SEPIO

Zero Trust Hardware Access

USE CASE

BACKGROUND

A large corporate bank identified a suspicious transaction within the enterprise. Upon further investigation, it was discovered that the palm-vein scanner used for biometric authentication was compromised and, subsequently, granting unauthorized access. As a result of the compromise, the bank's Zero Trust (ZT) model was at risk of being circumvented due to its reliance on identity-based access control.

ATTACK STUDY

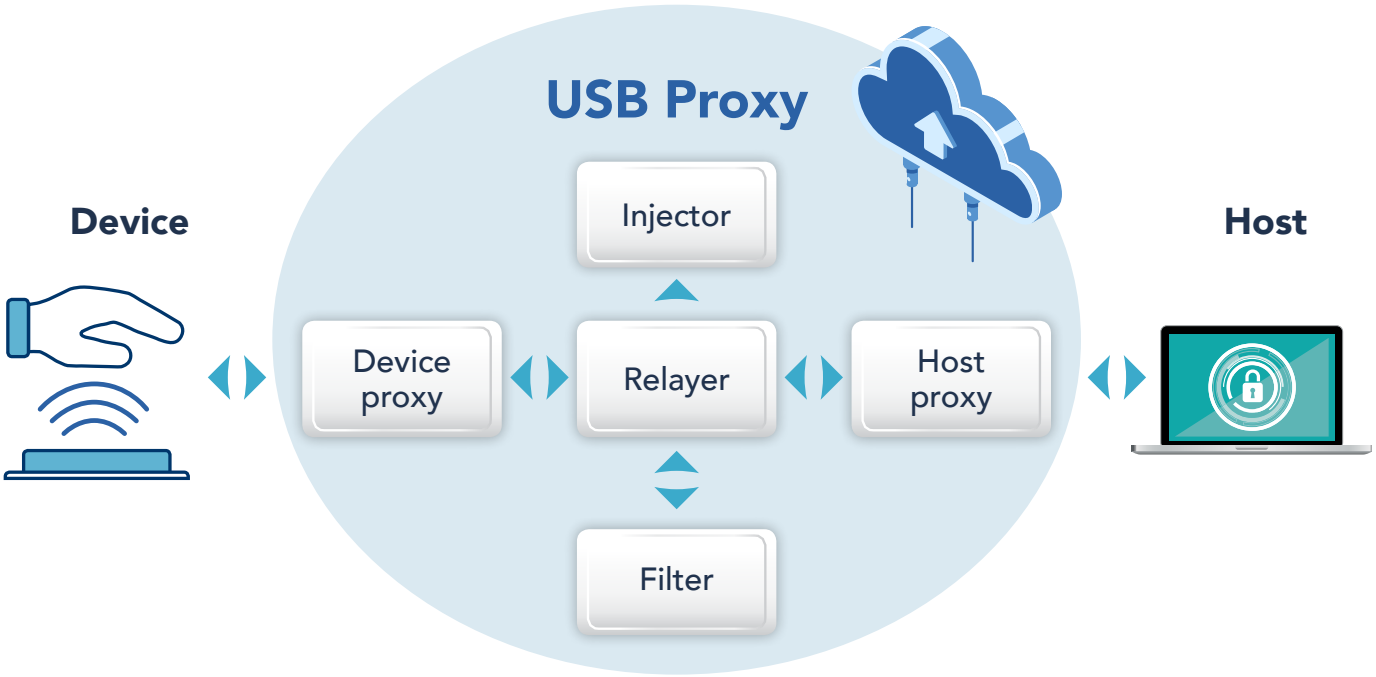
Zero Trust is a network security model based on the principle of "never trust, always verify". By acknowledging that threats not only originate outside the organization's perimeter but also within, ZT eliminates the component of trust that was once automatically given to internal users and devices. Every user and device, internal or external, must be authenticated and authorized before granting access to an enterprise's resources and data.

The effective enforcement of Zero Trust relies on the accurate authentication and authorization of devices. Hence, the organization must have complete asset visibility and the relevant tools in place to detect malicious activity originating from hardware devices. However, attackers have found success in bypassing such security measures through the use of Rogue Devices. Spoofed Peripherals are able to evade Endpoint detection software by impersonating legitimate HIDs through Physical Layer manipulation, which such security software does not cover. In this case, by impersonating a legitimate device, the attacking tool was approved and verified since it raised no alarms to any Endpoint detection tools. As a result, the attacker was able to bypass biometric authentication.

TOOLS USED

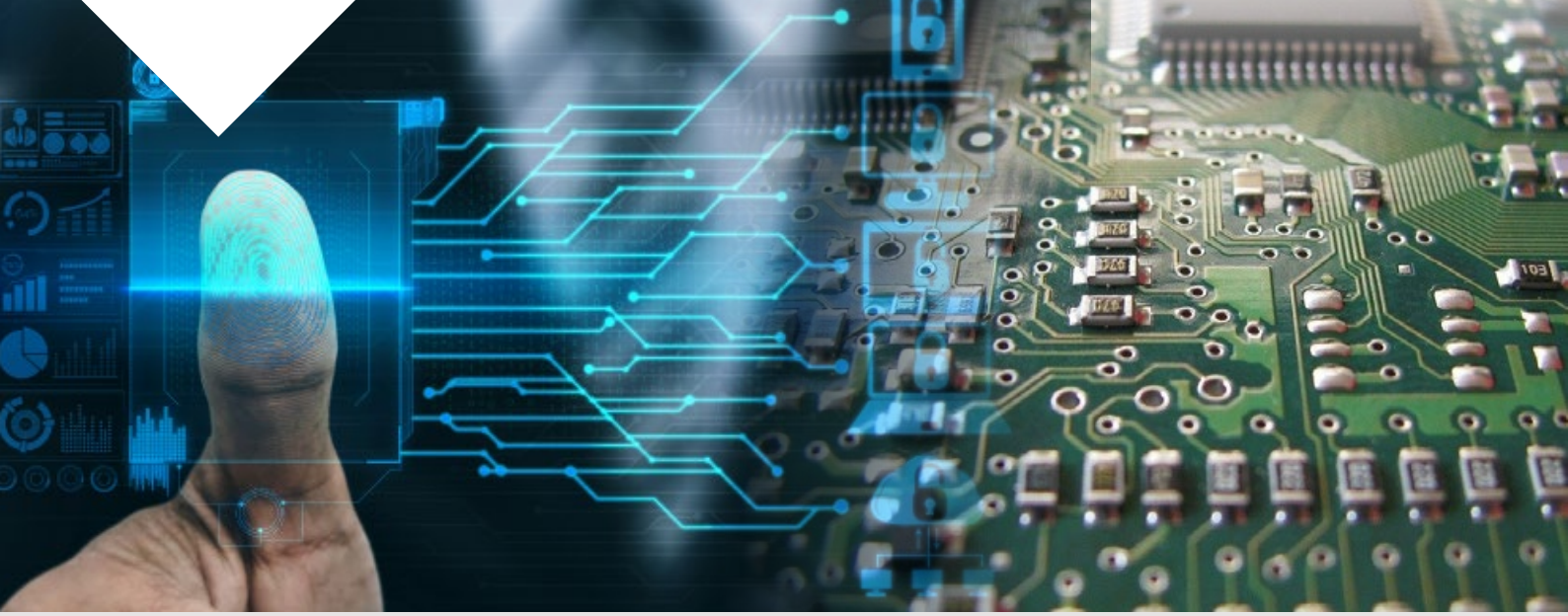
In this incident, the perpetrator used a BeagleBone board running USBProxy to carry out the MiTM attack. The tool was attached between the biometric scanner (the device) and the computer system which stores the records of genuine handprints (the host).

One-time physical access to attach the Rogue Device gives the attacker remote access to carry out the actual attack.



These four plug-ins allow the perpetrator to intercept the communication between the host and the device. By modifying the packets in transit, the attacker manipulated such communication (without either entity knowing), bypassing the authentication process as the host believes access should be granted.

The USBProxy goes undetected as it operates on the Physical Layer, which existing security solutions do not cover. This lack of visibility allows the attack to persist for an extended period, giving the malicious actor time to move laterally throughout the network by continuously bypassing the biometric authentication measure that separates network access requests.



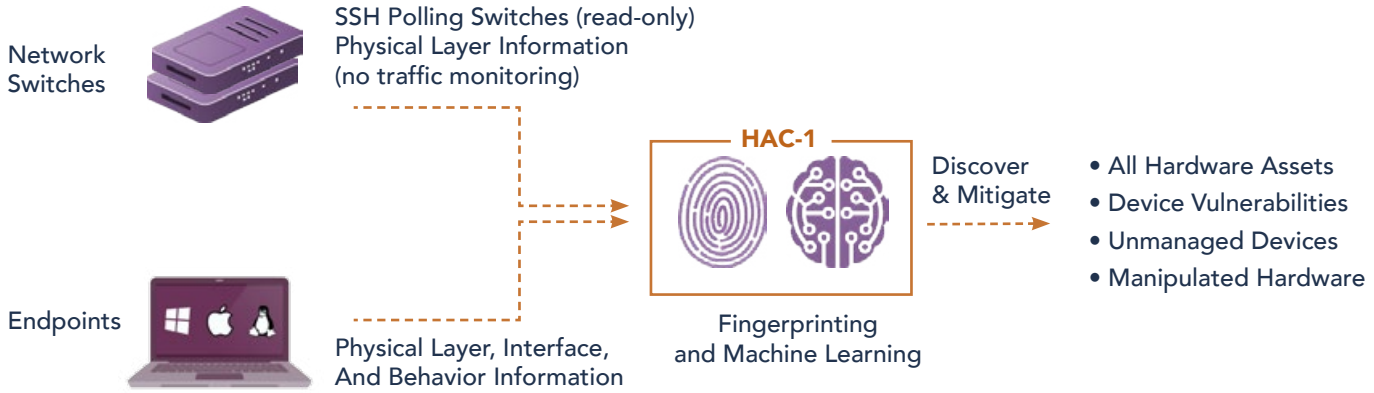
HAC-1 SOLUTION

Sepio Systems' Hardware Access Control solutions (HAC-1) provides a panacea to the gap in device visibility. As the leader in Rogue Device Mitigation, Sepio's solution identifies, detects, and handles all peripherals; no device goes unmanaged.

HAC-1 uses Physical Layer fingerprinting technology and Machine Learning to calculate a digital fingerprint from the electrical characteristics of all devices and compares them against known-to-be-vulnerable devices through its extensive built-in threat intelligence database.

In doing so, HAC-1 not only detects all managed, unmanaged, and hidden devices operating within the enterprise's infrastructure but reveals devices' true identity. The comprehensive policy enforcement mechanism recommends best practice policy and allows the administrator to define a strict, or more granular, set of rules for the system to enforce. When a device breaches the pre-set policy, HAC-1 automatically instigates a mitigation process that instantly blocks unapproved or Rogue hardware, stopping the perpetrator from bypassing micro-segmentation and other ZT security measures. With HAC-1, organizations benefit from Zero Trust Hardware Access whereby the principle of "never trust, always verify" is applied at the first layer of defense, the Physical Layer, enhancing the overall efficacy of the Zero Trust Architecture.

How It Works



HAC-1 - Visibility & Security of Hardware Assets

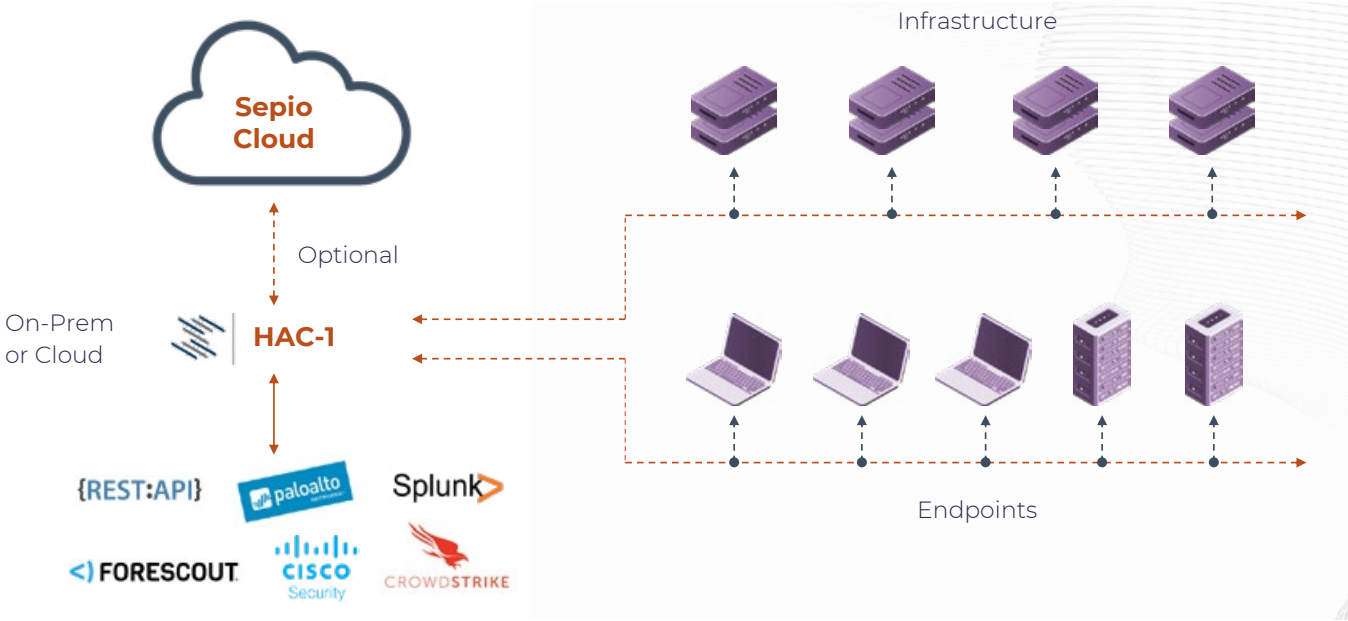
Main Benefits

Complete Visibility of all Hardware Assets: With all devices and anomalies detected, enterprises benefit from a greater overall cybersecurity posture. Gaining full visibility of all hardware devices from endpoint peripherals to connected devices (IT/OT/IoT), Sepio uses unique physical layer hardware fingerprinting technology and data augmentation from endpoints and networks.

Full Control through Predefined Policies: Enterprise-wide policies enable compliance, regulation and best practices. With predefined templates and no baselining or whitelisting, and no requirement for a clean environment start, Sepio provides a fast and easy setup.

Rogue Device Mitigation (RDM): Threat mitigation upon discovery of rogue or threatening devices. Integrations with existing security platforms such as NACs and SOARs for mitigation and remediation enhancements.

System Architecture



LEARN MORE

SEPIO