belkin

TECHNICAL NOTE

KVM Peripheral Compatibility Requirements

The use of secure KVMs has become a commonplace approach to maintaining air-gap networks when sharing peripherals amongst systems in different security enclaves. Shared peripherals provide a means for east/west attacks that can leverage a compromised system to access secure networks and systems.

Belkin's secure KVMs conform to the latest NIAP Protection Profile 3.0 standards, meeting and exceeding the most stringent requirements for peripheral sharing devices. This document discusses the requirements that the NIAP standard and Belkin's other unique cybersecurity enhancements place on peripherals such as keyboards, mice, monitors, and CAC readers that are connected to the KVM.

NIAP Protection Profile for Peripheral Switching Systems 3.0 has specific provisions for ensuring that USB keyboards, mice, monitors, speakers, and CAC readers block any attempt to inject malware or leak sensitive information from one system to the other. This starts with emulation for USB keyboards, mice, and monitors. It includes optical data diodes to prevent reverse flow of data and usage guidelines around peripheral authentication that seek to prevent improperly designed peripherals from introducing security vulnerabilities.

Monitor Requirements:

Belkin's secure KVMs read a monitor's EDID information upon bootup of the KVM and store it in read-only memory. This approach allows the connected computers to see and scale their images to what the monitor can accommodate while physically blocking the ability to manipulate the monitor's EDID memory as a means of slowly transferring information from one system to the other. For this to function correctly, the monitors must be connected to the KVM and powered on before the KVM is powered on. The EDID read operation is performed only at initial bootup of the KVM. Switching monitors requires that the KVM be power cycled to read the new EDID settings.

Video display problems with secure KVMs are typically caused by an improper EDID file read from the monitor or marginal signal integrity from the graphics controller unit in the computer to the KVM and then to the monitor. Docking stations for laptops do impact the video signal emanating from the computer and special attention is sometimes needed to ensure problem-free operation. Belkin maintains an extensive test environment with common computing platforms, cable lengths and monitors to ensure a wide range of compatibility across multiple deployment scenarios.

Keyboard and Mouse Requirements:

From keyloggers to rubber ducky attacks, manipulating a USB keyboard or mouse is a common way of stealing sensitive information from protected computers. Belkin's secure KVMs use HID emulation and optical data diodes to thwart common attack vectors. The process starts with the keyboard or mouse enunciating themselves as HID compliant peripherals through the USB HID Base Class identifier, 03h. Composite devices (for example, keyboards that contain a built-in USB hub or built-in CAC reader) will either be rejected as non-compliant or limited to only the keyboard functions being visible to the KVM depending on what USB Base Class they enunciate themselves as. Once an HID-compliant peripheral is detected, commands from that peripheral are received through an optical data diode that physically limits traffic flow to one direction only. This is vital as a rubber ducky attack that dynamically changes the USB class from keyboard to USB mass storage device can pass the initial check, but would fail to download any data through the optical data diode. The complete lack of a reverse messaging path is a crucial defense mechanism against data theft, but it also prevents common feedback mechanisms that users have come to expect – CapLock, NumLock, and ScrollLock indicators on keyboards, for example will not illuminate as the message from the operating system to the keyboard has no way of being received by the keyboard. Finally, dedicated processors on each channel emulate HID commands from the keyboard and mouse to add another layer of security.

USB keyboards designed for security applications may have a built-in CAC reader. If so, the KVM may only detect and accept HID keyboard commands and not allow for the CAC reader to be activated. Similarly, some USB hubs used between the keyboard/mouse and the KVM can be rejected if they enunciate themselves as USB hubs instead of HID keyboards or mice. Where possible, Belkin recommends not using composite peripherals or hubs.

CAC Reader Requirements:

Some of the Belkin secure KVMs provide for a CAC port for use in connecting and sharing an external CAC reader amongst connected computers. The same circuitry and logic used for keyboard and mouse isolation applies to the CAC ports. The CAC port is hard-coded to only accept USB peripherals that enunciate with the proper USB class 0Bh for smart card readers, subclass 0x00, protocol 0x00. Devices that do not conform will be rejected by the KVM. NIAP usage guidelines instruct users that they should not unplug a CAC reader after the KVM is powered up and operational. However, a user is not physically prevented from doing so. The Belkin CAC-enabled secure KVMs have an auto-sensing capability that detects if the CAC reader is unplugged and seeks to re-initialize the reader when plugged back in. Belkin believes this is a critical step to prevent rubber ducky type of attacks where the USB peripheral dynamically changes its attributes. To accommodate the unplug detection, Belkin SKVMs require that the CAC readers follow standard design guidelines and are properly grounded.

Some USB card readers have begun to ship with improper grounding. When connecting the card reader to a computer, this is perfectly acceptable, but for the secure KVM, it represents a compatibility problem. The Belkin F1DN008Utt and F1DN005U are properly grounded to allow the KVM to detect an unplug event and re-initialize the reader. If the readers available do not authenticate with the SKVM, contact Belkin's support team for further instructions.

Contact

For additional information, contact:

E-mail:
FederalBusinessDivision@belkin.com