PFP CYBERSECURITY

Integrity & Reliability from Chips, Boards to Systems for Hardware, Firmware & Configuration

THE PROBLEMS

1. DEPENDENCY ON CHINESE MANUFACTURING

A DoD study indicates ~22% of tier 2 and ~72% of tier 3 suppliers of 39 product lines reliant on Chinese Manufacturing

Figure 1: COTS electronics fabricated overseas is a big risk

2. COTS ELECTRONICS PRESENTS MAJOR THREATS

Most COTS electronics used in DoD systems are fabricated overseas and could be tampered (Figure 1).

3. TAMPERED COMPONENTS FROM SUPPLY CHAIN IS ONE OF THE TOP VULNERABILITIES FOR US WEAPON SYSTEMS

Such vulnerabilities can be activated at a later point in time without direct access by the attacker (the GAO report (GAO-19-128) "WEAPON SYSTEMS CYBERSECURITY"), see Figure 2.

Figure 2: Numerous vulnerabilities include tampered internal component

4. SUPPLY CHAIN FIRMWARE ATTACKS CAN BYPASS CURRENT FIRMWARE INTEGRITY MONITORING

"The active exploitation of some of the discovered vulnerabilities can't be detected by firmware integrity monitoring systems due to limitations of the Trusted Platform Module (TPM) measurement. The remote device health attestation solutions will not detect the affected systems

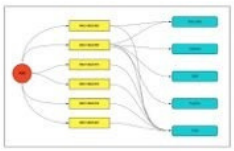

Figure 3: Software supply chain attacks impacted all server brands

REQUIREMENTS

GSA Subpart 504.70 - Cyber-Supply Chain Risk Management, Effective 2022-4-1, directs agencies to implement supply chain risk management principles to protect against the insertion of counterfeits, tampering, malware, poor manufacturing, etc.

Meeting GSA 504.7002 and DFARS 252-2 Requirements

FAR	PFP SigLytics™
The insertion of counterfeits	Detects counterfeits and devices with counterfeits, legit devices with lower grade configurations, etc.
Unauthorized production	Authenticate using signatures and PKI to verify physical and logical configuration (BOM and SBOM) with private keys
Tampering	Detects tampering in hardware and firmware, Level 0 and 1 endpoints, Trojans in silicon, etc.
Theft	Authenticate using signatures and PKI to verify physical and logical configuration (BOM and SBOM) with private keys
Insertion of malicious software	Detects change of execution from malware
Poor manufacturing & development practices throughout the system development life cycle	Detects counterfeits and devices with counterfeits, legit devices with lower grade configurations, etc.

PFP Meets the Following DFARS 252-2 Requirements

DFARS

"Counterfeit electronic part" means an unlawful or unauthorized reproduction, substitution, or alteration that has been knowingly mismarked, misidentified, or otherwise misrepresented to be an authentic, unmodified electronic part from the original manufacturer, or a source with the express written authority of the original manufacturer or current design activity, including an authorized aftermarket manufacturer.

"Counterfeit electronic part" Unlawful or unauthorized substitution includes used electronic parts represented as new, or the false identification of grade, serial number, lot number, date code, or performance characteristics.

"Electronic part" means an integrated circuit, a discrete electronic component (including, but not limited to, a transistor, capacitor, resistor, or diode), or a circuit assembly (section 818(f)(2) of Pub. L. 112-81).

"Malicious software" means computer software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. This definition includes a virus, worm, Trojan horse, or other code-based entity that infects a host, as well as spyware and some forms of adware.

1577 Spring Hill Road # 405 Vienna, VA 22182 www.pfpcyber.com 540 - 200 - 8344

PFP CYBERSECURITY

The Gaps

1. No tools for operators to assess integrity of equipment to gain confidence

2. No tools to assess integrity to eliminate counterfeits and tampered microelectronics and electronics from supply chain

The Needs

Users prefer a solution which meets the following characteristics:

1. Can be applied to many parts and many different classes of parts

2. Can be operated by users and operators without deep technical knowledge

3. Open systems with flexibility of technology without proprietary equipment

4. Highly scalable and portable

5. Can give results anywhere, anytime

The Value

1. Detects unseen attacks from supply chain and during operation

2. Enable cyber resilience with machine detection and recover back to known good state

Out-of-Band Monitoring

PFP enables out-of-band screening and verification of electronics from chips to systems, at scale. All electronic devices generate un-intended emanations which are unique to each device due to variations in manufacturing processes, and specific firmware configuration. PFP uses Machine Learning to create a baseline and detect changes.

Trusted Supply Chain and Continuous Monitoring from Chips to Systems

The PFP SigLytics has been proven for chip authentication (analog, digital, memory, FPGA, etc.), printed circuit assemblies, legacy devices, computer servers, IoT, etc. Figure 5 shows a process for supply chain security and continuous monitoring during operation from chips, computer servers, storage, power supply, vehicle electronics, to systems. This process can also be applied to level zero devices such as sensors, cables, leakages and analog signals, etc. For security, reliability, quality and safety, users could compare new devices and devices in operation against corresponding baseline for incoming inspection, manufacturing, spot check, and continuous monitoring in operation.

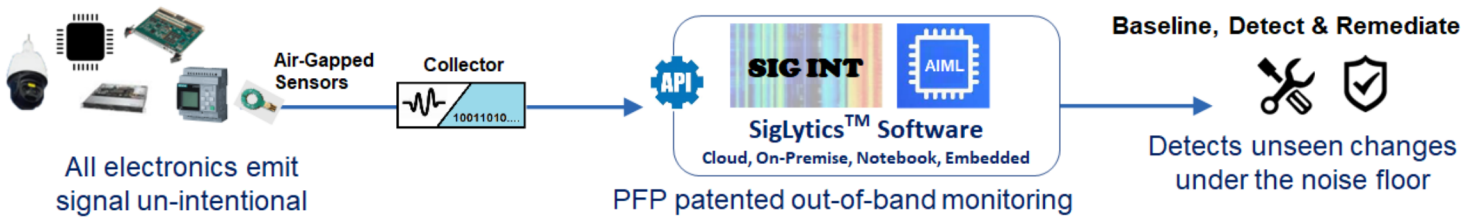

Figure 4: Principle of the PFP integrity assessment platform

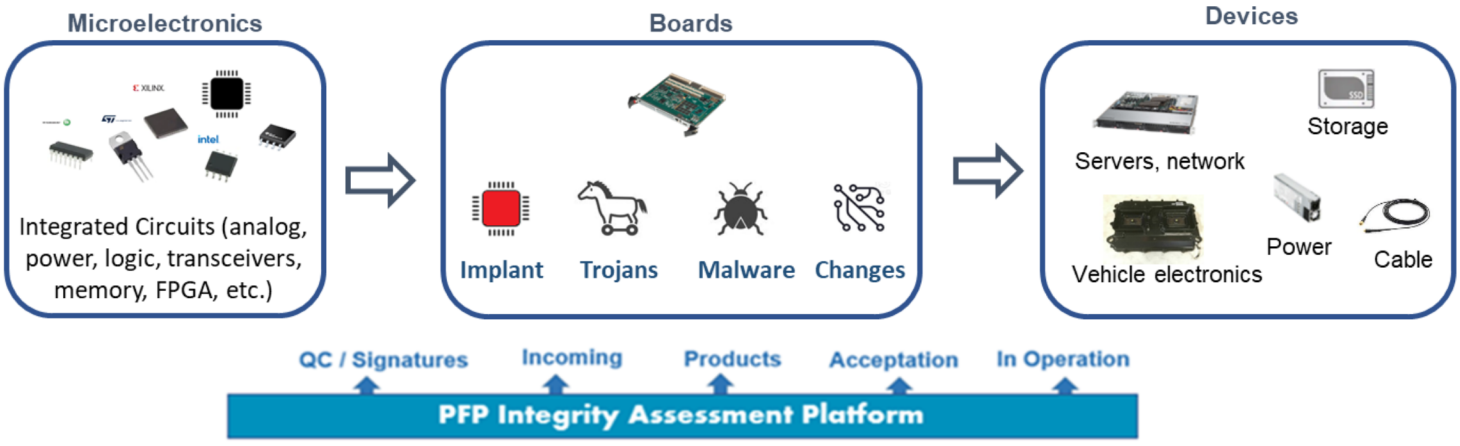

Figure 5: From chips, boards to devices and systems

Contact Information | Steven Chen | SChen@PFPCyber.com