Why use a secure KVM?

Background

By connecting everything, everywhere, the internet has become a necessity in many business and personal activities. Nowadays, all the devices that connect to the internet are exposed to cyber-attacks which are becoming more diversified every year.

Peripheral Vulnerabilities

Due to being portable, vulnerable and widely spread computer peripherals have been identified by attackers as ideal vehicles for abusing and penetrating secure environments.

The IT Challenge

Computer networks are continuously challenged by various security threats.

In an effort to protect valuable assets from reach of the outside world, organization of all kinds (Private, Health, Commercial, Financial, Government, Military…etc.) are forced to divide their internal network into multiple physical segments.

Physically separating classified and non-classified computer environments is believed to effectively provide high security, where one network is dedicated for sensitive data that is kept isolated with no connection to other networks or the internet while other networks allow some or full internet access for routine tasks such as web browsing, email access, etc.

The End User Challenge

In organizations where network segregation is implemented, employees are challenged by having to interact with multiple computers using multiple sets of keyboards video displays and mouse on their desk. Separate access to multiple systems can be time consuming for the end user and costly for the business, as it is necessary to purchase multiple monitors, keyboards and mice for each employee.

Commercial KVMs

A commercial Keyboard Video Mouse (KVM) sharing device, is a peripheral sharing switch device that is designed to allow a user to work on multiple computers using a single set of keyboard, video, mouse and audio peripherals.

Commercial KVM Vulnerabilities

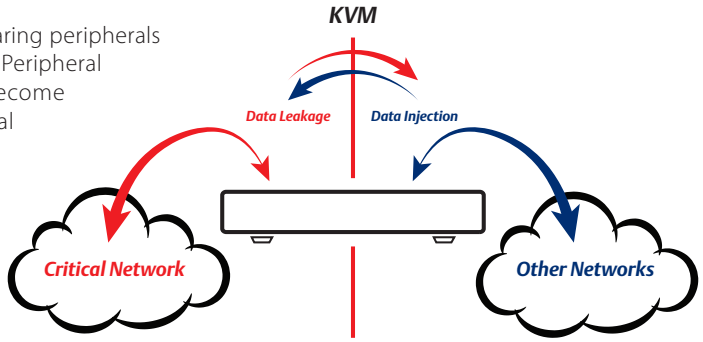
Commercial KVMs are not secure and may be abused by an attacker to cause data leakages between connected networks as they have no security mechanisms to protect against data leakage and malicious code attacks through shared USB, keyboard, video, mouse and audio peripherals.

Key Commercial KVM Vulnerability Points:

- Have none / or very weak security protection mechanisms.
- Product firmware may be tampered and replaced remotely or locally.
- Product may be physically tampered or completely replaced by a modified product.
- Product may have buffers of keyboard strokes that may be used to create a leakage.
- Display Plug and Play channel may be abused to cause data leakages.
- USB ports may be used for unauthorized peripheral devices such as mass storage devices or wireless keyboards.

The Security Risk in Peripheral Sharing

A major risk derived from the use of peripherals arises especially when sharing peripherals between computers that belong to different security classification levels. Peripheral sharing switch devices such as a Keyboard-Video-Mouse (KVM) may become mediators that share compromised / untrusted / unauthorized peripheral devices. This is a major threat as most KVMs are "touching" few networks having different security levels. Breached peripherals or KVMs may be exploited for data leakage, signaling attacks and malicious code distribution across all the computers that share them.

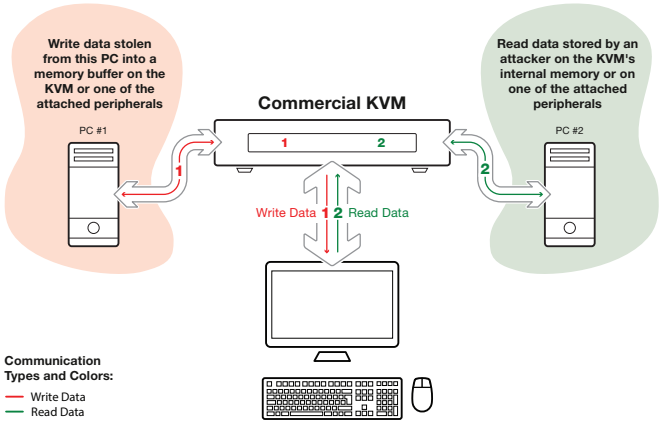


Secure KVM is the Only Solution for Safe Peripheral Sharing

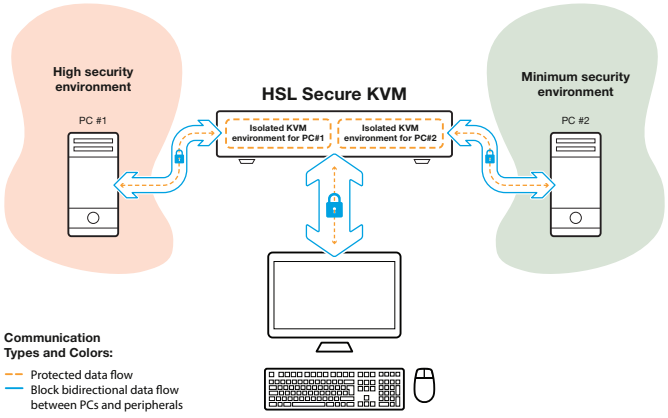
By sharing a single set of keyboard, video, mouse and audio peripherals while maintaining full isolation, secure KVM switches eliminate the need for multiple sets of peripherals when interacting with multiple computers. Secure KVMs are designed and built to protect against data leakage and malicious code attacks through shared USB, keyboard, mouse and audio peripherals.

Secure KVM - Building Blocks

- **Display Protection:** Video input interface isolation through the use of different power and ground planes, different electronic components and different emulated EDID chips per channel.
- **Audio Protection:** Audio data flow path electrical isolation and unidirectional data diodes that allow sound to travel only in one direction from the PC to the speaker.
- **Keyboard & Mouse Protection:** Accept only USB HID devices (keyboard & mice), ruling out others. Unidirectional data diodes that allow data to travel only in one direction from the devices to the computer.
- **USB Threats Protection:** Protect against data leakage, signaling and virus injection by completely blocking unauthorized USB devices and traffic.
- **Biometric/Smart-Card Reader Support:** Support user authentication across multiple isolated computers.
- **Hardware Tampering Protection:** Using tamper-proof electrical design with an internal anti tampering sub-system that triggers when the product chassis is tampered. Protect against unauthorized opening using serialized holographic labels that provide visual indication of tampering attempts.
- **Firmware Tampering Protection:** Using ROM (Read Only Memory) and One-Time-Programmable (OTP) microprocessors. Prevent data storage inside the product by having no memory buffers.



Illustration#1: *Non-secure commercial KVM - unprotected data flow*



Illustration#2: *HSL Secure KVM - protected data flow*

Secure KVM Testing & Certification

What is a protection profile for peripheral sharing switch device?

A protection profile, defined by the National Information Assurance Partnership (NIAP), is a security standard that outlines the constantly evolving threats which are aimed at IT environments through the abuse of peripherals and peripheral sharing switch devices as well as the measures of protection against them.

The NIAP PP certification validates that the switching devices have meet the strict testing and technical requirements for security mandated by the U.S National Security Agency (NSA) along with 25 other governments worldwide.

High Sec Labs Secure Peripheral Sharing Switch Devices Provide the Highest Security by Design

All NEW HSL secure KVM products are certified with the newest NIAP Common Criteria (CC) Protection Profile version 3.0 (PP3.0) certification for Peripheral Sharing Switch (PSS) devices and with EAL4+ certification.