Richard P. Feynman Center for Innovation

LA-UR-25-28988

Technology Snapshot

Automatic Peripheral Device Disconnection

A deployable LANL-developed capability for automatic USB control in secure computing environments

Applications

Sectors: cybersecurity, secure computing, classified operations

Areas: peripheral device control, endpoint hardware security, secure conferencing

Industries: government, defense, critical infrastructure, secure enterprise systems

Markets: high-assurance workstation security, physical USB-layer protection, operational risk mitigation

Partnership Opportunities

LANL is seeking partners to evaluate, integrate, or further develop this capability for specific operational settings. Ideal collaborators include secure hardware manufacturers, defense-focused integrators, or organizations managing sensitive computing environments.

Technology Readiness Level 5

A prototype unit has demonstrated autonomous USB disconnection with dynamic threshold logic and verified operation across multiple webcam models.

IP Information

This technology is patent pending.

Contact Information

For inquiries, contact FCI at licensing@lanl.gov.

Overview

In high-security and classified environments, webcams and similar USB peripherals pose ongoing privacy and security risks. When left connected, these devices can remain powered and exposed, even after meetings end, introducing the potential for unintended surveillance or exploitation.

To address this, LANL has developed a compact hardware-based capability that automatically disconnects USB devices when no longer in use. By monitoring real-time power draw, the system identifies idle states and enforces a physical disconnection, eliminating reliance on manual intervention or software safeguards.

Advantages

- Automatically disconnects USB webcams and peripherals with no user input
- Adapts in real time to different devices using a dynamic cutoff threshold
- Prevents false disconnects through onboard hysteresis filtering
- Provides a hardware-level status indicator immune to software tampering
- Eliminates reliance on operating system permissions or manual disconnects
- Reduces the risk of security violations in classified or sensitive environments
- Functions as a standalone drop-in with no software dependencies

Technology Description

The LANL-developed device uses real-time power monitoring and a dynamic cutoff threshold to detect when a webcam becomes idle. Instead of relying on fixed values or user calibration, the system calculates a moving average of power consumption and adapts its threshold accordingly. This allows it to work seamlessly across a wide range of webcam models and conditions.

To prevent false disconnects caused by momentary power dips, the system incorporates hysteresis logic, requiring sustained low readings before triggering. Together, these features enable consistent, autonomous operation without software drivers or manual tuning.

Continued on next page

DISCLAIMER: THE INFORMATION PROVIDED IS FOR INFORMATIONAL PURPOSES ONLY. THE TECHNOLOGY, RESEARCH, AND INTELLECTUAL PROPERTY DESCRIBED ARE SUBJECT TO ONGOING RESEARCH AND DEVELOPMENT AT LOS ALAMOS NATIONAL LABORATORY, AS MANAGED AND OPERATED BY TRIAD NATIONAL SECURITY, LLC (TRIAD). TRIAD AND ITS MEMBERS, OFFICERS, EMPLOYEES, AND AGENTS, SPECIFICALLY DISCLAIM ANY REPRESENTATION, WARRANTY, OR GUARANTEE AS TO THE SAFETY, EFFICACY, USEFULNESS, BENEFIT, PERFORMANCE, SUCCESS, OR ANY PARTICULAR OUTCOME OF THE TECHNOLOGY, RESEARCH, OR INTELLECTUAL PROPERTY RELATING HERETO, IN WHOLE OR IN PART.

Technology Description, **Continued**

An LED status light confirms webcam activity in real time. Controlled directly by the hardware, the indicator cannot be overridden by malware or firmware exploits. The platform-independent design requires no host-side software and functions as a plug-and-play drop-in to secure workstations.

Market Application

This capability supports organizations that require continuous enforcement of visual privacy and data protection at the hardware level.

Potential uses include:

- Government and defense workstations enforcing classified conferencing security
- Critical infrastructure operators managing restricted-access environments
- Telehealth systems requiring automated privacy controls for HIPAA compliance
- Enterprise IT environments seeking to reduce data exposure risk from webcams
- Security-conscious end users in financial, legal, or research roles

Next Steps

LANL is offering this capability for evaluation and further development. Partners may explore operational testing, adapt the design to specific form factors, or integrate it into hardened endpoint security solutions.

DISCLAIMER: THE INFORMATION PROVIDED IS FOR INFORMATIONAL PURPOSES ONLY. THE TECHNOLOGY, RESEARCH, AND INTELLECTUAL PROPERTY DESCRIBED ARE SUBJECT TO ONGOING RESEARCH AND DEVELOPMENT AT LOS ALAMOS NATIONAL LABORATORY, AS MANAGED AND OPERATED BY TRIAD NATIONAL SECURITY, LLC (TRIAD). TRIAD AND ITS MEMBERS, OFFICERS, EMPLOYEES, AND AGENTS, SPECIFICALLY DISCLAIM ANY REPRESENTATION, WARRANTY, OR GUARANTEE AS TO THE SAFETY, EFFICACY, USEFULNESS, BENEFIT, PERFORMANCE, SUCCESS, OR ANY PARTICULAR OUTCOME OF THE TECHNOLOGY, RESEARCH, OR INTELLECTUAL PROPERTY RELATING HERETO, IN WHOLE OR IN PART.