SEPIO

SUPPLY CHAIN CHALLENGES

PROBLEMS AND SOLUTIONS

A Sepio white paper

INTRODUCTION

According to the GAO-18-667T, Reliance on a global supply chain introduces multiple risks to federal information systems. Supply chain threats are present during the various phases of an information system's development life cycle and could create an unacceptable risk to federal agencies.

Malicious actors could exploit supply chain vulnerabilities, leading to the loss of the confidentiality, integrity, or availability of federal systems and the information they contain.

When attacking the supply chain, it is typically the hardware (but not limited to) especially when some hardware components include built-in firmware) that is tampered with. Devices can be compromised at any point throughout the supply chain and the Rogue Device can be delivered by a supplier to the end user. Moreover, due to the interconnectedness of the involved organizations, suppliers often have access to a target's sensitive information. When the target is highly secured and gaining an onsite presence is almost impossible for an attacker, such as a government agency, it is more attainable to attack a third party with fewer security measures in place as confidential data can still likely be accessed.

As mentioned, supply chains are becoming increasingly complex which makes detecting an attack, and its origin, extremely difficult and in many aspects supply chain attacks represent the "Holly Grail" of hardware based attacks. Additionally, implants can be microscopic and can easily go unnoticed to the human eye, avoiding any suspicion as to the device's true intentions. Some attack tools are present only on the network's physical layer – Layer 1 – not detected by security software solutions that have network visibility from Layer 2 and above.

> **"There are intelligence organizations around the world every day thinking about how they can attack at the hardware level because of the opportunities."**
>
> **Robert Bigman,** Former CISO @CIA

ATTACKS

Manipulation

Attacks on the supply chain commonly involve hardware being intercepted and manipulated. This can include the manipulation of the printed circuit board (PCB) whereby bad actors inject malicious functionality after a reverse engineering process has identified areas in which new capabilities can be added.

Additionally, chips can be manipulated in order to carry out an attack and everyday peripherals can be spoofed to act with malicious intent, in this scenario, the original functionality of the chip will remain intact, while the "additional" functionality may be triggered by an external event (physical - by sending a specific RF signal or logical - via a certain access to a memory area that usually is nonexistent). Manipulation can happen at any point throughout the device's route along the supply chain. The device will be unpackaged, modified, repackaged and put pack in transit.

Side Channel Attack

These attacks aim to extract secrets from a chip or system through measurement and analysis of physical parameters. Side channel attacks have proven to be successful in breaking algorithmically robust cryptography operations, thus meaning that anything else protected by conventional cryptographic methods is no longer protected.

- **Sound-based attack.**

In this type of attack, the sound of the user's keystrokes is recorded to steal passphrases. By listening to the sound of the keys being pressed, the attacker attempts to determine the text that is being produced.

- **Timing attack.**

Here, perpetrators will attempt to compromise a cryptosystem by analyzing the time taken to execute cryptographic algorithms. Since every logical operation in a computer takes time to execute, the time can differ depending on the input.

- **Electromagnetic field (EMF) radiation**

This attack allows the electromagnetic radiation that is emitted from a device to be measured. From here, a signal analysis can be performed since different operations produce different amounts of radiation.

- **Thermal-imaging attack**

The infrared images that come from observing the surface of a Central Processing Unit (CPU) can provide information about the code being executed on that CPU.

- **Power-analysis attack**

The attacker can study the power consumption of a cryptographic hardware device, allowing them to "see inside" otherwise tamperproof hardware. This non-invasive attack provides the ability to extract cryptographic keys and other secret information from the device.

- **Acoustic cryptanalysis attack**

Power consumption of devices cause heating, which is offset by cooling effects. These temperature changes create thermally induced mechanical stress which can create low-level acoustic emissions from operating CPUs.

ATTACK METHODS

Fault Attack

These attacks target a physical electronic device whereby the attacker essentially causes stress to the device through an external mean e.g. incorrect voltage, excessive temperature or signal power interference. The stress generates errors in such a way that it results in a security failure of the system.

Power Line Attack

Through malware, perpetrators can control the workload of the device's CPU, thus having the ability to also control its power consumption. The emissions conducted on the power cables are measured and the signal is processed and decoded back into binary information by the attacker.

Wireless Implants

Through the HID, computer operating systems have allowed for devices to be accepted when they are plugged in to make keyboard, mice and other input devices as easy to connect as possible. By exploiting this weakness, attackers have utilized devices that act like HIDs to carry out attacks since they will be recognized as genuine by the computer.

These Rogue Devices look authentic to the human eye – such as a charging cable or a keyboard – and are used by victims without questioning their intent. The device incorporates a remote access point that allows the attacker to control the endpoint without ever needing to gaining physical access to it, thus making the job easier.

Spy Chips

These are malicious chips which can access the configurations of the target's firewall. From here, the firewall settings can be changed to provide the attacker with remote access to the target device, disable its security features and provide access to the device's log of all the connections it is exposed to.

Spy chips are tiny in size – just bigger than a grain of rice – and can go easily unnoticed on a motherboard.

MITIGATION

Automated Optical Inspection

An Automated Optical Inspection (AOI) test, originally used in the assembly lines, enables fast and accurate inspections of populated PCBs to ensure that the item is built correctly and without any manufacturing modifications. This is done by verifying that the device is assembled according to a comparison of a golden image. An AOI solution can detect soldering changes of certain components and inconsistency in the assembled components. The main shortcoming of this solution is the fact that you need to have direct visual of the PCB, which requires significant effort when the devices are already deployed.

JTAG Boundary Scan

This is a method for testing interconnects on PCBs or sub-blocks inside an integrated circuit. Thus, JTAG is an essential tool for testing boards in development, production and in the field meaning it can be used to test at any time through the supply chain. Overall, JTAG provides information about the state of a board with minimal access. Direct internal access to the PCB is required, making post-deployment tests challenging.

Radio Frequency Power Detector

One should keep in mind, that as the attackers are aware of various RF geo-location sensor characteristics, they will use more "exotic" RF bands, and "bury" the signals using spread spectrum direct sequence or other concealment options.

Power Line anomaly detection

As ex-filtration of data and C2 connection can be implemented by using Power-Line communication (where data is transmitted over standard power cabling) Analyzing the physical layer characteristic of these power cables can provide detection of digital data "piggy-backing" over this physical channel.

X-ray

X-ray scan can be helpful for those cases where you do not want to open the unit (for various possible reasons, including voiding warranty). X-ray can detect the existence of additional/modified modules inside the supplied unit (while comparing it to a golden image or a vast database of similar devices). Nevertheless, technology for detecting when a certain unit has been X-rayed exists , which might allow the attacker to terminate its activity once suspicion has risen.

Physical Layer Fingerprinting

Through in-depth analysis of the device's physical layer characteristics - voltages, currents, eye-pattern of signals, PoE parameters etc. One can create a unique physical fingerprint for each device, later making this information usable for anomaly detection - through AI or ML based algorithms. Such detection algorithm is implemented in Sepio HAC-1 solution.

HAC-1 Solution

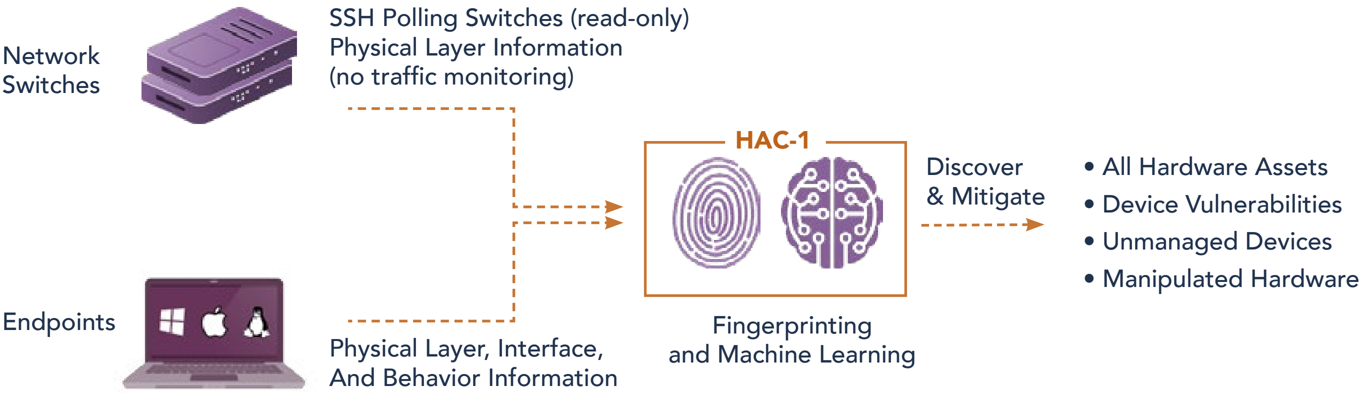
Many times, IT and security teams in the energy sector struggle in providing complete and accurate protection of their hardware assets - especially in today's extremely challenging IT/OT/IoT environment. This is because, often, there is a lack of device visibility which leads to weakened policy enforcement of hardware access. This vulnerability may result in security incidents such as ransomware attacks, data leakage, etc. In order to address this challenge, ultimate visibility into your Hardware assets is required, regardless of device characteristics and the interface used for connection.

Moreover, malicious actors have adapted to the dynamic cybersecurity defenses deployed to block cyber-attacks by taking advantage of the "blind spots" – mainly through USB HID-emulating devices or Physical Layer network implants. These Rogue Devices are covert by nature and go undetected by existing security software solutions, thereby leaving the organization extremely vulnerable.

Sepio has developed the Hardware Access Control (HAC-1) solution to provide 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 fingerprints. In doing so, HAC-1 is able to provide organizations with ultimate device visibility and detect vulnerable devices and switches within the infrastructure.

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. When a device breaches the pre-set policy, HAC-1 automatically instigates a mitigation process which instantly blocks unapproved or Rogue hardware.

How It Works



HAC-1 - Visibility & Security of Hardware Assets

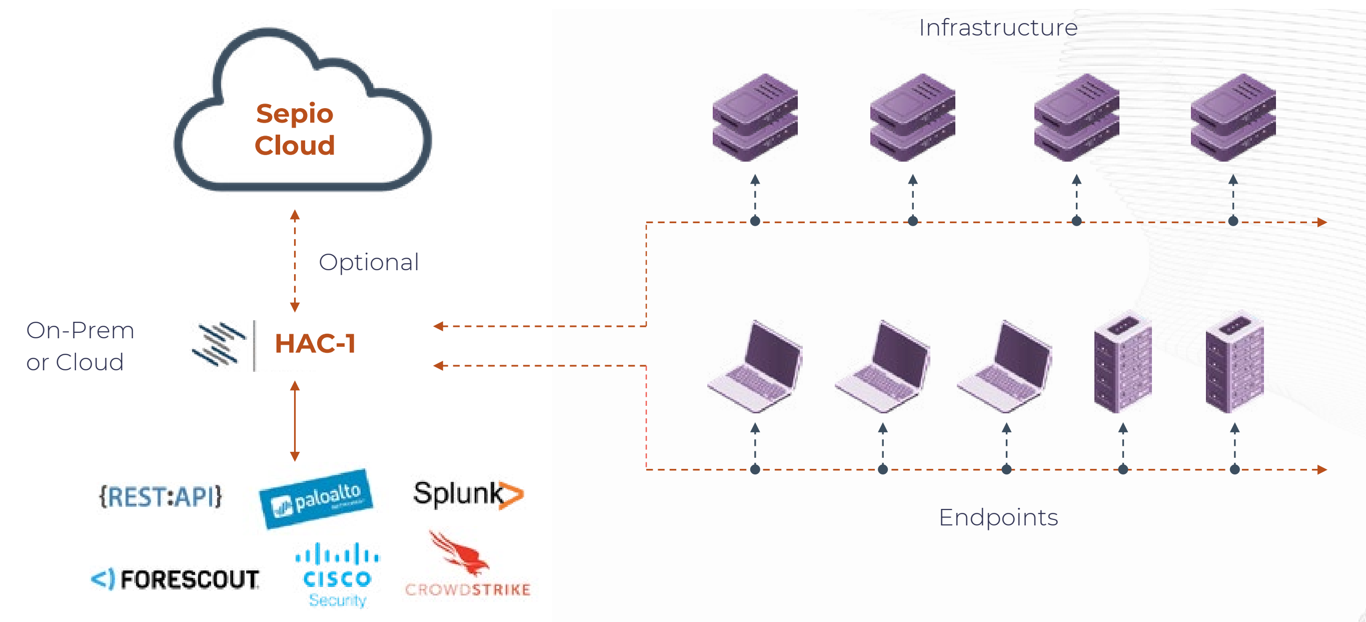
Main Benefits:

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