved in government, military and public sector installations, cyber threats continue to be prevalent. Key concerns include securing sensitive information, network breaches, malware attacks and cyber terrorism. With secure KVM switches deployed, government agencies can minimize security threats by ensuring data integrity between user desktops accessing secure and unsecure networks. With security features such as tamper-evident tape, chassis intrusion detection, and tamper-proof hardware coupled with software security, the ATEN Secure KVM switches are well-equipped to mitigate the vulnerability of a variety of cyber attacks.

For more information on ATEN's Secure KVM Solution, including the CS1182 and CS1184, please visit **http://www.aten.com**.