SEPIO

Hackers Bypass Biometric Sensors

CASE STUDY

BACKGROUND

A large corporate bank, using palm-vein biometric authentication, found that their scanner had been compromised and wrongful access was being granted to unauthorized personnel.

The discovery was made by a third-party security system who was able to detect that a device violation was present, in addition to the location of the foreign device; in this case the palm-vein scanner.

ATTACK STUDY

We can authenticate and identify an individual in 3 different ways; by what you know (such as a password, or personal identification number); by what you have (such as a one-time password (OTP) or a smart card); and by who you are (your physical characteristics, such as a fingerprint). This last method is known as biometric authentication.

Biometric authentication has been prevalent for decades and comes in various forms such as fingerprint recognition, eye scans, typing patterns and palm geometry.

Fingerprint recognition is the most common among biometric authentication and, what was once only used by high profile agencies needing maximum security, can now be found on everyday devices such as smartphones and laptops.

Nonetheless, hackers are finding increasingly devious ways to bypass this type of biometric authentication. Similar to physical locks having a master key, fingerprint scanners have what is known as a "master print". By simply obtaining access to this, attackers can bypass fingerprint authentication. A more complex way to do this is by using a biometrics software called Verifinger. With close up images of an individual's finger, from multiple different angles to gain a complete picture, Verifinger can allow an attacker to duplicate their victim's fingerprint which is then replicated into a wax or wooden hand that can be used to manipulate fingerprint recognition.

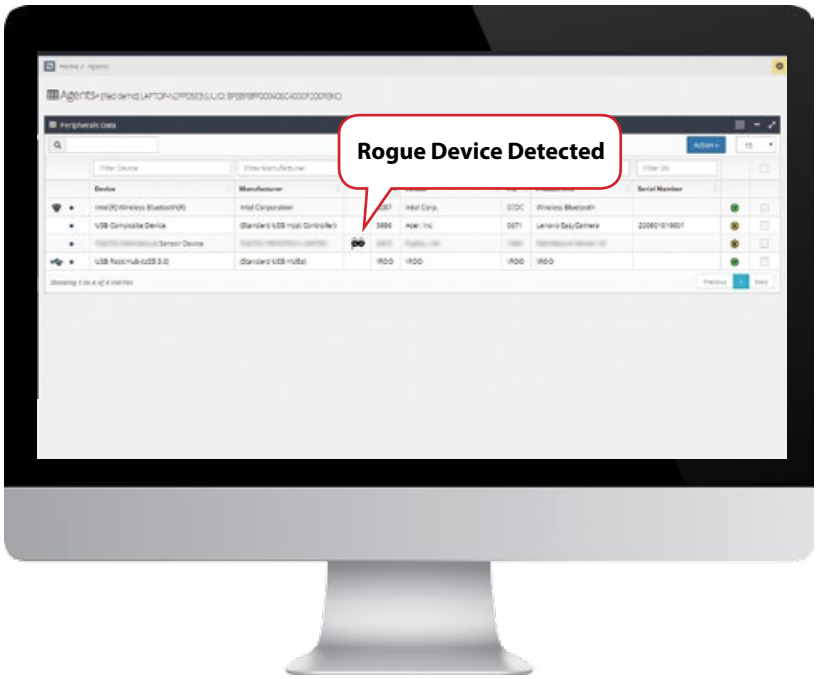
Palm-vein scanners are a more secure form of biometric authentication, looking at not only the individual's palm ridges, texture, spatial attributes and geometric characteristics, but also the pattern of their veins. The near-infrared scanning creates a black pattern of the veins that is captured by the scanner and then compared with a stored record for the individual in question.

However, palm-vein authorization can be bypassed with a man-in-the-middle (MiTM) attack and unauthorized access can be granted.

TOOLS USED

In this specific incident, a BeagleBone board running USBProxy was used that, when attached to the scanning device and the computer system that stores the records of genuine handprints, allowed the attacker to bypass the authentication.

The BeagleBone does not require any extra hardware in addition to its superior set of input/output features, making it easy to interface with exterior electronics.



HAC-1 SOLUTION

Many times, enterprises' IT and security teams struggle in providing complete and accurate visibility into their hardware assets, especially in today's extremely challenging IT/OT/IoT environment.

This is due to the fact that often, there is a lack of visibility, which leads to a weakened policy enforcement of hardware access. This may result in security accidents, such as ransomware attacks, data leakage, etc.

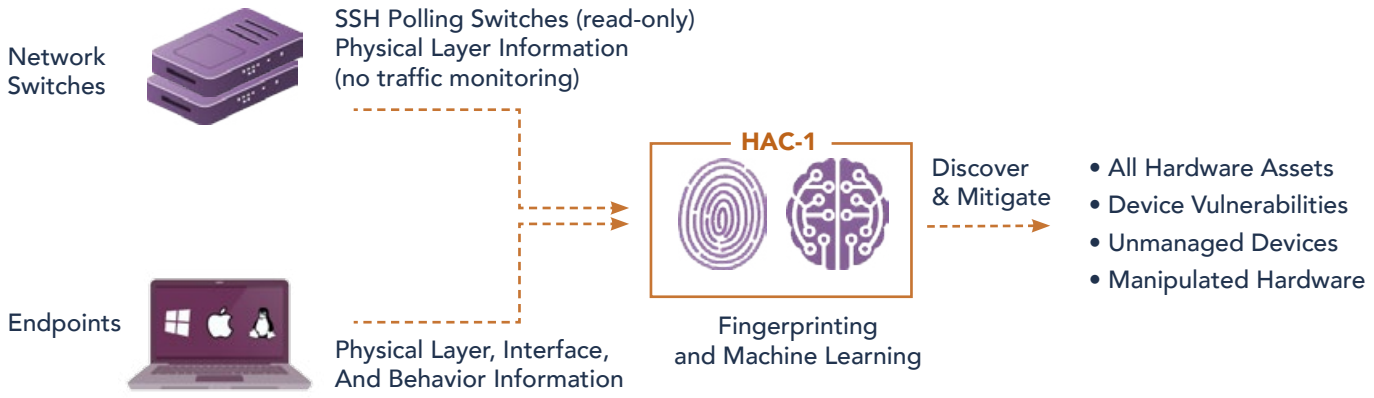
In order to address this challenge, ultimate visibility into your Hardware assets is required, regardless of their characteristics and the interface used for connection as attackers. Moreover, it is important to be practical and adjust to the dynamic Cyber security defenses put in place to block them, as well as take advantage of the "blind" spots – mainly through USB Human Interface Device (HID) emulating devices or Physical layer network implants.

In addition to the deep visibility layer, a comprehensive policy enforcement mechanism recommends on best practice policy and allows the administrator to define a strict, or more granular, set of rules for the system to enforce.

Sepio is the leader in the Rogue Device Mitigation (RDM) market and is disrupting the cybersecurity industry by uncovering hidden hardware attacks operating over network and USB interfaces. SepioPrime, which orchestrates Sepio's solution, identifies, detects and handles all peripherals; no device goes unmanaged.

The only company in the world to undertake Physical Layer fingerprinting, Sepio calculates a digital fingerprint using the device descriptors of all connected peripherals and compares them against a known set of malicious devices, automatically blocking any attacks. With Machine Learning, the software analyses device behavior to identify abnormalities, such as a mouse acting as a keyboard.

How It Works



HAC-1 - Visibility & Security of Hardware Assets

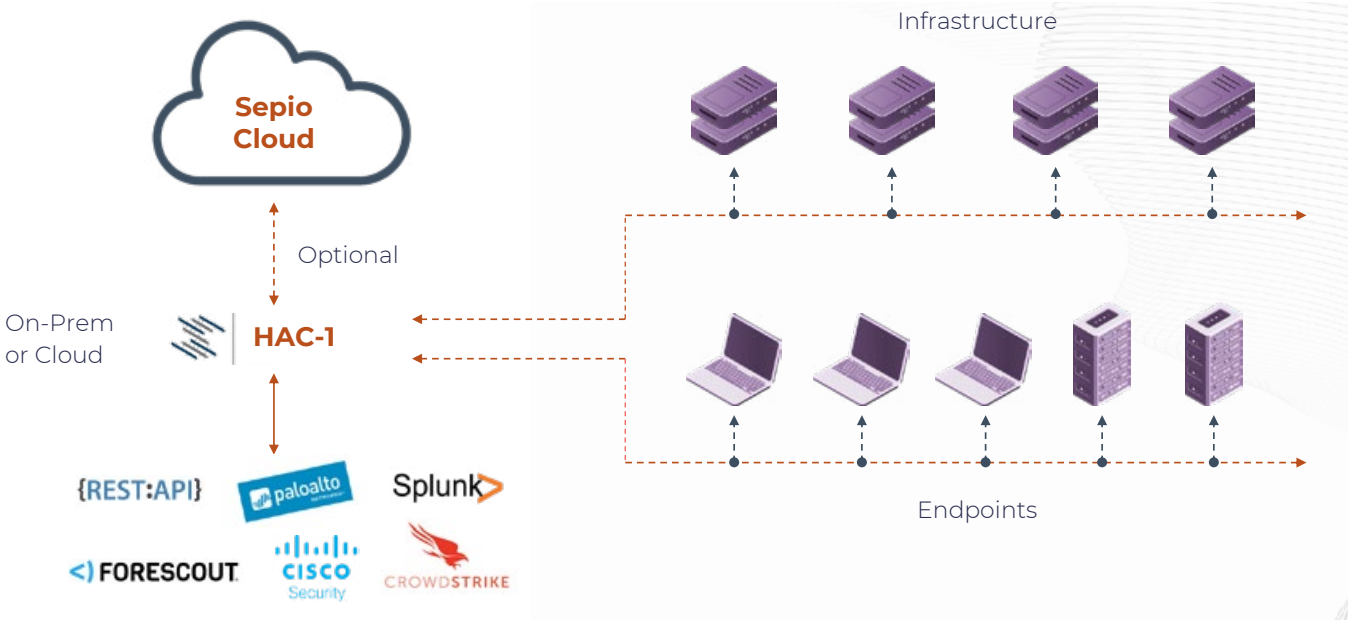
Main Benefits

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


access denied