WHITE PAPER

HSL SECURE KVM COMBINER

Hardware-Based Video Security Architecture

Ensuring Zero Data Leakage
in Multi-Computer Environments

HighSecLabs
Highest Security Solutions

HLT39128 Rev 1.0

TABLE OF CONTACTS

EXECUTIVE SUMMARY

High Sec Labs' Secure KVM Combiner represents a breakthrough in secure multi-computer operations, combining the capabilities of a KVM switch, a multi-viewer, and a scaler while maintaining the highest standards of data security. Through innovative hardware-based security mechanisms, the Combiner eliminates the risk of data leakage between computers of different security classifications and prevents unauthorized information flow from displays to host systems.

This white paper examines the comprehensive video security architecture of the HSL Secure KVM Combiner, detailing the engineering solutions that address critical vulnerabilities inherent in multi-display interfaces. By implementing physical separation, unidirectional signal conversion, and controlled EDID management, the Combiner provides unparalleled security suitable for government, military, financial, and enterprise environments where data isolation is paramount.

INTRODUCTION

THE CHALLENGE OF SECURE MULTI-COMPUTER ENVIRONMENTS

In secure operation centers, personnel routinely need to monitor multiple computers simultaneously—often systems with different security classifications displayed side-by-side on the same screen. This creates an immediate security concern: how can multiple computers share a single video display without creating pathways for data to leak between systems?

HSL's KVM Combiner addresses this fundamental challenge through a security architecture built on complete physical isolation. Each connected computer operates within its own dedicated hardware pathway, with no shared components, memory, or signal lines that could enable cross-contamination. Even when displaying multiple computers simultaneously on a single screen, each video channel maintains absolute separation from the others, making data transfer between systems physically impossible.

Traditional approaches to multi-viewing often rely on software processing or shared video memory, where multiple video streams pass through common components. The Combiner takes a fundamentally different approach: dedicated hardware channels process each video source independently before final display composition, ensuring that computer A's data never touches computer B's processing pathway.

The KVM Combiner gets its name from combining three essential functions into a single secure platform:

- **KVM Switch:** Seamlessly control multiple computers using a single keyboard, mouse, and touchscreen.
- **Multi-Viewer:** Simultaneously show multiple video sources on a single display.
- **Scaler:** Position, resize, and scale video sources for custom display configurations.

Most importantly, the Combiner achieves these capabilities while maintaining hardware-enforced security barriers that prevent data leakage or cross-contamination between connected computers.

SYSTEM ARCHITECTURE OVERVIEW

The Combiner employs a dual-interface architecture that strictly separates video and human interface device pathways:

Video Interface: Managed by the dedicated video board, controlling video switching, scaling, and multi-viewing

HID Interface: Controlled by system controller boards managing all keyboard, mouse, and touchscreen data

This document focuses exclusively on the Combiner's video security architecture. The HID security features, electrical isolation, and ground isolation mechanisms are separate subjects to be discussed in other documents.

SECURITY RISK ANALYSIS

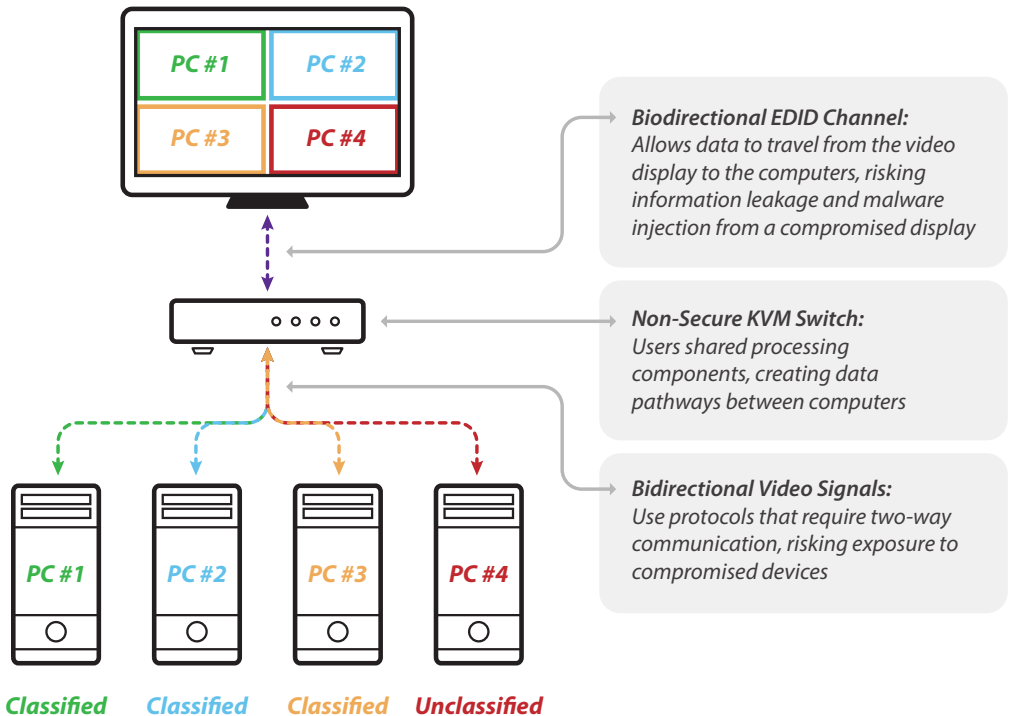

Fig 1. Overview of the risks of a non-secure KVM system

Any secure KVM system must address fundamental security vulnerabilities that arise from multiple host computers sharing video displays.

DATA TRANSFER BETWEEN COMPUTERS

The most significant security threat in multi-computer environments is the risk of data transfer between host computers. Many non-secure KVM solutions will share processing components between the host computers, creating data pathways that can potentially compromise the entire system.

INFORMATION LEAKAGE FROM THE VIDEO DISPLAY

Modern video standards incorporate bidirectional communication channels that enable displays to send information back to connected computers. While designed for enhanced functionality, these channels create security vulnerabilities that can be exploited to extract data or inject malicious code.

EDID MANIPULATION

Electronic Display Identification Data (EDID) is a mechanism that allows displays to communicate their capabilities to connected computers. This bidirectional channel creates a potential pathway for a compromised video display to be used to attack the host computers.

VIDEO PROTOCOL VULNERABILITIES

Standard video protocols such as HDMI and DisplayPort contain several features that, while useful in consumer applications, pose significant security risks in classified environments.

- **HDCP (High-bandwidth Digital Content Protection):** Content protection protocol with bidirectional authentication
- **HEAC (HDMI Ethernet and Audio Return Channel):** Ethernet connectivity over HDMI cables
- **ARC (Audio Return Channel):** Audio feedback from display to source
- **CEC (Consumer Electronics Control):** Device control commands over HDMI
- **DisplayPort AUX Channel:** Auxiliary bidirectional communication channel

Each of these protocols must be neutralized to achieve true video security.

SECURITY ARCHITECTURE

The Secure KVM Combiner utilizes comprehensive, hardware-based security mechanisms that address each potential threat by enforcing unidirectional flow of signals. This makes software-based intrusion impossible.

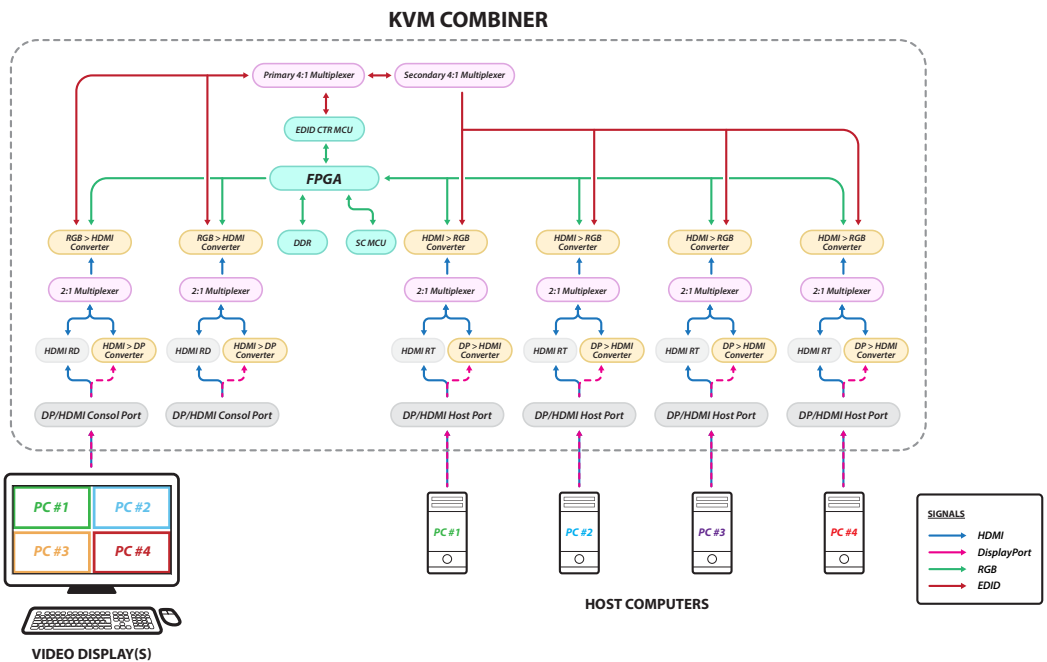

Fig 2. Diagram of the HSL Secure KVM Combiner's video board

VIDEO BOARD DESIGN

At the heart of the Combiner's security architecture is the video board, built around a central Field-Programmable Gate Array (FPGA). The FPGA receives video streams from host computers, processes them according to user commands received from the system controller MCU, and transmits the composed image to connected displays.

The video board incorporates five distinct security mechanisms that work together to eliminate all potential security vulnerabilities.

Security Mechanism 1: Physical Separation

Each host computer connects through a dedicated, independent set of electronic components. There is no pathway or shared component to transfer data between computers. This physical separation at the component level removes the risk of data from classified computers leaking into non-secure systems by making inter-computer communication impossible.

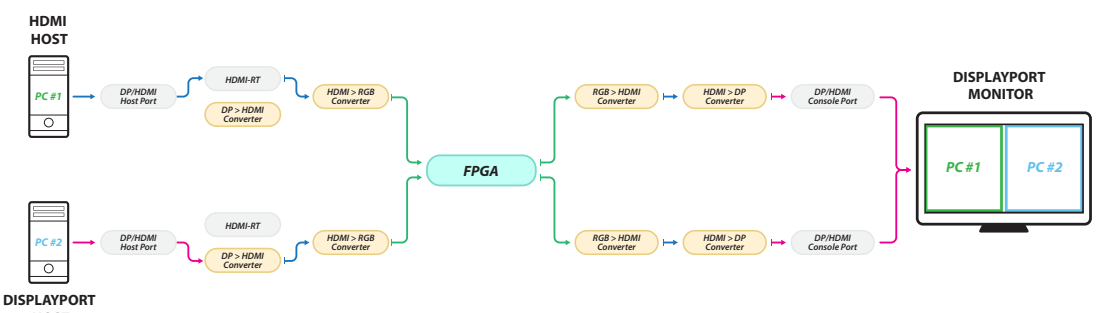

Fig 3. The paths of video signals from two host PCs traveling through the Combiner to the video display

Security Mechanism 2: DisplayPort-to-HDMI Conversion

The Combiner accepts both DisplayPort and HDMI inputs but converts DP signals to HDMI for internal processing, in accordance with NIAP's protection profile. If either the host computer or the display uses a DP output, signals are converted from HDMI to DP at the output stage. The signal converters themselves are unidirectional in nature, which enforces data flow in only one direction.

Security Mechanism 3: HDMI-to-RGB Conversion

Before reaching the FPGA, all incoming HDMI signals are converted to RGB, so the only video data passing from the host computer to the display is the color information about the image shown. These RGB signals are then converted back to HDMI on the output side, with separate unidirectional chips handling each conversion. This prevents any signals from traveling backwards through the system.

Security Mechanism 4: Physical Removal of Risky Interfaces

Specific HDMI pins and interfaces are physically absent from the video board, such as HDCP, HEAC, ARC, and CEC. These protocols are bidirectional, and simply disabling their interfaces in software would leave the possibility for malicious actors to enable them. Physically removing the pathways these protocols take prevents any possible way to establish bidirectional data flow, no matter how sophisticated the attack may be.

Security Mechanism 5: Controlled EDID Management

EDID management represents the most complex security challenge in the video subsystem. The Combiner implements a sophisticated EDID control system that maintains security while providing necessary display compatibility.

EDID Management Architecture

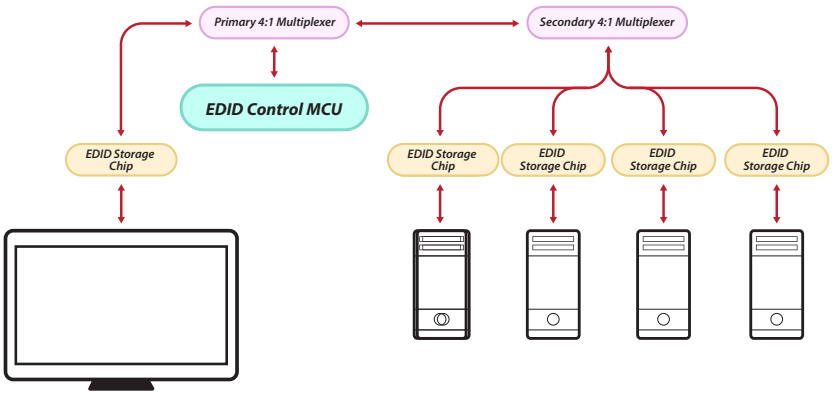

Fig 4. Diagram of the Combiner's EDID management architecture

The EDID Control MCU manages all EDID operations using dedicated hardware to enforce strict isolation between the video display and each host computer.

The system uses three key components to maintain separation:

- **Primary 4:1 Physical Multiplexer:** The Primary Multiplexer acts as the main isolation barrier, connecting the EDID MCU to either the displays or the host computers, never both simultaneously.
- **Secondary 4:1 Multiplexer:** When the Primary Multiplexer connects the EDID Control MCU to the host computers, the Secondary Multiplexer selects which individual host computer receives EDID data.
- **Dedicated EDID Storage Chips:** The HDMI/RBG converters of each host channel have their own independent EDID storage chips, ensuring there are no shared pathways between computers.

Operation Modes

The system supports two EDID modes, selected during device startup based on the KVM system's security requirements.

Mode 1: Predefined EDID (Maximum Security)

In this mode, the EDID MCU uses a predefined EDID file stored in its flash memory rather than reading from the connected display. The process works as follows:

1. All display contact is disabled.
2. The multiplexer switches to Host Mode.
3. The predefined EDID is loaded onto each host channel's dedicated HDMI-to-RGB converter.
4. Each host reads only its own EDID from its dedicated, independent chip.

This approach provides maximum security by eliminating all communication with the display, removing any possibility of display-based attacks or data exfiltration.

Mode 2: Read EDID from Primary Display (Controlled Reading)

When you need to use the actual display's capabilities, the system performs a carefully controlled read operation:

1. The multiplexer connects to the primary display.
2. The EDID MCU reads and verifies the EDID data.
3. The multiplexer switches to host mode, completely disconnecting the display.
4. The verified EDID is distributed to each host's dedicated HDMI-to-RGB converter.
5. Each host reads from its own independent interface.

After this initial read, the display is completely isolated with no ongoing communication. Host computers never directly contact the display; they only read from their own dedicated storage chips.

Critical Security Features

The EDID management system provides four critical security protections:

- **One-Time Operation:** EDID reading occurs only once at device startup. After the initial configuration, changing hosts or displays does not trigger an EDID re-reading. This prevents runtime exploitation attempts that might occur through hot-plugging displays or cycling connections.
- **Physical Isolation:** The hardware multiplexers enforce a physical either/or connection which can connect to displays or hosts, but never both simultaneously. Rather than a software limitation that could be bypassed; it is a fundamental hardware constraint that makes simultaneous communication impossible.
- **Independent Channels:** Each host computer reads EDID from its own dedicated chip with no shared components, memory spaces, or signal paths. This architectural isolation eliminates any possibility of cross-contamination between computers of different security classifications.
- **EDID Verification:** When reading from the video display, the MCU verifies the EDID structure and content before distribution. This prevents compromised EDID data from exploiting vulnerabilities in host computers' video drivers.

SECURITY VALIDATION

COMPREHENSIVE PROTECTION AGAINST IDENTIFIED THREATS

The Combiner's layered security architecture provides comprehensive protection against the fundamental threats in multi-computer display environments:

Data Transfer Between Computers

The most critical security requirement—preventing data transfer between host computers—is achieved through complete physical separation of all computer pathways. Each host channel uses dedicated components with no shared memory, processors, or signal lines. This hardware-based approach means no electrical pathway exists for data transfer between computers.

Information Leakage from the Video Display

The Combiner eliminates any communication from the video display to the host computers through multiple security mechanisms working together. Unidirectional signal converters ensure data can flow only from computers toward the display. Physically removing the pins for certain protocols prevents them from carrying signals in the wrong direction. The controlled EDID management system allows legitimate backward communication channels while keeping them from being exploited. Together, these measures make it impossible for displays to send signals back to host computers under any circumstances.

EDID Manipulation

EDID presents a unique challenge because displays legitimately need to communicate their capabilities to computers. The Combiner solves this through hardware-based isolation that physically separates display access from host access. EDID reading occurs only once during startup, and each host reads from its own dedicated storage chip rather than from the display itself. Since hosts never directly communicate with displays, EDID cannot be manipulated during runtime operations.

Video Protocol Vulnerabilities

Modern video standards include several bidirectional protocols designed for consumer convenience: HDCP for content protection, HEAC for Ethernet connectivity, ARC for audio feedback, and CEC for device control. In secure environments, these features become vulnerabilities. The Combiner physically removes the pins that carry these signals, making bidirectional protocols not just disabled but physically impossible to use. In addition, converting DisplayPort signals to HDMI eliminates the DP AUX channel entirely, removing another potential pathway for attack. An attacker cannot enable these protocols through software because the necessary hardware pathways do not exist.

CONCLUSION

High Sec Labs' Secure KVM Combiner offers operational efficiency with uncompromising security. Through its comprehensive hardware-based security architecture, the system eliminates major vulnerabilities while maintaining full KVM switching, multi-viewing, and scaling functionality.

Providing layers of physical separation, signal conversion, interface removal, and controlled EDID management creates defense-in-depth that protects against both known attack risks and potential future exploits. The use of hardware security mechanisms rather than software ensures that these protections cannot be circumvented through software attacks or configuration changes.

For environments where security cannot be compromised, the HSL Secure KVM Combiner delivers the only acceptable solution: hardware-enforced isolation that makes data leakage not just unlikely, but physically impossible.

www.highseclabs.com

High Sec Labs (HSL) develops high-quality cyber-defense solutions in the field of network and peripheral isolation for protecting national assets and infrastructure.

The company, headquartered in Or Akiva, Israel, was founded in 2008 and has a second manufacturing site in the United States.

High Sec Lab's roots are deeply embedded in the defense and commercial industries developing cyber protection solutions. Among its customers are some of the world's leading governments and defense organizations as well as commercial companies such as banks, healthcare providers, and national infrastructure companies.

HighSecLabs
Highest Security Solutions