BLACK BOX WHITE PAPER: CLASSIFIED INFORMATION KEPT CLASSIFIED WITH SECURE KVM

LEAVE THE TECH TO US

INTRODUCTION

Cyber threats are constantly evolving, becoming more frequent and sophisticated every day. Our reliance on technology, sharing of global resources and need for real-time collaboration have led to a growing web of data. While interconnectivity helps us work together more efficiently and effectively, it also leaves us increasingly vulnerable to devastating cyberattacks.

Unsecure KVM (keyboard, video and mouse) switches are susceptible to cyberattacks and can allow cybercriminals to access classified data. If a cybercriminal wants to steal information off a classified server, they can stick a USB drive with malware on it into a KVM switch to access multiple servers instead of just one. KVM switches are also susceptible to the malicious use of LCD monitors (via EDID signal), microphones or CAC devices.

Also, cybercriminals can pull hardware information through sound waves from a traditional KVM switch. They can get programmable ROM sequences from sound waves, which lets cybercriminals reconfigure or reprogram the server to make it unsecure. Through all of these methods, a wealth of classified information can get into the wrong hands and be used to harm government agencies.

Until recently, the National Information Assurance Partnership (NIAP) used Common Criteria Evaluation & Validation Scheme (CCEVS) to evaluate and approve KVM switches for security. NIAP has implemented the Common Criteria Recognition Arrangement (CCRA) Management Committee Vision Statement for the application of the Common Criteria and no longer evaluates against Evaluation Assurance Levels (EAL). This strengthens evaluations by focusing on technology specific security requirements. As a result, they upgraded the Protection Profile (PP) for peripheral sharing switches to PPS 3.0 NIAP Protection Profile for Peripheral Sharing Switch Version 3.0, which 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.

GOVERNMENT AGENCY NETWORK ENCLAVES THAT INCLUDE CLASSIFIED INFORMATION:

SIPRNet — is the U.S. Department of Defense's (DoD) largest interoperable command and control data network supporting the Global Command and Control System (GCCS), the Defense Message System (DMS), collaborative planning and numerous other classified applications.

NIPRNet — Non-Secure Internet Protocol Router NETwork is the U.S. Department of Defense network for exchanging "sensitive but unclassified" information.

TRADITIONAL 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. Traditional desktop KVM switches can typically access 2, 4, 8 or 16 different PCs or networks. With traditional KVM switches, users can easily access information and applications on completely separate systems by pushing a button or using keystrokes.

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 and react faster in critical situations. Use of KVM devices reduces heat in a work area and saves power.

WHAT ARE SECURE KVM SWITCHES?

Major defense agencies use advanced security measures to isolate networks and safeguard information from outside threats. However, there is one place where isolated networks and sensitive information come together: the user desktop. Now, as desktop security becomes more critical than ever before, Black Box is introducing a signature line of secure KVM and KM switches.

KVM switches allow access and management of multiple computers from a single workstation with a keyboard, mouse and monitor. A secure KVM switch is a 2-, 4-, 8- or 16-port desktop switch that provides control and separation of PCs connected to networks of differing security classifications. Unlike traditional KVM switches, secure KVM switches can only be controlled using push button control. Hotkey commands are disabled, which ensures only the right users have access.

Secure KVM switches won't allow a USB drive that isn't recognized to access any information. They allow administrators to choose which USBs are authorized or recognized. They feature non-reprogrammable ROM to block the pulling of hardware information from sound waves. And that's just the tip of the iceberg. Secure KVM switches do much, much more to protect government agencies from today's most terrifying cyber threats.

THE GOVERNMENT'S CYBERSECURITY SITUATION

Cyberattacks on government systems are increasing at an exponential rate. According to the U.S. Government Accountability Office (GAO), cybersecurity incidents affecting federal agencies have consistently grown, increasing about 1,300 percent from fiscal year 2006 to fiscal year 2015. [1]To make matters worse, GAO has consistently found weaknesses in the federal government's methods to protect federal information systems and its cybersecurity infrastructure as well as in its methods for guarding personally identifiable information.[2]

While there is no current data on the number of attempts to compromise intelligence and defense computer systems specifically, they are no doubt under similar stress as foreign governments, terrorists and malicious hackers that target classified data and government documents attempt to shut down networks and destroy valuable infrastructure and steal intellectual property.

Government agencies are also threatened by their own employees. Recent research by IBM and others states that nearly 60 percent of today's cyberattacks are performed by insiders. While some of these attacks are accidental, the number is still alarming.[3]

To combat these risks, government agencies need to fix all of their cybersecurity weaknesses.

A crucial place to start is their KVM systems.

HOW DO SECURE KVM SWITCHES COMBAT CYBERATTACKS?

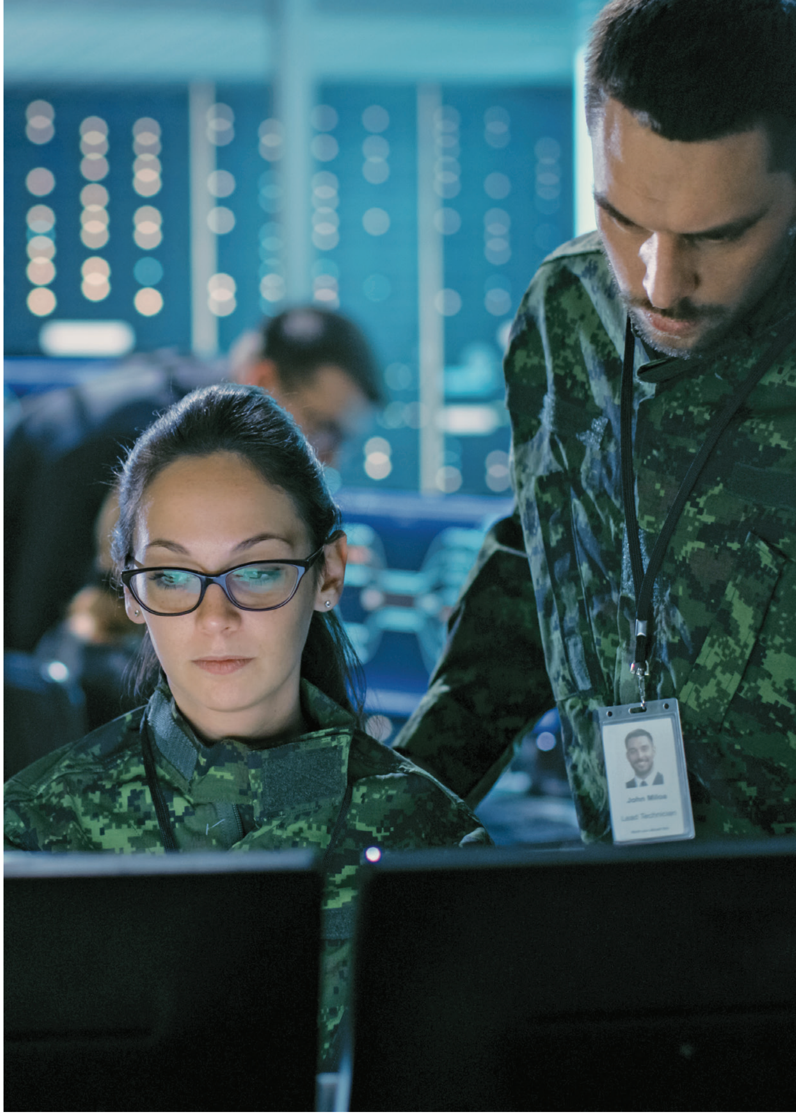
Black Box Secure KVM Switches are designed for use in secure defense and intelligence applications where sensitive data must be protected. They prevent data leakage between computers that can run at different security levels. Secure KVM switches eliminate any potential cyberattacks by allowing users to control KVM operations on multiple computers with DisplayPort, HDMI, DVI, or VGA (via adapter). They feature mechanical, electrical and optical signal isolation to prevent hacking and data leakage in environments where security is paramount.

KEYBOARD & MOUSE EMULATION

Secure KVM emulates the presence of a keyboard and mouse for every attached computer through a USB cable. Both selected and non-selected computers maintain a constant connection with the unit's keyboard mouse emulation controllers, allowing for ultra-fast switching and restricting discovery of newly-connected peripherals during switching operations. Emulation of keyboard and mouse also prevents direct connection between the peripherals and the connected computers, shielding systems from potential vulnerabilities.

CAC SUPPORT

Many secure KVM switches support CAC (Common Access Card) devices, such as smart-card and biometric readers that bolster security when using the device. However, Black Box Secure KVM Switches take CAC security even further, allowing users to assign specific peripheral devices to the CAC port of a secure KVM switch. Once a peripheral device has been registered by an authenticated administrator, users can then switch the connection between that device and the PCs along with KVM switching.



EDID LEARN & VIDEO EMULATION

Black Box Secure KVM Switching products simulate a generic EDID as default, allowing them to operate most of the connected monitors. Selected and non-selected computers maintain constant connection with the unit's video and AUX emulation controllers, allowing for ultra-fast switching and restricting discovery of newly-connected monitors during switching operations. This prevents unwanted and unsecure data from getting transmitted through DDC lines.

ACTIVE ANTI-TAMPER TECHNOLOGY

Black Box Secure KVM Switches are guarded from any type of tampering. If someone takes the device, removes the hologram label and opens (unscrews) the housing, the device becomes completely inoperable. This stops criminals from making malicious changes to a KVM switch.

INFLEXIBLE FIRMWARE

Black Box Secure KVM Switches feature firmware that is protected by multilayer protection and cannot be changed. This means that the logic of the switch cannot be modified in any way.

ISOLATED PORTS

The Black Box Secure KVM Switch line provides port isolation between networks, ensuring no data is leaked between secure ports and the outside world.

[1] https://www.gao.gov/products/GAO-16-885T

[2] https://www.gao.gov/products/GAO-17-440T

[3] https://www.prweb.com/releases/2017/11/prweb14920789.htm

WHY CUSTOMERS CHOOSE BLACK BOX SECURE KVM:

- Fully-configurable CAC port for external USB peripherals (optional)
- Secure EDID emulation prevents unwanted and unsecure data to be transmitted
- Keyboard cache wiping. Keyboard data is automatically cleared to prevent sharing. During power down, all connected devices are disconnected from the computers and all internal cache other than the auditing log is wiped.
- Mechanical, electrical and optical signal isolation to prevent hacking and data leakage in environments where security is critical – absolute isolation / no data leakage between ports
- Non-reprogrammable ROM
- Active anti-tamper switches
- External hologram, tamper-evident seals
- Secure video and AUX emulation restricts discovery of newly-connected displays during switching operations which prevents unwanted and unsecured data from getting transmitted between the computers and the display
- Native resolutions up to 4K @30Hz (DP/HDMI), 2560×1600 @ 60Hz (DVI-I), also VGA Compatible (via adapter)
- Front panel buttons with LED indicators
- Keyboard and mouse emulation maintain a constant connection with the selected and non-selected computers
- Secure EDID learning and video emulation, allowing a quick and secure connection and constant communication
- Fixed firmware and hardware equipped with anti-tampering technology
- Chassis intrusion protection – unit shuts down connection with all attached PCs/peripherals and disables any functionality
- Opto-isolated USB ports keep USB data paths electrically isolated from each other to prevent data leakage between ports
- Able to interact with multiple computers belonging to different security classification levels while maintaining full isolation
- Absolute isolation – no leakage between ports / isolated data channels
- Supports all available OS's: Windows, Mac OSx and Linux
- Locking power connector
- Made in the USA, TAA compliant

BLACK BOX'S SECURE KVM SWITCHES' ISOLATED PORTS, PERMANENT HARDWIRING AND OTHER HARDWARE FEATURES ELIMINATE SECURITY ISSUES	
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 to strict standards for data separation.
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.	Absolute isolation - No data leakage between ports.
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. No data is stored in non-volatile memory.
Physically tampering with the switch.	The switch is designed with external, tamper-evident seals placed over the boundary between the upper and lower half of the enclosure. If tampered with, the device will become permanently disabled.

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, cyberattacks 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 secure KVM switching options.

NIAP 3.0-certified Secure KVM Switches from Black Box 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.

MILITARY CUSTOMER USE CASE:

A military (defense) customer came to Black Box with two pressing issues: inefficient network access and a cluttered workspace. Their operators needed to access multiple computer networks in secure communications centers. It was a time-consuming process because each computer network required a separate keyboard, monitor and mouse which meant the operator had to move between the different systems to access sensitive data and intelligence networks. This also required a table for all six different monitors, six different keyboards and six different mice, which made for a cluttered and cramped workspace. To overcome these challenges, they purchased an 8-Port Secure KVM Switch from Black Box that reduced their configuration to one monitor, one keyboard and one mouse, saving valuable time for operators having to switch between multiple networks and opening up a wealth of desk and office space. Now they operate more efficiently in a clean workspace while ensuring their vital data has no way of being compromised.