THE USB eLOCK PRODUCT LINE

Centrally Authenticated USB Port Blocking and Filtering Suite

HighSecLabs
Highest Security Solutions

Patent Pending - Under NDA

HLT31321 Rev 1.1

The Problem / Need

USB is Everywhere

HighSecLabs
Highest Security Solutions

The Basic USB Paradox

Completely blocking all USB Ports
MAKES A PC UNUSABLE

But Leaving USB ports open
MAKES A PC VULNERABLE

HighSecLabs
Highest Security Solutions

The Risk

2000-2019 Most Popular Suspects Involved in Data Theft Events:

- Open USB ports
- Users
- Visitors
- Technicians
- Administrators
- Peripheral devices / vendors / supply chains

HighSecLabs
Highest Security Solutions

Characteristics that Make USB a Threat

- **Multifunctional port**
  Numerous device types can connect through the same physical port.
- **Highly popular standard commonly used by manufacturers**
  Implemented in numerous computer peripherals (keyboards, pointing devices, printers, disk drives, network adapters, digital cameras…etc).
- **Supported by all computer and mobile operating systems**
  Plug & Play with Windows, Linux, Mac, Android, iOS, Windows Phone.
- **Allows on-the-fly high-speed bidirectional connectivity**
  Huge databases can be downloaded in a matter of seconds or minutes.
- **Exposed when used on bare-metal PC or server**
  Can be exploited through use of computers or servers that are virtualized or have no OS.

The Threat

Why Should Organizations Filter USB Activity?

- Many data theft / malicious code injection events involve USB ports.
- Users will always attempt to connect USB devices to corporate PCs.
- USB devices are a fertile ground for malicious attacks.
- USB may be abused by trusted administrators having the **highest system privileges.**
- Users are unaware of the potential risks derived from infected USB devices and are accustomed to using USB everywhere.
- BYOD (bring your own device) exposes corporate IT to personal device security flaws.
- Peripheral devices cannot be trusted.

HighSecLabs
Highest Security Solutions

Current Solutions

Popularity	Method	Weaknesses
#1	Software to control and monitor USB, Policy	• Similar to anti-virus – fights yesterday's wars • Does not protect against technicians / administrators • OS dependent – may not be efficient for virtualized platforms • Does not protect against bad peripherals • Does not protect during boot
#2	Policy, training (prevent users from bringing USB devices)	• Not feasible anymore • Users will always violate such policies • Does not protect against inadvertent connection
#3	Circumventing the PC by blocking USB ports	• No PS/2 ports anymore • What will you do with the authorized devices? • Expensive and not efficient

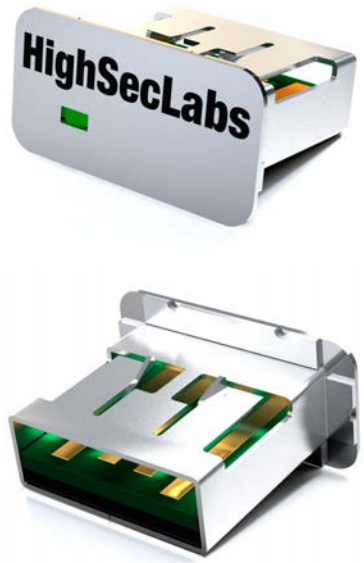
» There is a critical need for a method that will block and monitor 100% of the USB ports in the organization «

HighSecLabs
Highest Security Solutions

USB eLOCK Concept

The 2 Elements of the eLock Solution

Blocking - USB Plug



Filtering - USB Filter

USB eLOCK Concept

System Highlights

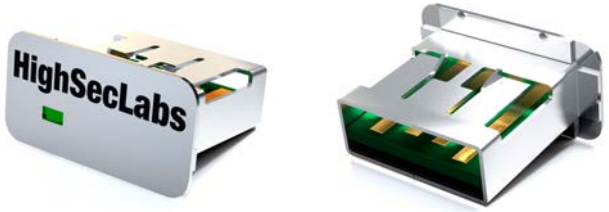
- Secures all computer and server USB ports from unauthorized use.
- Combines hardware (physical) and software means.
- Mechanically locks USB ports – prevents inserting USB devices during work and boot time.
- Allows only a USB keyboard and mouse through a secure hardcoded USB filter.
- Configurable USB peripherals filter to support authorized USB devices other than keyboards / mice.
- Supports both standalone & centrally managed deployment scenarios.

HighSecLabs
Highest Security Solutions

USB eLOCK Details

eLock USB Plug

- **USB Plug:**
  Electronically tagged mechanical USB port that physically locks individual USB ports. Forced removal permanently damages the USB port.



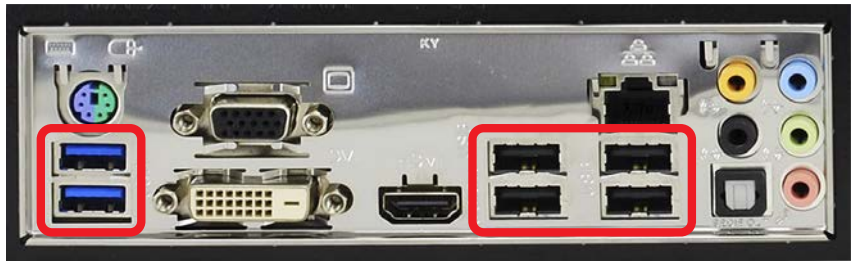
- **Steel Plate Extension:**
  Blocks multiple USB ports with only one eLock USB plug.
  Mount the metal plate together with the USB eLock Plug to block a group of USB ports.

USB eLOCK Details

How does USB eLock Secure USB Ports? (Physical Layer)

Prevents physical access to USB ports by installing a USB Plug with a metal plate extension

Exposed USB ports



Protected USB ports

USB plug with metal plate extension

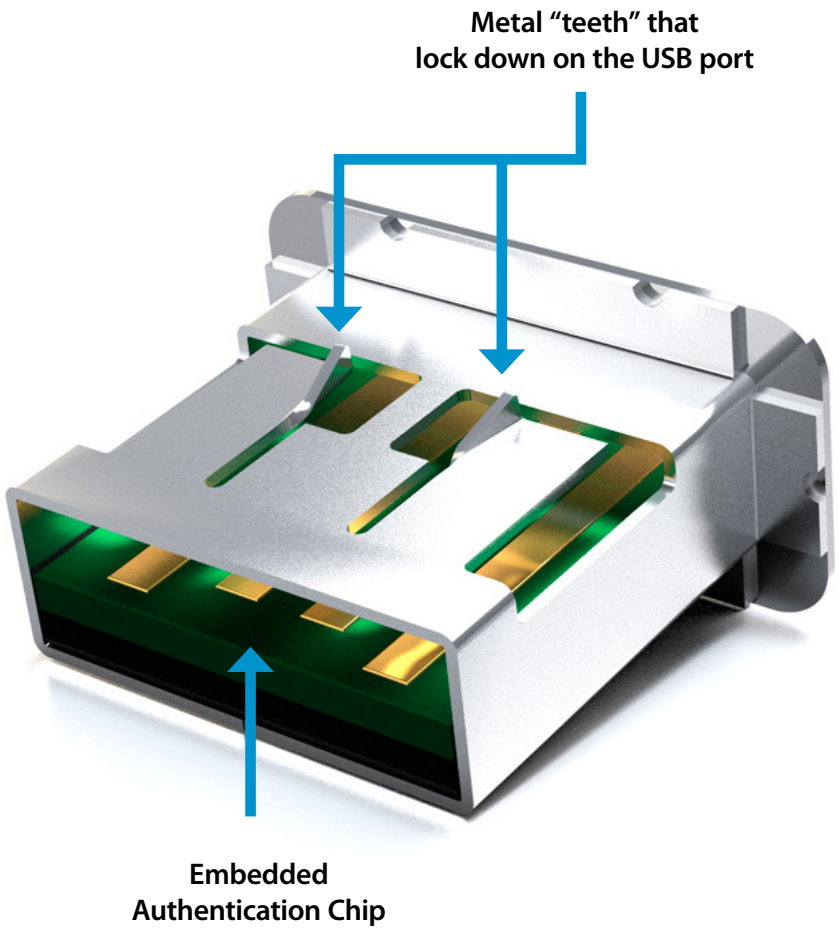
USB plug with metal plate extension

HighSecLabs
Highest Security Solutions

USB eLOCK Details

Prevent removal by metal "teeth" lockdown

- The USB plug has two metal "teeth"
- Once the plug is inserted and one tries to remove it, the "teeth" physically block removal
- If force is used, the plug can be removed only at the price of rendering the USB port inoperable!



HighSecLabs
Highest Security Solutions

eLock USB Port Filter

Overview

- Designed to allow secure connection of two approved USB devices to the computer.
- Physically mounts and locks on a standard USB port via metal “teeth”.
- Forced removal damages the USB port.

eLock USB Filters

Hardcoded HID Filter

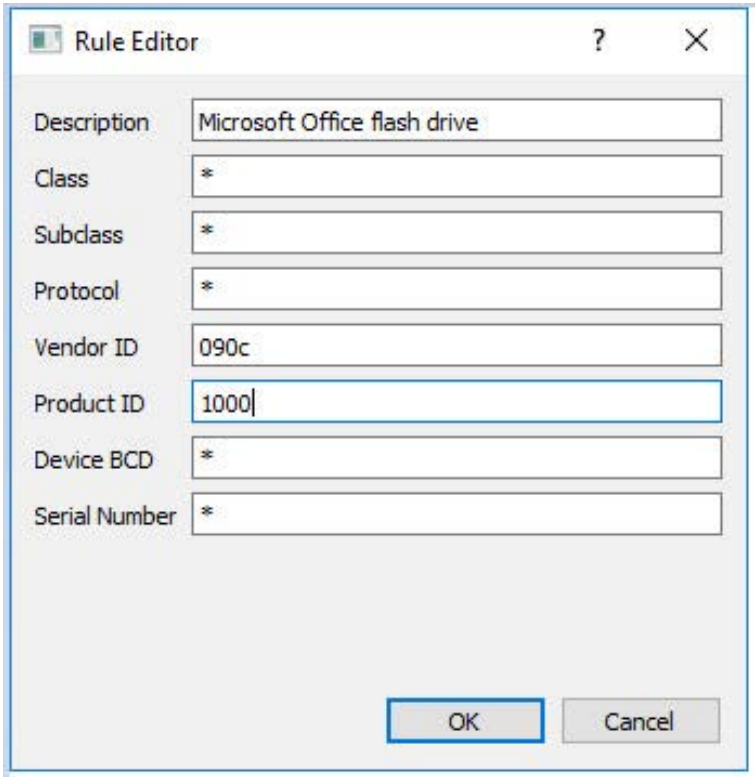
- Accepts only USB HID Devices (Keyboard/Mice) and rules out others
- Passes only standard keyboard and mouse reports
- Blocks all other traffic
- Highly secure, read-only non-programmable chip

Configurable Filter

- USB-ID-based filter
- Accepts USB devices based on unique identifiers such as Serial/HID/VID/Class ID, etc.
- Configurable identifiers to fit with specific customer peripherals

USB eLOCK Details

Screen Capture of Filter Whitelist…



HighSecLabs
Highest Security Solutions

USB eLOCK Details

How Does it Work?

1. Connect USB devices to the filter.
   - Keyboard/mouse in case of the HID filter
   - Any authorized USB device in case of the configurable filter
2. Connect the filter to any PC USB port
3. Use the USB Plug to block all remaining USB ports

HighSecLabs
Highest Security Solutions

Application Example – Point of Sale

HighSecLabs
Highest Security Solutions

Keyboard and Mouse Threats

#	Attack Type	Vulnerability	Risk
	Signal/Virus	• Programmable components may include malicious code and are vulnerable to manipulation. • May include memory chips that can store data. • Bi-directional keys (Num Lock, Scroll Lock, Cap Lock, Pause Break) can be used to send and decode data between systems.	Data leakage and malicious attacks through shared USB, keyboard and mouse peripherals.

HID Filter

Solution Components	Solution Highlights
Unidirectional Optical Data Diodes	✓ Allowing data to flow only in one direction, from the device to host computer. ✓ Preventing host-to-peripheral data flow eliminates data leakage through the shared peripheral.
Hardware-based Peripheral Isolation per Port	✓ Each port is fully isolated from other ports.
Hardcoded HID Filter	✓ Accepts only USB HID Devices (Keyboard and mice) rules out others. ✓ Hardcoded ASCII keyboard/mice characters. ✓ Incapable of processing any other code than HID-ASCII.

HighSecLabs
Highest Security Solutions

USB Threats

#	Attack Type	Vulnerability	Risk
	Virus	• Highly popular standard commonly used by computer and mobile users. • Provides on-the-fly high-speed, bi-directional flow of data to and from the computer. • Multifunctional port: numerous device types can connect through the same physical port. • Programmable components may include malicious code and are vulnerable to manipulation. • Can be used to store/inject data.	Data leakage and malicious attacks through shared USB, keyboard and mouse peripherals.

	Solution Components	Solution Highlights
eLock	**Block Unauthorized USB**	✓ Completely block and disable unauthorized USB devices and traffic.
HID Filter	**Secure & Dedicated Keyboard/Mouse Ports**	✓ Accepts only USB HID Devices (Keyboard & Mice) rules out others. ✓ Refer to Keyboard and mouse threats table for additional information.
	Biometric/Smart-Card reader support	✓ Special secured port (fUSB) for smart-card/biometric reader to support user authentication.

HighSecLabs
Highest Security Solutions

HARDWARE & FIRMWARE TAMPERING THREATS

#	Attack Type	Vulnerability	Risk
	Firmware Reprogramming / Implant Malicious Hardware	• Open product and implant malicious hardware. • Attempt to reprogram firmware components to include malicious code. • Attempt to store/inject data.	Data leakage and malicious attacks through shared USB, keyboard and mouse peripherals.

HID Filter

Solution Components	Solution Highlights
Tamper-proof Electrical Design	✓ Firmware is stored on ROM (Read Only Memory). ✓ One-Time-Programmable (OTP) microprocessors preventing firmware tampering/rewrite.
No Memory Buffers	✓ Peripheral signals are passed-through, with no data stored inside products.
Always-ON Tamper Evident System	✓ **External:** Serialized holographic labels provide a visual indication of any tampering attempt and warning labels are placed on the product chassis.

HighSecLabs
Highest Security Solutions

HID Filters Models

Mfr. Part Number	Model	Full Description
CPN28791	FH10N-N-4	USB eLock HID filter without locking teethes
CPN19435	FH10N-4	USB eLock HID filter with locking teethes
CPN19437	FC10N-4	USB eLock Configurable Filter

THANK YOU

HighSecLabs
Highest Security Solutions Ltd.

For more information, please visit www.highseclabs.com