Technical Note

The Case for Secure Peripheral Sharing Devices

The world of cybersecurity is currently in a state of flux. From "cloud computing" to AI to machine learning, buzzwords are thrown around with little understanding of what they mean or do. Competing vendors each claim their technology is the best and only option for defending against the threat of hackers. Yet, constant news releases of stolen private identification information suggest that hackers seem to move faster in finding and exploiting vulnerabilities before patches can be released and applied.

In an attempt to achieve complete isolation and prevent data leakage, government agencies and military organizations are now embroiled in both offensive and defensive cyberwarfare. They have concluded that physical network segregation is the preferred method of protecting classified computer environments from those open to the internet and likely to be compromised. Where an operator is required to access both the private and open computer systems simultaneously, the use of a secure KVM has become commonplace as a means to safeguard the air-gap isolation while minimizing the clutter on the operator's desk. A Google search reveals several free toolsets that can be used to leverage a non-secure KVM to easily bridge the air-gap and start exfiltrating private data off of secure computers. Common Criteria and specifically NIAP publish the criteria and maintain a list of certified devices to conform to the latest requirements for secure peripheral switching devices such as KVMs.

The latest Common Criteria/NIAP standard is the NIAP Protection Profile for Peripheral Sharing Devices version 4.0. This document seeks to track the major differences from version 3.0 to version 4.0 as they relate to vulnerability mitigations.

NIAP PP PSS 3.0 to NIAP PP PSD 4.0

NIAP's first foray into defining the characteristics of secure peripheral sharing devices came in 2000 with the publication of the Protection Profile (PP) for Peripheral Sharing Switch (PSS) 1.0 standard. In 2007, NIAP updated the protection profile to version 1.1 then 1.2 in 2008. Version 2.0 was introduced in June of 2010 and updated to 2.1 in September of 2010. Versions 1.x and 2.x were predicated on a basic assumption that the computer systems were pristine and operators 100% trustworthy and that the KVM did not introduce any vulnerabilities. Systems certified to these legacy standards needed to guard against physical tampering – provisions as to how were left to the discretion of the manufacturer – and that they did not have persistent memory that could expose a user's data from one connected computer to the other.

Version 3.0 was introduced in 2015 and marked the first time that government agencies adopted the philosophy of zero trust. The underlying assumption in the new standard was that any computing device or peripheral that was exposed to the public internet has probably been compromised and all efforts must be taken to ensure the attack cannot propagate to secure environments that have been isolated from the beginning. In essence, NIAP PP PSS 3.0 assumed the hacker has already breached security provisions and is inside the network and sought to keep him/her from gaining access to more critical systems and data. As such, NIAP PP PSS 3.0 built upon the tamper evidence and memory requirements of the previous iterations and for the first time introduced elements such as active anti-tamper, optical data diodes, and EDID emulation in addition to USB emulation.

Active anti-tamper added a powered circuit inside the KVM that would detect a physical breach attempt and render the unit inoperable regardless if it were powered on or off when the tamper attempt occurred. In the Belkin NIAP PP 3.0 certified KVMs, a battery backed circuit was activated as part of the final assembly step of the unit. Once active, any attempt to open the case would trigger anti-tamper switches built onto the motherboard, delete the firmware, and burn a fuse, rendering the EEPROM inaccessible. As such, the unit would immediately brick and be inoperative. Belkin used optical data diodes on all USB input ports and emulated the USB HID commands to ensure that keystrokes or cursor movement commands flowed in one direction and physically blocked data from being able to be read and downloaded from connected computers. Finally, monitor EDID information was read once at the KVM's bootup and emulated from then on to physically block attempts to use the monitor's built-in memory as a way to bridge the air-gap. Data diodes were used on audio inputs to ensure that connected speakers could not be used as microphones in signaling attacks or to eavesdrop on private conversations near the KVM.

With all the advancements that NIAP PP PSS 3.0 introduced, several problems were left unaddressed. For example, the audio isolation required for PP 3.0 only blocked signaling attacks in the audible frequency range. New attacks emerged that leveraged ultrasonic frequencies to bridge the air-gap, requiring significant modifications to the audio isolation provisions. When NIAP PP 3.0 was authored and published, display resolutions were mainly 1080P and used VGA or DVI for video ports. Over the last couple of years, monitor technology and graphics cards have made tremendous leaps in performance and the norm today is 4K resolution with DisplayPort and USB-C as the main interfaces. NIAP PP3.0 understood that multi-protocol interfaces such as DisplayPort and USB-C were used for not only video but also data transmission while only loosely defining the criteria for preventing the data backchannel from being leveraged to attack a secure computer. Not only did display technologies change but there were also advances in keyboards, pointing devices, and even audio devices that the restrictive nature of the protection profile prevented from being utilized in secure applications.

In the NIAP PP 3.0 definition, firmware upgrades to accommodate newer technologies fell into a grey area where manufacturers in consultation with certification laboratories were left to determine if the upgrade constituted enough change to require new evaluations or if it was minor enough to forego additional testing. Finally, the basic need for a KVM to share peripherals between multiple computers comes down to eliminating clutter and making an operator's work environment more ergonomic and efficient. NIAP 3.0 did not have a way of defining remote controls for the KVMs and thus resulted in replacing redundant keyboards, mice, and monitors with bulky KVM boxes on an operator's desk. While the use of the secure KVM did indeed declutter the desk, it left room for further optimization by securely leveraging remote controls to control a hidden KVM switch.

Starting in 2017, NIAP convened an industry-wide technical committee to define the next iteration of the protection profile for secure switching devices. NIAP PP PSD 4.0 was published in July of 2019 and will be the only applicable standard for new evaluations when version 3.0 is archived on January 18, 2020. The initial major change that 4.0 ushered in is in the overall structure of the requirement. Instead of a single, monolithic document that discussed the vulnerabilities and test criteria for certification, version 4.0 is comprised of a base profile and individual modules for various aspects of the peripheral sharing device. The structure allows each module to be independently updated or revised as needed and should make the standard more agile in addressing the rapid pace of new vulnerability discovery and mitigation strategy development. In addition, protection profile 4.0 is no longer simply for Peripheral Sharing Switches but more holistically defines Peripheral Sharing Devices. As such, it paves the way for NIAP protections on devices ranging from microphones to single port isolators, single user matrix switchers, and other devices that the previous protection profile did not define.

From a cybersecurity perspective, NIAP PP PSD 4.0 leverages most of the advances in PP 3.0 but does reduce requirements on a few elements while advancing requirements in other areas. The chart below captures the major differences between PP PSS 3.0 and PP PSD 4.0:

Security Function	PP PSS 3.0	PP PSS 4.0
Passive Anti-Tamper	Tamper Labels	Tamper Labels
Active Anti-Tamper	Battery backup mandatory	Active anti-tamper is optional
Audit Log	Mandatory	Optional only if active anti-tamper is implemented or programmable USB peripheral port is supported
Field Firmware Updates	Not allowed	Defined patches allowed with audit-log and only with authenticated admin account
Audio Input	Not allowed	Optional only if no other switching function claimed (i.e., no video, KM, authentication device). Data diode required if audio input supported.
Audio Output	Analog only, audio diode required for 40dB up to 20KHz isolation	Analog output or digital with video; 40dB isolation up to 60KHz; 8th order elliptic filter required; isolation must be maintained in tamper mode or power off; ability to split audio from keyboard/mouse controls.
Keyboard/Mouse	Optical data diode, PS/2; KM only mode	USB emulation for HID input; configurable ports for approved peripherals with ability to whitelist/blacklist specific devices; guard mode for KM switching; PS/2 support removed.
Video	VGA, DVI, HDMI, and DP	VGA, DVI, HDMI, DP, USB-C; DP to HDMI to DP conversion specified to physically block potential backchannel; ability to provide 2nd level video rendering for PiP and multiviewer capabilities.
General	Peripheral device filter (authentication device, KM, etc.)	Peripheral device filter and acceptance/rejection bi-color LED; remote controls; definitions for KVM extenders, isolators. Explicitly prohibits multi-user matrix.

The Protection Profile for Peripheral Sharing Devices 4.0 should allow secure KVM and secure isolation technology vendors to bring new innovations and advances to users without needing to wait for the standard to evolve. The inherent agility supported by the modular structure should allow vendors to quickly address emerging vulnerabilities. Stricter requirements for logging should provide administrators additional tools to control user action on the KVMs for stricter controls in their environment. Optional elements should allow vendors to customize offerings that address additional cost points. The official ability to use a remote control to manage the KVM should pave the way for advances in ergonomics and installation methodologies that further cleanup the operator's desk and enable more efficiency and effectiveness. The advanced audio filtering requirements do add significant technical complexity and cost but now block attacks carried on outside of human audible frequency ranges.