Secure Desktop KVM Switch Update

BLACK BOX®

Keep classified information classified.

Introduction

Until recently, the National Information Assurance Partnership (NIAP) used Common Criteria Evaluation & Validation Scheme (CCEVS) to evaluate and approve KVM switches for security. EAL2 and EAL4+ are tests regarding the process of the design, testing, verification, and shipping of security products. This protection profile is an international standardized process for information technology security evaluation, validation, and certification.

NIAP has determined that EAL and CCEVS are no longer adequate security standards for KVM switches that connect to systems with differing security classifications. As a result, they upgraded the Protection Profile (PP) for peripheral sharing switches to PPS 3.0. Still, the next generation of secure switches are going to need to be TEMPEST-approved for the tightest security measures available.

Desktop KVM Switches

A desktop KVM switch, at its most basic, is simply a hardware device that enables one workstation consisting of a keyboard, video monitor, and mouse to control more than one CPU. Desktop KVM switches are usually 2- or 4-port switches, and by pushing a button or using keystrokes, users can easily access information and applications on completely separate systems.

KVM technology provides monitoring solutions for automation, processes, and workflow. It gives users improved operability and a quick return on investment due to better workplace ergonomics and productivity. KVM switches enable users to save space by reducing interface devices; save costs by eliminating redundant peripherals. Use of KVM devices reduces heat in a work area, and saves power.

Secure Desktop KVM

Secure KVM switches fill a special need in desktop switching for users, such as those in law enforcement, military, or security, who need to access information stored at different classification levels on physically separate systems.

Government agency systems that could include classified information

SIPRNet — Secret Internet Protocol Router Network is a system of connected computer networks used by the U.S. Department of Defense (DoD) and the U.S. Department of State to transmit classified information.[1]

GWAN — Government Wide Area Network

NSANET — The Intranet system of the National Security Agency of the United States.

JWICS — Joint Worldwide Intelligence Communications System

Site TS/SI/TK/B Ops Net — Top Secret, Signal Intelligence, Talent Keyhole, Background

NIPRNET — Nonsecure Internet Protocol Router Network is used to exchange sensitive but unclassified information between internal users as well as providing access to the Internet.[2]

1. http://en.wikipedia.org/wiki/SIPRNet
2. http://en.wikipedia.org/wiki/NIPRNet

In the past, to ensure security, in government or military applications, KVM systems were disregarded. Computers with different security classifications each had their own keyboard, monitor, and mouse. With the advent of specially constructed KVM switches, secure KVM became a viable technology solution.

A secure KVM switch is a 2- or 4-port desktop switch that provides control and separation of PCs connected to networks of differing security classifications.

Through isolated ports, permanent hard-wiring, and other types of hardware features, security issues are eliminated.

Security Issues	Security Solutions
Microprocessor malfunction or unanticipated software bugs cause data to flow between ports.	"Secure desktop KVM switches mitigate these threats by adhering in their design to strict standards for data separation."[3]
Timing analysis attacks, which means a snooper looking at what happens on one port to determine data flow patterns on another.	Unidirectional data flow is enforced by hardware "data diodes" so data isolation doesn't rely on software integrity.
Malicious modification of microprocessor software causing data to leak between ports.	Only one computer is connected at a time to any shared circuitry. Links are unidirectional, preventing timing analysis.
Subversive snooping by detecting electromagnetic radiation emitted from the equipment.	Microprocessors are one-time programmable and soldered on the board. Data isolation does not rely on software; it is ensured by hardware.
Detection of signals on one computer by monitoring for crosstalk (leakage) signals on another computer.	Carefully shielded metal case with dual shielding in critical areas and a low emissions profile.
Signaling by shorting the power supply or loading the power.	Each port is independently powered by its USB port. Shorting the power supply on one port will not cause the power on the other ports to be switched off.
Data transfer by means of common storage or common RAM.	Shared circuitry and the keyboard and mouse are powered down at each switchover to clear all volatile memory of any previous connections.
Physically tampering with the switch.	The switch is designed with tamper-proof seals to be fitted over the countersunk screws.

Changes to Authority for Validation

New rules pending

Think of it as having air bags in a vehicle. The airbags ensure safety in the case of a crash, but don't stop a car from being stolen. Similarly, EAL certification, while ensuring some level of internal security, did not stop certain attacks from external sources.

NIAP-approved secure KVM switches until very recently used a validation system known as Common Criteria (CC). The NIAP CC Evaluation and Validation Scheme (CCEVS) is managed and staffed by the National Security Agency (NSA). The focus of CCEVS is to establish a national program for the evaluation of information technology products to the International CC for Information Technology Security Evaluation.

Common Criteria (CC) Validation Process no longer considered rigorous enough to protect against hacking and data leaks.

The former standard approved by NIAP was only effective for CPUs connected to multiple networks of the same level or classification, for example for SIPRNET to SIPRNET (that is, secure networks to secure networks).

Definition of TEMPEST

TEMPEST testing, while classified, is regarded a process that assesses the port-to-port isolation required for certain KVM switches. A TEMPEST approval means the necessary isolation is achieved and qualified. Additionally the threat of data linking by various covert electromagnetic eavesdropping mechanisms have been evaluated and found to be secure.

The TEMPEST designation is often required by military organizations. TEMPEST, as a security standard, pertains to technical security countermeasures, standards, and instrumentation that prevent or minimize the exploitation of vulnerable data communications equipment by technical surveillance or eavesdropping.

A full suite of protections should include:

- Software security
- Physical security
- Common Access Card (CAC) support
- Port separation
- Memory buffers
- True KVM functionality
- Keyboard and mouse devices can only be enumerated at the keyboard and mouse ports. Devices such as flash drives, mass storage units, or cameras – any device that could potentially capture data – will be rendered useless if connected to a USB port on a secure KVM switch.
- Port isolation facilitates RED/BLACK data separation. Channel-to-channel >60-dB or >80-dB crosstalk isolation protects against signal snooping, so software tools and applications cannot be used to access any connected computer from another connected computer.
- Data isolation through hardware makes it impossible for the computer to send data along the keyboard and mouse signaling channels. Unidirectional data flow like this prevents the K/M interfaces from becoming covert computer-to-computer signaling channels from software holes or unanticipated bugs.
- Memory is automatically cleared after data is transmitted through the KVM switch. No residual data is ever left in the device.

Conclusion

The security situation confronting the United States has changed drastically in two decades. In order to enhance their assurance, U.S. agencies should ensure the products they choose fit the highest security profile available, and potentially exceed those requirements.

While this white paper focuses on government and military applications for secure desktop KVM switching, cyber attacks can happen to any institution. Security is vital to data at universities, research and development departments, the energy sector, and larger corporations as well. Any organization that values its data yet recognizes that users need access to the wider Internet would do well to consider their KVM switching options.

Choosing a secure KVM switch requires more than comparing features and looking for an EAL validation. Different devices rated EAL2 or EAL4+ can vary widely in functionality, and may not provide the degree of security available for switching between systems with different security classifications. Only a full and careful evaluation of the full set of specifications detailed in a Validation Report plus additional protections can ensure a product meets the needs of the qualifying agency.

WP00079-Secure KVM_v2