

Support of USB Devices

USB Lockdown – Secure KVM Switching

Support of USB Devices

USB Lockdown – Secure KVM Switching

Table of Contents

2	Preface
3	Intrinsic Security Issues
3	USB as a Security Risk
3	The New PP for KVM Switches
3	Avocent USB Lockdown Feature
4	Conclusion
4	References

Preface

The National Information Assurance Partnership (NIAP) released the latest version of the Protection Profile (PP) for peripheral sharing switches (PSS). Effective June 1, 2010, the Peripheral Sharing Switch for Human Interface Devices Protection Profile (PSS-PP) Version 2.0, which was specifically written to address the unique security risks associated with USB KVM switches, includes more stringent requirements for USB. Since Avocent introduced the industry's first secure KVM switch for connecting a USB keyboard and mouse in 2006, we have been restricting USB access.

Intrinsic Security Issues

Federal agencies classify and store information at various levels. Individuals are accorded access to that information based on the level of their security clearance and their need to know. The point of these basic principles (and the rigorous procedures derived from them) is to establish and document an absolute “chain of custody” for all classified materials. The most common method to maintain such a chain of custody is to physically separate compartmented or classified materials on different networks and computing platforms.

Secure KVM switching involves passing otherwise separate streams of classified information through a single device.

Without adequate protections, that proximity represents a conspicuous point of vulnerability to many different types of risk. For example:

- Information could be commingled across compartments and classification levels
- Materials could be diverted onto unprotected or public networks
- Files or documents could be smuggled onto flash memory devices
- Malicious code could be introduced via external devices

USB as a Security Risk

Several years ago, desktop computers were delivered only with PS/2 ports to support a keyboard and mouse. In the late 1990s, computer manufacturers started including Universal Serial Bus (USB) support on their new systems.

Today, USB has become a standard connection for not only the keyboard and mouse but also thumb drives, removable CD drives, portable hard drives and other storage media.

Threats outside the firewall such as spam or viruses have long been recognized as major security risks. With the growth of USB storage devices, large amounts of data can now be compromised or stolen behind the firewall within the corporate network.

As the popularity of USB has increased, so have the number and types of secure violations. A quick Internet search on theft using USB devices will lead to hundreds of examples across all industries. The risk has become so prevalent that in 2009, the Department of Defense prohibited the use of all removable media devices on unclassified (NIPRNet) and classified (SIPRNet) networks.ⁱ All branches of the US military have specifically banned flash memory devices.ⁱⁱ USB presents an obvious new challenge to organizations where security must be maintained at the highest levels.

More recently, many media outlets reported that the Department of Defense lifted the ban on USB drives. On June 30, 2010, United States Strategic Command issued a clarification. They clearly state, “The U.S. Department of Defense has not lifted the ban on use of USBs.”ⁱⁱⁱ

In the referenced Communications Tasking Order, issued February 12, 2010, it was specified that there will be limited use of removable devices with strict guidelines in specific mission-critical circumstances. Furthermore, removable media is only permitted on Department of Defense computers, using government-owned devices that meet certain compliance tests.

The New PP for KVM Switches

During this same period, NIAP, in response to its customers and comments from vendors, announced sweeping changes to its strategy for Common Criteria Evaluation and Validation Scheme (CCEVS). The PSS-PP provides the Common Criteria requirements for evaluating secure KVM switches.

On June 1, 2010, NIAP issued a new PP that “limits the use of USB connects to keyboard, mouse and display. No other USB device shall be valid.” This includes potentially harmful devices such as mass storage drives and thumb drives, as well as smart card/common access card (CAC) readers. Since USB devices such as thumb drives and external hard drives would allow users to pass information between attached computers or systems, any “secure” switches that accept these devices are in clear violation of the PSS-PP. Just to further clarify, any switch using CAC or using a CAC mode is not validated under the new protection profile.

The following areas were changed in the new version of the protection profile:

1. Changed security assurance components from EAL4 to EAL2
2. Assumptions, threats and security adjusted to accommodate invalid USB devices
3. Added new security functional requirement (invalid USB connection)

For more on the new PSS-PP, refer to our FAQ document on www.avocent.com/federal.

Avocent USB Lockdown Feature

The Avocent USB lockdown feature is designed into each secure switch with USB support. Contrary to other “secure” KVM designs, the USB port on the Avocent secure switch is restricted by U.S.-designed firmware to allow only the keyboard and mouse to switch to target computers. If a thumb drive or other USB device is inserted into a secure switch USB port, nothing happens. The USB device is simply not presented to the local computer. Devices considered unsecure, such as flash drives or other mass storage devices, cameras and all other USB devices, are strictly prohibited by the switch firmware.

The Avocent secure KVM switch identifies itself as a keyboard and mouse. The host polls for data and either data is transmitted or the reply will indicate that no data is available at the time of the poll. The

Avocent secure KVM switch also serves as a host to the peripheral device or devices plugged in to the user port.

In 2006, Avocent decided that with the rapid adoption of USB as a standard and the massive proliferation of the types of devices that use USB as a communication standard, the USB lockdown feature would be mandatory to protect against the types of security breaches discussed throughout this document. In 2010, the introduction of the new protection profile confirms this approach.

Conclusion

Choosing a secure KVM switch requires more than comparing a few features and looking for EAL conformance. Current devices that are rated vary widely in their functionality and the degree of real security they provide. With a full and careful evaluation, agencies can:

- Select the products that best meet their security requirements
- Understand exactly why and how those products measure up
- Acquire the maximum amount of true protection that is available
- Avoid “comparing apples and oranges,” leaving themselves exposed to vulnerabilities

There is only one way to ensure that the KVM switches deployed by agencies will indeed deliver the maximum level of security they require and that is to evaluate the full set of specifications detailed in a product’s validation report, as well as any additional protections it may offer.

Avocent has been providing secure KVM products to the community for more than 10 years. We have hundreds of organizations continually providing feedback which allows us to stay ahead of any potential security risks. We have a full suite of solutions to meet different environments and levels of security. USB lockdown is just one of many features that demonstrates our market knowledge and commitment to design products specifically targeted to the secure organization. Our new SC 600 and 700 series have been validated

against this new protection profile. In addition, we are confident we could submit our EAL4+ USB models (excluding those with CAC support) and obtain validation with no required modifications. After all, we have been securing USB connections since 2006.

For further information, please request a copy of our secure KVM white paper entitled Beyond the Profile: The Next Generation of KVM Switching or contact one of our secure technology specialists.

References

ⁱ <http://blogs.zdnet.com/security/?p=2206&tag=nl.e589>

ⁱⁱ <http://www.defensenews.com/story.php?i=3958967>

ⁱⁱⁱ http://www.stratcom.mil/news/article/171/federal_times_clarification_usb_policy

Contact Us

For more information about Avocent or to locate an Avocent Partner near you, visit www.avocent.com.

About Emerson Network Power

Emerson Network Power, a business of Emerson (NYSE:EMR), is the global leader in enabling Business-Critical Continuity™ from grid to chip for telecommunication networks, data centers, health care and industrial facilities. Emerson Network Power provides innovative solutions and expertise in areas including AC and DC power and precision cooling systems, embedded computing and power, integrated racks and enclosures, power switching and controls, monitoring and connectivity. All solutions are supported globally by local Emerson Network Power service technicians. Aperture and Avocent solutions from Emerson Network Power simplify data center infrastructure management by maximizing computing capacity and lowering costs while enabling the data center to operate at peak performance. For more information, visit www.Aperture.com, www.Avocent.com or www.EmersonNetworkPower.com.

Emerson Network Power.

The global leader in enabling *Business-Critical Continuity™*.

- AC Power
- Connectivity
- DC Power
- Embedded Computing
- Embedded Power
- Infrastructure Management & Monitoring

EmersonNetworkPower.com

- Outside Plant
- Power Switching & Controls
- Precision Cooling
- Racks & Integrated Cabinets
- Services
- Surge Protection