KEYBOARD VIDEO AND MOUSE SWITCH SECURITY TECHNICAL IMPLEMENTATION GUIDE (STIG) OVERVIEW

Version 2, Release 6

22 January 2016

Developed by DISA for the DoD

Trademark Information

Names, products, and services referenced within this document may be the trade names, trademarks, or service marks of their respective owners. References to commercial vendors and their products or services are provided strictly as a convenience to our users, and do not constitute or imply endorsement by DISA of any non-Federal entity, event, product, service, or enterprise.

TABLE OF CONTENTS

LIST OF TABLES

Page

LIST OF FIGURES

1. INTRODUCTION

1.1 Executive Summary

This *Keyboard, Video, and Mouse (KVM) Overview* is published as part of the *Sharing Peripherals across the Network (SPAN) Security Technical Implementation Guide* (*STIG*). The *Keyboard, Video, and Mouse (KVM) Checklist* provides the technical security policies, requirements, and implementation details for applying security concepts to KVM and A/B switch technology. Throughout this document, the term "switch" refers to both KVM and A/B switches, unless otherwise noted. The KVM checklist is meant to be used in conjunction with the *Network Infrastructure* and appropriate operating system (OS) STIGs.

This overview document supersedes the *Sharing Peripherals across the Network Overview, Version 2 Release 2, 20 October 2012*.

1.2 Authority

DoD Instruction (DoDI) 8500.01 requires that "all IT that receives, processes, stores, displays, or transmits DoD information will be […] configured […] consistent with applicable DoD cybersecurity policies, standards, and architectures" and tasks that Defense Information Systems Agency (DISA) "develops and maintains control correlation identifiers (CCIs), security requirements guides (SRGs), security technical implementation guides (STIGs), and mobile code risk categories and usage guides that implement and are consistent with DoD cybersecurity policies, standards, architectures, security controls, and validation procedures, with the support of the NSA/CSS, using input from stakeholders, and using automation whenever possible." This document is provided under the authority of DoDI 8500.01.

Although the use of the principles and guidelines in these SRGs/STIGs provide an environment that contributes to the security requirements of DoD systems, applicable NIST SP 800-53 cybersecurity controls need to be applied to all systems and architectures based on the Committee on National Security Systems (CNSS) Instruction (CNSSI) 1253.

1.3 Vulnerability Severity Category Code Definitions

Severity Category Codes (referred to as CAT) are a measure of vulnerabilities used to assess a facility or system security posture. Each security policy specified in this document is assigned a Severity Category Code of CAT I, II, or III.

Table 1-1: Vulnerability Severity Category Code Definitions

	DISA Category Code Guidelines
CAT I	Any vulnerability, the exploitation of which will **directly and immediately** result in loss of Confidentiality, Availability, or Integrity.
CAT II	Any vulnerability, the exploitation of which **has a potential** to result in loss of Confidentiality, Availability, or Integrity.
CAT III	Any vulnerability, the existence of which **degrades measures** to protect against loss of Confidentiality, Availability, or Integrity.

1.4 STIG Distribution Keyboard Video and Mouse Switch

Parties within the DoD and Federal Government's computing environments can obtain the applicable STIG from the Information Assurance Support Environment (IASE) website. This site contains the latest copies of any STIGs, SRGs, and other related security information. The address for the IASE site is http://iase.disa.mil/.

1.5 Document Revisions

Comments or proposed revisions to this document should be sent via email to the following address: disa.stig_spt@mail.mil. DISA will coordinate all change requests with the relevant DoD organizations before inclusion in this document. Approved changes will be made in accordance with the DISA maintenance release schedule.

1.6 Other Considerations

DISA accepts no liability for the consequences of applying specific configuration settings made on the basis of the SRGs/STIGs. It must be noted that the configuration settings specified should be evaluated in a local, representative test environment before implementation in a production environment, especially within large user populations. The extensive variety of environments makes it impossible to test these configuration settings for all potential software configurations.

For some production environments, failure to test before implementation may lead to a loss of required functionality. Evaluating the risks and benefits to a system's particular circumstances and requirements is the system owner's responsibility. The evaluated risks resulting from not applying specified configuration settings must be approved by the responsible Authorizing Official. Furthermore, DISA implies no warranty that the application of all specified configurations will make a system 100 percent secure.

Security guidance is provided for the Department of Defense. While other agencies and organizations are free to use it, care must be given to ensure that all applicable security guidance is applied both at the device-hardening level as well as the architectural level due to the fact that some of the settings may not be able to be configured in environments outside the DoD architecture.

1.7 Product Approval Disclaimer

The existence of a STIG does not equate to DoD approval for the procurement or use of a product.

STIGs provide configurable operational security guidance for products being used by the DoD. STIGs, along with vendor confidential documentation, also provide a basis for assessing compliance with Cybersecurity controls/control enhancements, which supports system Assessment and Authorization (A&A) under the DoD Risk Management Framework (RMF). DoD Authorizing Officials (AOs) may request available vendor confidential documentation for a product that has a STIG for product evaluation and RMF purposes from disa.stig_spt@mail.mil. This documentation is not published for general access to protect the vendor’s proprietary information.

AOs have the purview to determine product use/approval IAW DoD policy and through RMF risk acceptance. Inputs into acquisition or pre-acquisition product selection include such processes as:

- National Information Assurance Partnership (NIAP) evaluation for National Security Systems (NSS) (http://www.niap-ccevs.org/) IAW CNSSP #11
- National Institute of Standards and Technology (NIST) Cryptographic Module Validation Program (CMVP) (http://csrc.nist.gov/groups/STM/cmvp/) IAW Federal/DoD mandated standards
- DoD Unified Capabilities (UC) Approved Products List (APL) (http://www.disa.mil/network-services/ucco) IAW DoDI 8100.04

2. ASSESSMENT CONSIDERATIONS

2.1 Introduction

KVM switches are used to connect a single keyboard, video monitor, and mouse to multiple information systems (ISs), saving space and equipment. Modern devices have also added the ability to share other peripherals like USB devices and audio. These switches are commonly used to reduce clutter in testing laboratories, server rooms, and on client computers. A/B switches are used to switch a single peripheral between multiple ISs or multiple peripheral devices on a single interface for a single IS.

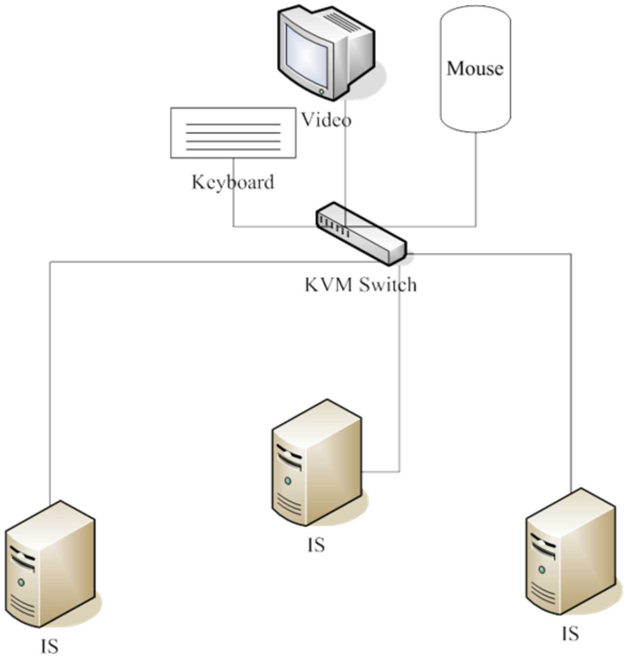
2.2 KVM Switches

KVM switches may be separated into two general categories, analog and network attached switches. Analog switches are directly connected to the devices being controlled. Network attached switches use a network protocol to communicate with the devices being controlled. Switches may also be categorized based on usage as follows.

- Single user KVM switch
- Multi-user analog KVM switch
- Multi-user network attached KVM switch

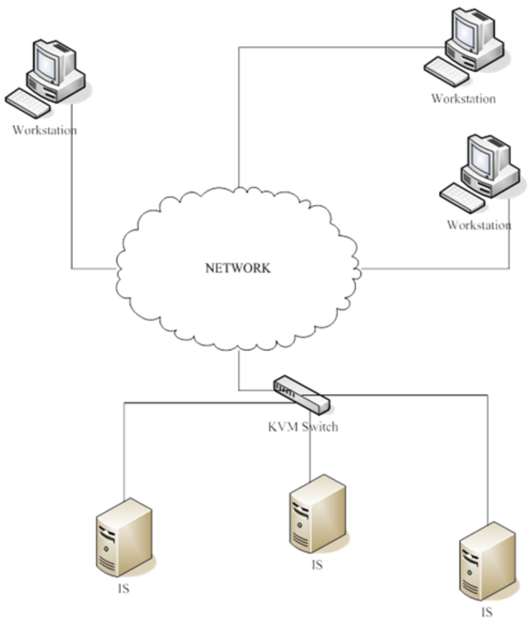
In the example depicted in Figure 2-1, Analog KVM Switch Connection, an analog KVM switch is directly connected to the keyboard, video, mouse, and systems.

Figure 2-1: Analog KVM Switch Connection



Network attached KVM switches may have analog components attached, but also have the ability to be accessed via client software either over a network or via dial-up remote access. The client software may be either a proprietary software client supplied by the switch manufacturer or a web browser. The network protocol may be a standard protocol like Transmission Control Protocol/Internet Protocol (TCP/IP) or may be a proprietary method of data transmission. The switch may allow any combination of connections: single user to any single system, multiple users to a single system, or multiple users to multiple but different systems. See Figure 2-2, Network Attached KVM Switch.

Figure 2-2: Network Attached KVM Switch



2.2.1 Single User KVM Switches

A single user KVM switch is a simple analog KVM switch attached to systems of the same security classification level located within a single user's work area for the purpose of consolidating multiple sets of keyboards, video monitors, and mice for a single user to one set. These switches will be manually operated and have minimal programmable menus or features. The single user KVM switch definition and policies will only apply if the classification level of all ISs involved is unclassified. In all other cases, either the multi-user analog KVM switch or multi-user network attached KVM switch definitions or policies will apply. These switches are restricted to unclassified ISs to allow for use with minimal documentation.

To ensure the users have been advised of their responsibility when using switches, the ISSO will maintain a written user agreement. Additionally, the ISSO will ensure that documentation explaining the user's responsibilities when using a switch and the correct operation of the switch is supplied to the users in either a section of the local user's guide or equivalent document provided by the site. This user's guide must, at a minimum, describe the correct switching procedures and banner markings which are detailed in the KVM Checklist.

Although the KVM switch itself is considered an unclassified object, it must be protected in a manner suitable for the system with the highest classification to which it is connected. For example, if the switch is connected to a sensitive system and an unclassified system then it will be protected in the same manner as the sensitive system. This also means that physical access to the KVM switch will be restricted to individuals that are allowed physical access to all ISs attached to the switch.

A smart (intelligent or programmable) keyboard will not be attached to a KVM switch. This definition applies to any keyboard that contains memory and/or can be programmed, either via the connected system or directly by the user in a learning mode. This includes keyboards with smart card readers, Universal Serial Bus (USB) ports, and removable media drives. It does not apply to keyboards that have enhanced non-configurable functionality, such as an Internet keyboard. Programmable keyboards present the possibility of data being transferred between systems of different classifications. Wireless keyboards or mice used with a KVM switch must comply with the Wireless STIG.

All KVM switches will be labeled as required for all government owned equipment. Additionally, all switch positions, cables, and connecters will be labeled with the identity and security classification of the system to which they are attached. Any unused port/connector on a KVM switch will be blocked with tamper evident seals.

If the KVM switch has a configuration file, the ISSO or SA will maintain a backup of the configuration. If a machine-readable backup is not possible then a document describing the settings selected will be maintained.

2.2.2 Multi-User Analog KVM Switches

Multi-user analog KVM switches are analog KVM switches found in any environment that does not meet the requirements for single user analog KVM switches. Most often this would be a server area where there are many separate servers, each of which needs occasional administrative access. A KVM switch can save both space and money by allowing a single set of hardware to support all of the servers. However, these multi-user switches are not restricted to a single set of hardware provided that there is no network component involved. Another environment where these switches would commonly be found is the laboratory environment where there are many test ISs.

There are analog KVM switches that fill the whole gamut from being controlled by mechanical switches and no configurable features to touch-sensitive switches that are fully configurable with menus, multiple colors, and “hot key” triggered scripts. Some switches support user-level access control, which can be tailored to granular access to each system attached to the KVM. However, if user sign-on access is not supported, then access to the switch must be restricted to individuals with access to each system attached to the switch.

2.2.2.1 Requirements for Spanning Classification Levels

Multi-user analog KVM switches are the only type of KVM switches that can be used to span security classification levels. KVM switches should not be able to directly transfer information from one system to another. However, information could inadvertently be transferred between systems by a user entering data on one system while thinking that he is accessing another system attached to the same KVM switch. Therefore, prior to an analog KVM switch being attached to any IS, the AO for that IS must approve the connection. The KVM must also be approved for use as part of the site’s SIPRNet Connection Approval Office (SCAO) connection approval documentation.

Cascaded KVM switches can lead to a user accessing a different IS than intended because of the multiple switch positions needed to be set to correctly access a specific system. Therefore, KVM switches will not be cascaded either with another KVM switch or any other switch. This risk may be mitigated through use of a physical or logical tamper evident solution, careful labeling of cables, and strict adherence to a configuration management process.

KVM switches are also available that can switch speakers, voice, and peripherals. The only peripherals currently approved for KVM switch that span classification levels are the keyboard, video, and mouse. These switches will have this feature disabled or blocked with a tamper evident solution. Users must be trained not to attach any devices other than a keyboard, video monitor, or mouse to the KVM switch.

2.2.3 Multi-User Network Attached KVM Switch

Multi-user network attached KVM switches can be used in very similar implementation to the multi-user analog KVM switches. However, because of the additional cost, these switches are generally only used if there is a requirement for remote administration of the ISs, such as a “lights out” server environment where there would normally not be administrative personnel. Because of the network access, many of the features that were optional on an analog KVM switch are required for a network attached KVM switch.

If a network attached KVM switch is used in a laboratory environment to give access to laboratory systems for a use other than administration, consideration should be given to the use of an “out-of-band” or private network to segregate the traffic from the functional traffic for both security and performance reasons. However, if a network attached KVM switch is used to administer ISs, the switch will be administered out-of-band. Additionally, KVM switches will only be attached to a network of the same classification level as the ISs attached. Refer to the Network Infrastructure STIG for out-of-band network administration.

Network attached KVM switches must be configured to use robust user-level access control, including two-factor authentication controls. Because all administrative traffic must be encrypted to protect it from interception, the KVM switch will be configured to require encryption for all communications via the network.

Some network attached KVM switches have the ability to encapsulate and forward USB protocol between the attached ISs and the client connected via the network. With this functionality, the possibility exists to boot an IS, attached to the KVM switch IS, over the network from a USB attached device. Because of the extreme consequences that would arise from a compromised KVM switch, this feature will be disabled on the KVM switch and any IS attached to the KVM switch. If there is no need for a USB connection between an IS and the KVM switch, the USB ports will be blocked or disabled.

Some KVM switches now support the keyboard and mouse connections via a single USB cable instead of separate cables. In this arrangement, the KVM switch functions as a USB hub with multiple devices (the keyboard and the mouse) attached to it. This connection can also support a third device that could be used to boot the IS via the KVM switch over the network if both the KMV switch and IS are configured to allow this functionality. If a KVM switch is used that has this ability, even though the feature is disabled, the functionality will be documented and the use of the KVM switch will be approved by the IAM for all ISs attached to the KVM.

A more common feature of the KVM switch is the ability to directly control the power supplied to the attached ISs. With this feature, a client attached to a network attached KVM switch can interrupt the power to an IS effectively shutting it down. Because a compromised KVM switch could shut down all of the ISs using this feature without the need to access the operating systems of the attached ISs, this feature will not be used.

The ISSO or SA will maintain a backup of the KVM configuration. This backup will include the userid/password file(s) that exist on the system. If the userid/password files are stored elsewhere on the network, the ISSO or SA responsible for the ISs will ensure backup procedures exist for the remote userid/password file(s).

Note: Because of the problems inherent in the spanning of networks of different classification levels, network attached KVM switches will not be attached to ISs of different classification levels.

2.3 A/B Switch

An A/B switch is a simple device that switches either a single peripheral device between two or more ISs or, switches multiple devices to a single I/O port on an IS. Whether the switch has two or more switch positions, it is always referred to as an A/B switch. In the past, A/B switches were an inexpensive solution to sharing devices among multiple users without having to power down the ISs and move the cables. The other use was to accommodate multiple devices that are occasionally used on a single system without incurring the expense of adding additional I/O ports. This technology is obsolete and better solutions exist. However, A/B switches are still being used.

A/B switches should only be used to connect multiple peripheral devices to a single system and then only if no other solution can be found. A/B switches should never be used to share peripheral devices between two or more ISs. If an A/B switch is used to share peripheral devices between two or more ISs, the IS should be intended for a single user’s use, be within a single user’s work area, and be visible from all ISs to which it is attached.

Although the A/B switch itself is considered an unclassified object, it must be protected in a manner suitable for the IS with the highest classification to which it is connected. An example would be if the switch were connected to a sensitive system and an unclassified system, then it would be protected in the same manner as the sensitive system. This also means that physical access to the A/B switch will be restricted to individuals that are allowed physical access to all ISs attached to the switch.

Two people sharing a device attached to an A/B switch can lead to information being inadvertently transferred to or from the wrong IS. To avoid this possibility, A/B switches will not be used to share devices between two or more users.

All A/B switches will be labeled as required for government-owned equipment. Additionally, all switch positions, cables, and connecters will be labeled with the identity and security classification of the IS to which they are attached.

2.3.1 Requirements for Spanning Classification Levels

The ISSO will ensure that only approved switches are used. Use of A/B switches for spanning classification levels must be documented and approved as part of the site’s SIPRNet Connection Approval Office (SCAO) connection approval process.

Cascaded A/B switches can easily lead to a user accessing a different IS than intended because of the multiple switch positions needed to be set to correctly access a specific IS. Therefore, A/B switches will not be cascaded either with another A/B switch or any other switch.

If an A/B switch is connected to two ISs of different classifications, it will not be used to switch a peripheral device that has persistent memory or devices that support removable. This could lead to information being compromised by movement between systems of different classification levels. Additionally, input and output devices including but not limited to scanners, printers, and plotters will not be attached to A/B switches that span classification levels.