SEPIO | Attack Study

Instruments Under Siege:

The Hidden Cyber Risk in Testing Equipment

Industry

Defense

Scenario

Manipulated peripheral in air-gapped environment via compromised supply chain.

Attack Tool

Microsoft mouse with Raspberry Pi module inside.

Duration

Undetected within environment for several months.

Challenge

The infected mouse, when connected, was detected by the host PC as a functional approved mouse and HID keyboard – USB Class 3, Subclass 1, Protocol 1

Result

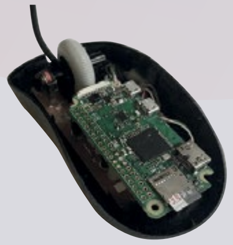
The mouse was programmed to run a PowerShell script which built and executed a hidden communication channel using the wireless interface of the Raspberry PI, bypassing the air-gapped environment. Calibration files were modified.

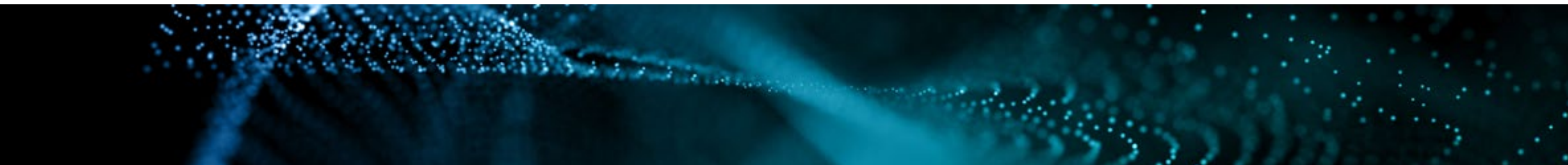
Sepio's Solution

Sepio detected the attack tool by collecting physical layer 1 information on the endpoint which determined the presence of the infected peripheral device. The physical layer 1 information provided information on which endpoint machine the device was connected to which accelerated the investigation.

Compromised USB mouse

Implanted Raspberry Pi Zero W





In many factories and labs, test and measurement equipment is treated as gospel. If the analyzer, scope, or tester says "pass," the product moves forward - often into safety-critical environments. But more and more, that "objective truth" depends on devices that are not protected by any reliable security screening solution.

On behalf of Sepio, this article highlights the broader cyber risk posed by compromised testing equipment, using the manipulation of calibration files via malicious USB as one concrete example.

Testing equipment: the perfect blind spot

Production lines, R&D labs, and certification facilities rely on a range of instruments:

- VNAs, spectrum analyzers, oscilloscopes
- Automated test equipment (ATE) and boundary-scan rigs
- Calibration benches and reference standards

These systems are often: Running outdated OS versions or vendor-locked firmware Exempt from standard IT hardening and EDR for "stability" reasons Routinely accessed with USB sticks for scripts, logs, and calibration files That combination makes them ideal targets. Attackers don't need to breach the ERP, source code repo, or production network if they can quietly compromise the measurement chain itself.

When calibration becomes an attack

Calibration files define how a vector network analyzer interprets calibration standards—open, short, load, through, etc. They underpin error correction, making sure the instrument's measurements reflect physical reality.

A malicious USB device capable of modifying files on the tester can: Identify calibration definition files.

Adjust parameters (e.g., reflection coefficients, frequency ranges) by small, controlled margins.

Leave the user interface and logs appearing "perfectly calibrated."

The result: the instrument now produces systematically biased "truth." Every device under test looks compliant against a shifted baseline, while no obvious alarms are triggered.

This is just one example. The same approach can target:

- Golden reference waveforms or mask files.
- Test limit tables and pass/fail thresholds
- Automation scripts that define measurement sequences
- Consequences for manufactured equipment.

When testing equipment is compromised and no security screening is in place, the downstream impact can be severe:

- **Field failures and safety risks.** Devices that are out of RF, power, or timing spec can still be shipped as "good." In automotive, medical, aerospace, or critical infrastructure, that can translate into safety incidents, degraded reliability, and hard-to-reproduce failures in the field.
- **Regulatory and compliance exposure** Many industries depend on traceable calibration and validated test processes (e.g., ISO, IEC, industry-specific standards). If it's later discovered that instruments were effectively "lying," organizations may face recalls, fines, and legal claims—even if their documented procedures appeared correct.

Corrupted root of trust in QA

QA and manufacturing engineering teams assume that if a board fails, the board is wrong—not the instrument. A poisoned instrument inverts that trust. Whole lots can be skewed, while traditional root-cause analysis keeps chasing design, component, or process issues instead of the test bench.

Forensic dead ends

Because the attack manipulates configuration and calibration data, not firmware signatures or visible UI, standard cyber forensics often misses it. Logs look normal; checksums of application binaries match; yet the physics of the measurements have been shifted.

Why this happens: security doesn't "live" on the test bench

Most security programs focus on:

- Endpoints (PCs, servers)
- Applications and cloud services
- IT and OT network traffic

Test equipment falls through the cracks:

- Often sits on isolated VLANs or lab networks with minimal monitoring
- Rarely runs modern EDR/AV, and when it does, policies are relaxed to avoid "interference"
- USB ports and hardware peripherals are unmanaged and unmonitored

In this environment, a malicious USB that appears as standard removable media—or as a composite device (storage + HID, for example)—can easily bypass basic controls, especially when no specialized hardware security solution is in place.

Conclusion

Calibration files manipulation illustrates a broader, uncomfortable truth: if you don't protect your testing equipment with reliable security screening, you are trusting production quality, safety, and compliance to devices that an attacker can quietly subvert.

By extending Zero Trust principles down to the hardware layer of lab and production test benches, Sepio helps organizations see what they've been missing—and restore integrity to the tools that define their manufacturing reality.

// How Sepio closes this gap

With AssetDNA and Zero Trust Hardware Access, Sepio enables organizations to:

- **Discover** and classify every device on test benches
- **Sepio identifies** USB and network-connected hardware based on physical-layer characteristics, not just spoofable identifiers like MAC or VID/PID.
- **Enforce** strict hardware access policies
- Define which USB devices and peripherals are allowed to connect to specific test stations and calibration equipment. Unknown or rogue devices can be blocked outright or quarantined.
- Detect anomalous or spoofed devices

Malicious USBs that present themselves as "just a thumb drive" can be flagged when their AssetDNA does not match known, trusted devices—even if their logical identity looks benign.

Integrate with existing security tooling

Sepio can feed alerts into SIEM/SOAR, NAC, and other platforms so that test equipment is treated as a first-class security asset, not an afterthought.

The goal is simple: make sure the instruments that define "pass" or "fail" are themselves continuously verified and protected at the hardware level.