SECURE VIDEOBAR DIODE

Eliminate the threat of eavesdropping and data breaches when sharing a videobar across multiple networks.

THREATS OF USING VIDEOBARS

- Videobars can be exploited to eavesdrop on classified and sensitive conversations, even in secure rooms.
- Wireless interfaces like Bluetooth and WiFi can be used to leak data or insert malicious code.
- Videobar memory can be exploited to transfer data between network resources.
- Backup batteries can retain data for delayed exfiltration.
- The camera and/or microphone can inadvertently leak conversations when left on.
- Speakers can be used for high-frequency data transmissions.
- Speakers can be repurposed as microphones to leak conversations.

KEY FEATURES

- **Unidirectional Data Flow**:
  - Sophisticated device emulation technology ensures there is never a direct connection between the peripherals and the host.
  - The video and audio channels are filtered and isolated separately to mitigate media specific vulnerabilities.
  - Video is sent over a unidirectional parallel bus, preventing crosstalk and data exchange between sources.
  - The Videobar Diode prevents non-audio data transfers by converting digital audio to analog, then back to digital.
  - A built-in low-pass filter restricts audio to the range the human ear can hear, preventing hackers from sending inaudible high-frequency signals to external hacking devices.
- **RS-232 Compatible**
  The Videobar Diode can be controlled by any RS-232 remote control device.
- **NIAP PP 4.0 Compliant**
  - The Videobar Diode is fully compliant with NIAP's Common Criteria PP4.0 Protection Profile.
- **Supply Chain Assurances**
  - All components are sourced from a secure supply chain.
  - The Videobar Diode is TAA/BAA compliant.

SECURITY FEATURES

- **USB Security**
  - Block unauthorized USB devices.
  - USB CAC Readers are authorized by default.
  - Whitelist and blacklist specific USB devices based on VID/PID characteristics.
- **Video Security**
  - Computer video input interfaces are isolated using different electronic components, power, and ground domains.
  - The display is isolated by a dedicated, read-only EDID emulation for each computer.
  - Access to the monitor's Extended Display Identification Data (EDID) is blocked.
  - Access to the Monitor Control Command Set is blocked.
- **Audio Security**
  - Enforce computer-to-speaker, one-way flow of sound through unidirectional optical data diodes.
  - Prevent sending high-frequency signals with a built-in low-pass filter.
  - Prevent eavesdropping and line-in re-tasking by blocking speaker-to-computer communication.
- **Firmware Anti-Tampering**
  - There is no access to the product's firmware or memory through any port.
  - Firmware is permanently stored on a non-reprogrammable Read Only Memory (ROM) to prevent any modification.
  - Firmware integrity is verified through a self-test procedure during power-up. Upon detection of a critical failure, the device disables normal operation and provides a clear visual indication of failure.

TRADE AGREEMENTS ACT TAA COMPLIANT

BAA COMPLIANT

HLT37418 Rev 1.0

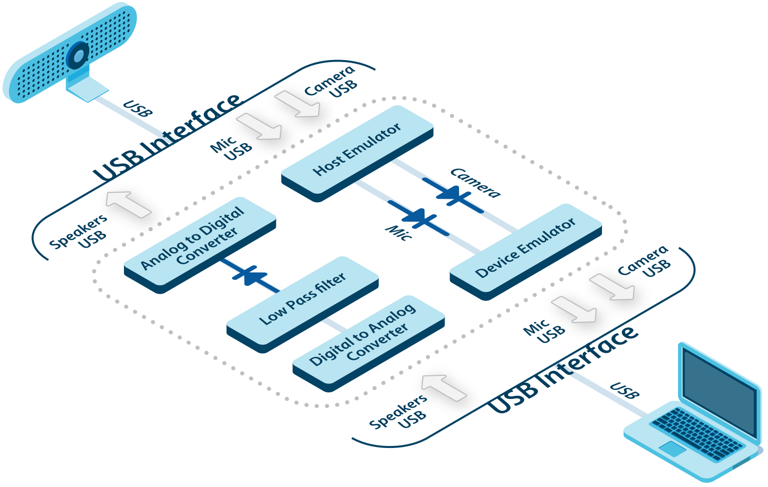
OPERATIONAL FEATURES

- **Secure Operation:**
  - The Videobar Diode enforces unidirectional data flow, making it impossible to use a videobar as a listening device or an intermediary for data transfers.
- **Easy to Install and Operate**:
  - The Videobar Diode does not require any software drivers to operate; simply connect the diode to the videobar and host PC.
- **Push-button Controls**
  - The video and audio channels are closed by default. They can be opened and closed manually via a push button with a colored light indicating the open/closed state of the channels.
- **Configurable Time-outs and Extensions**
  - An automatic time-out disconnects the audio and video channels after a set amount of time, preventing channels from being left open accidentally.
  - The Diode will send visual and audio indications of an upcoming time-out.
  - Pressing the push-button before a time-out will extend timed-out disconnect.
  - The amount of time before a time-out, the warning time before a time-out, and the number of allowed extensions are fully configurable by the user.

SPECIFICATION

PART NUMBER	FS11USB2
FEATURES	
Input Interface (Host)	USB 2.0 Type B
Output Interface (Videobar)	USB 2.0 Type C
Remote Control Unit Port	4-pin RS-232 Port
Configuration Port	Micro USB
PHYSICAL	
Dimensions	104x28x140mm / 4.1x1.1x5.5in
Weight	0.3kg / 0.64lbs
ENVIRONMENTAL	
Operating Temperature	0°C to 40°C / 32°F to 104°F
Storage Temperature	-20°C to 60°C / -4°F to 140°F
Operating Humidity	20% to 80% non-condensing
Storage Humidity	10% to 90% non-condensing
Altitude	0 to 10,000 ft
POWER	
Power Requirements	12VDC 1.5A
AC Input	100 to 240V AC
Power Source	External
SECURITY	
Compliance	Compliant with NIAP Common Criteria PP4.0 PSD
GENERAL INFO	
Manufactured	TAA and BAA Compliant
Product Life-Cycle	10 Years
Warranty	2 Years

ORDERING INFORMATION	FS11USB2
Model Number	FS11USB2
Part Number	CPN35322



Specifications are subjected to change without prior notice. Patents: www.highseclabs.com/patents/. HLT37418 Rev 1.0