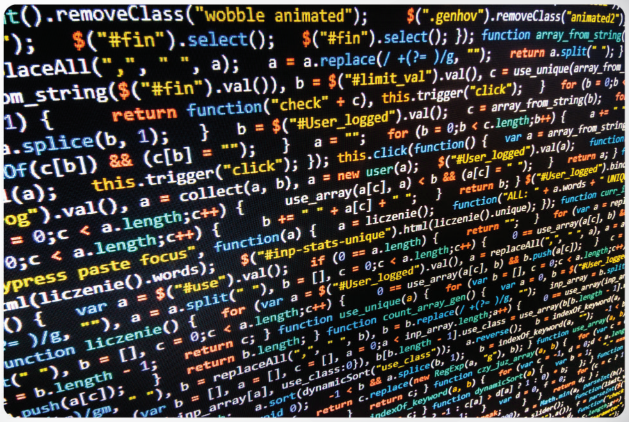
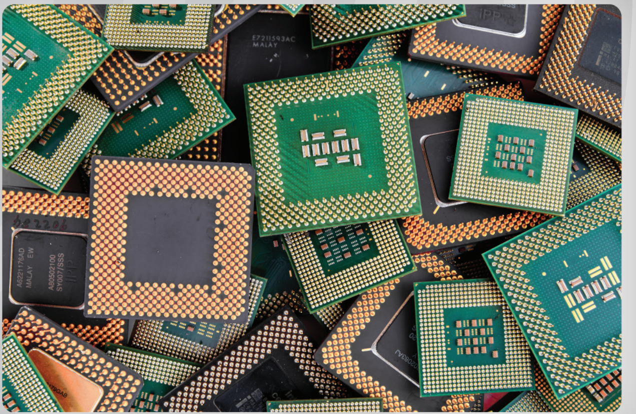
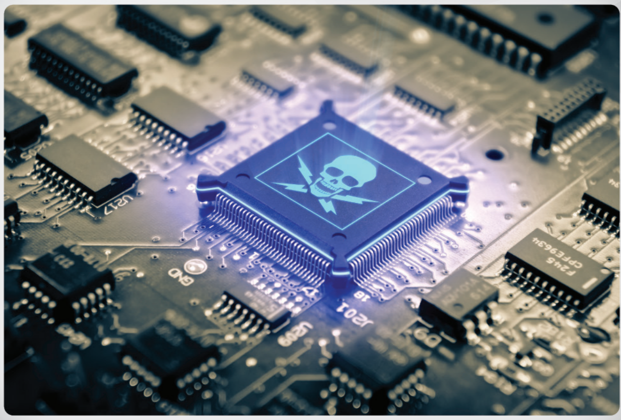
Supply Chain Protection

A White Paper on Counterfeit Detection







PFP

CYBERSECURITY

Supply Chain Protection

Summary

Power fingerprinting (PFP) is an integrity assessment technology based on observing unique fine-grained patterns in physical side channels from electronic devices. Side channel information, such as power consumption, is a unique function of circuit logic and layout, semi-conductor technology, manufacturing process and execution code. Supply chain compromise to include counterfeit products/components, hardware Trojan like deployments, and even subpar quality control are all detectable through these proprietary analytics developed by PFP.

Introduction

The complex, distributed, and multinational nature of electronics manufacturing increases the risk of exploitation of supply chain vulnerabilities. Throughout the supply chain, critical hardware and software products are exposed to potential tampering, including hardware Trojans and counterfeit components.

Hardware Trojans are malicious modifications of an integrated circuit, and detecting them is a very challenging task. Intrusion can happen at any stage in the semiconductor process: design, fabrication, or manufacturing. Further, the tamper often represents a small percentage of the system and usually goes to great lengths to remain undetectable by activating only under specific conditions. Approaches for detecting hardware Trojans have been developed, but have limitations. Threat detection techniques based on running industry-standard functional tests are fairly limited and can only address functionality described in the design specifications. These solutions are very limited in detecting stealthy Trojans, which are only triggered by hidden, rare or very-specific conditions. Formal verification and other static analysis at the design stage is not able to catch tampering at manufacturing. Real world examples include a supposed Israeli-placed hardware-backdoor in a microprocessor that allowed them to shut down a Syrian radar facility before an attack on a suspected nuclear facility. [1]

Counterfeit electronics have become a major challenge in a complex supply chain. see [2 - 12] Figure 1 shows the increase in counterfeiting that has quadrupled since 2009. Counterfeit parts (recycled, remarked, cloned, or out-of-spec/defective) can result in reduced lifetime and pose reliability risks to mission critical systems. Furthermore, the tools and technologies used by well-financed counterfeiters have become extremely sophisticated making the resulting parts very difficult to detect. Current methods for counterfeit detection include: Physical inspections (e.g. x-ray imaging, scanning electron microscopy, microblast analysis, and material analysis) and electrical/timing

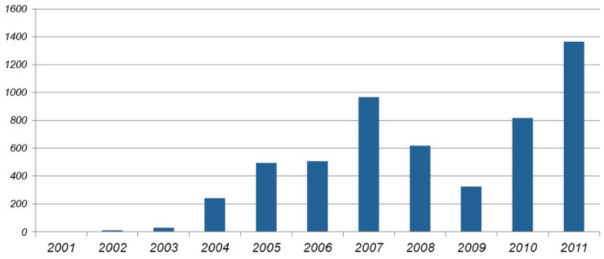


FIG 1. Counterfeit parts have quadrupled since 2009 [13]

inspections (e.g. parametric and functional tests, structural tests, and path-delay analysis). Physical inspections have several drawbacks, for example, many of them are destructive, can require excessive test time and cost (e.g. several hours to test a single component), are difficult to automate, and depend on the interpretation of a subject-matter expert.

There is a fundamental need for a technology that can inspect a specific electronic device or component and determine when it has been tampered or is a counterfeit. A key element in solving supply chain security challenges is an effective firmware method that delivers quantitative classification metrics to distinguish tampered from untampered components.

As recently as 2015 the real cost of counterfeit components have been highlighted in industry periodicals such as Electronic Components News®. Figure 2 highlights typical statistics of counterfeit component deployments. Approximately 32% of counterfeits were not discovered until already in production, possibly costing manufacturers billions of dollars in rework.[14]

Current state of the art threat detection methods include electrical tests using customized testing fixtures/harnesses as shown in Figure 3 (e.g., the ABI Sentry®). These testers measure different DC and AC parameters at the pins, such as IV curve tracing and impedance, and determine legitimacy by comparing the observed values against those of a reference device. While these basic electric tests are able to detect counterfeits with the wrong die and electrically failing parts, they only exercise a small part of the circuit, and thus, can easily miss many types of counterfeits, including relabeled and recycled parts.

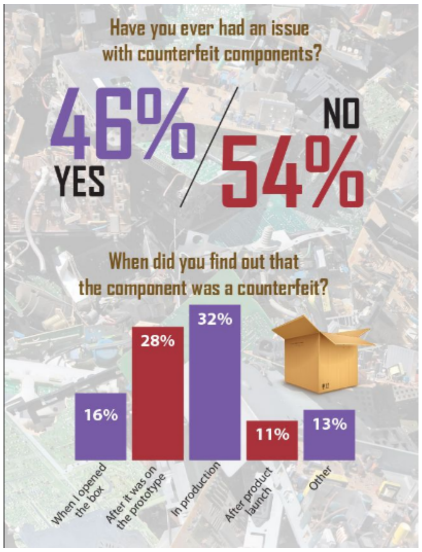


FIG 2. When are counterfeits detected? [14]

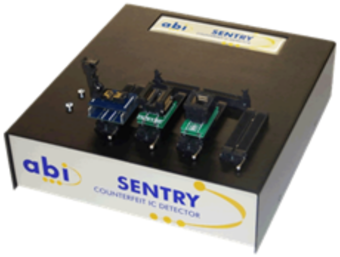


FIG 3. An electrical reference counterfeit detector

PFP Technology

Power fingerprinting (PFP) is a novel approach that utilizes physical side channels to assess the integrity of an electronic device. Side channels are those physical measurements that can be made from outside the specific component, but which contain information about the execution status of the target. For instance, features such as power consumption or electromagnetic emissions are side channels intrinsic to device operation. Side channels, such as power consumption and electromagnetic emissions, depend on the circuit layout, semiconductor technology, and manufacturing process, which make them unique for a given hardware.

PFP is effective across the full execution stack, from hardware to firmware to software and is independent of platform and application. PFP is capable of detecting, with extreme accuracy, when unauthorized modifications, such as hardware Trojans or counterfeit parts, have compromised the integrity of an electronic system. PFP provides dynamic verification of hardware systems and a non-destructive process for tamper and intrusion detection at the supply-chain.

PFP performs fine-grained anomaly detection on the device's side channels to determine whether it has deviated from expected operation (Figure 4). A PFP monitoring setup uses a physical sensor to capture the fine-grained side-channel signals, which contain tiny patterns that emerge during operation that are unique to the hardware and software executing within the device. PFP test equipment can be built using Commercial Off-The-Shelf (COTS) components. Also, PFP can be performed much faster compared to other inspection approaches, since PFP can observe and perform its analysis in parallel with routine functional testing. PFP has been shown effective in a variety of chips, devices and platforms to assess the execution integrity of hardware and firmware.

PFP in Supply Chain Assurance

PFP is intended to be used as part of an acceptance or laboratory test to validate component and subsystem integrity. For large component volumes, the manufacturer would integrate PFP sensors into the Automatic Test Equipment (ATE) setup used to validate functional correctness, as shown in Figures 5a &b. While the ATE is performing functional tests, the PFP monitor captures side channel signals and transfers them to the PFP analysis engine. Assessment results are then provided in the PFP Dashboard and logged for subsequent reporting and traceability.

Baseline Extraction

PFP's tamper detection performance is determined by the availability and quality of reference baselines. The most straightforward way to produce the necessary baselines is by collecting them directly from a gold (trusted) sample. When a gold sample is available, side channel signals are measured directly from the components using PFP tools and stored in a library for later use (see Figure 5b).

In many cases, however, a gold sample is not available. In these cases, there are still methods to produce PFP baselines. For instance, statistical analysis can be performed on a set of incoming parts to detect outliers. Such approach can be effective when only a subset of the parts are tampered or counterfeits. An example of this situation is "salting", where the genuine parts are mixed with counterfeits.

Another approach to extract baselines from critical parts without a trusted gold sample is to perform regular PFP characterization on a small subset of the parts. The subset is then reversed engineered using destructive techniques. If reverse engineering shows no tampering, the PFP references can be trusted and used to validate the remainder of the parts as well as all future procurements.

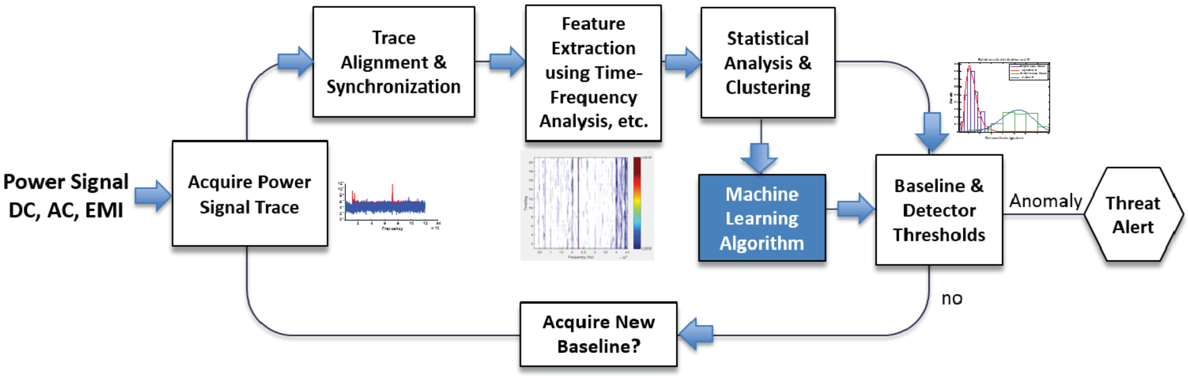

Power Signal
DC, AC, EMI
Acquire Power Signal Trace
Trace Alignment & Synchronization
Feature Extraction using Time-Frequency Analysis, etc.
Statistical Analysis & Clustering
Machine Learning Algorithm
Baseline & Detector Thresholds
Anomaly
Threat Alert
no
Acquire New Baseline?

FIG 4. Trojan Detection using PFP

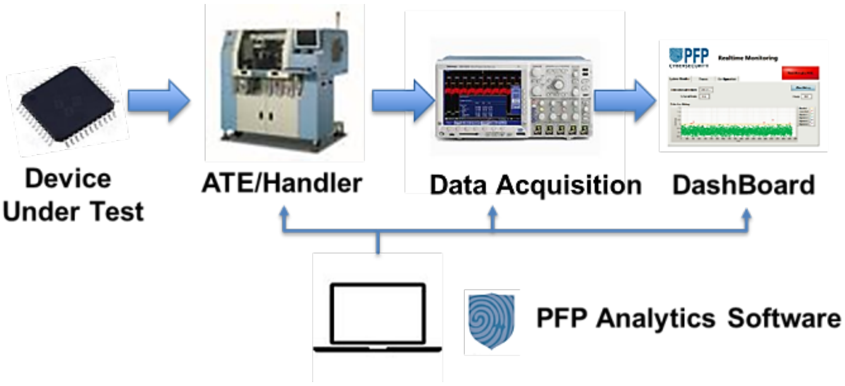


FIG 5a. PFP Test Hardware and Flow for Supply Chain Assurance

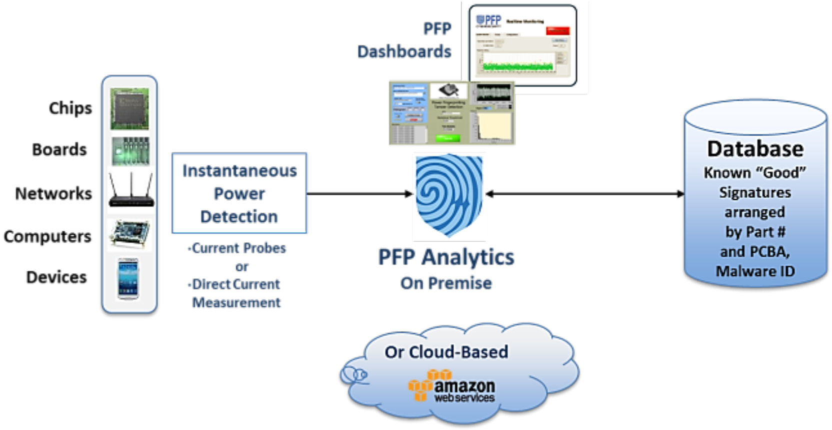
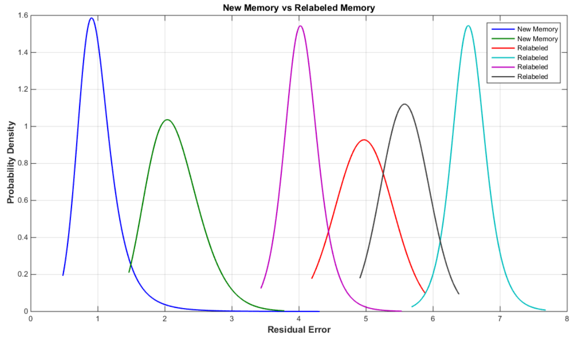


FIG 5b. Key PFP Software Components of Counterfeit Detection System

Case 1: Intel Memory Chips

In one of the selected cases, PFP with the University of Connecticut's Center for Hardware Assurance, Security, and Engineering (CHASE) examined 9 different samples of Intel's TB28F400B5-T80 Flash memory (Figure 6). In the sample set, there were original, relabeled, and recycled parts. PFP correctly identified 100% of the counterfeit parts. The results showing the original and relabeled parts are shown in the table of Figure 6.



Memory, Intel TB28F400B5-T80	
IC Nomenclature	Condition
U0390519C, 9297	New
U0390519C, 9297	New
U9301038Y, 9297	Relabeled
U9110964A, 9297	Relabeled
U9140702Y, 9297	Relabeled
U41617P4C, 1992	Relabeled
U0180416Y, 9297	Relabeled

FIG 6. PFP Test Data from Intel Memory Chip Evaluation

Case 2: FPGA Aging

PFP has conducted analysis on a group of Xilinx FPGAs with targeted accelerated aging and samples from different batches. PFP clearly separated the samples into categories of new versus used as well as from different batches, as shown in Figure 7.

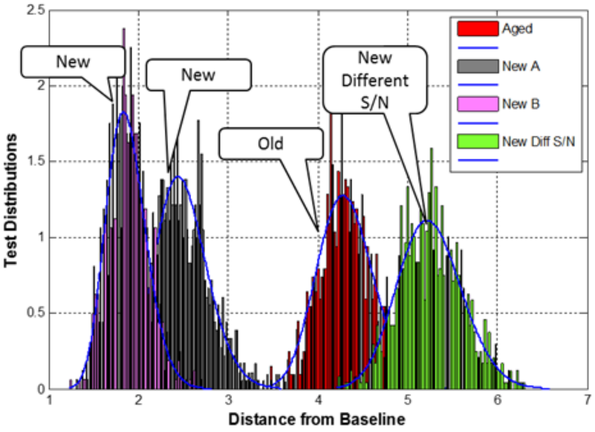


FIG 7. FPGA Aging Test

Case 3: FPGA Tampering

PFP conducted various FPGA tampering tests by inserting a 4-bit counter in a Xilinx FPGA. As shown in Figure 8, PFP detected the tamper insertion in machine time both in the dormant and the active modes of the tamper code.

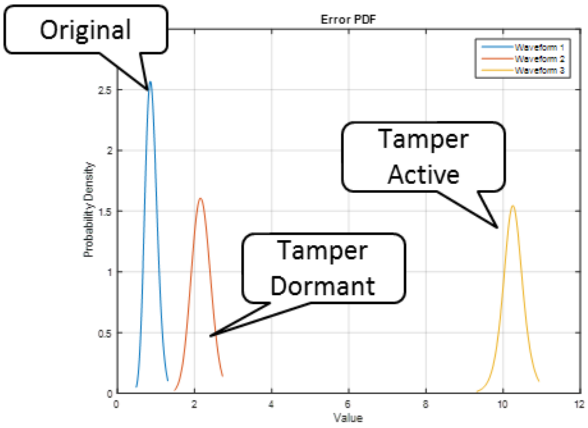
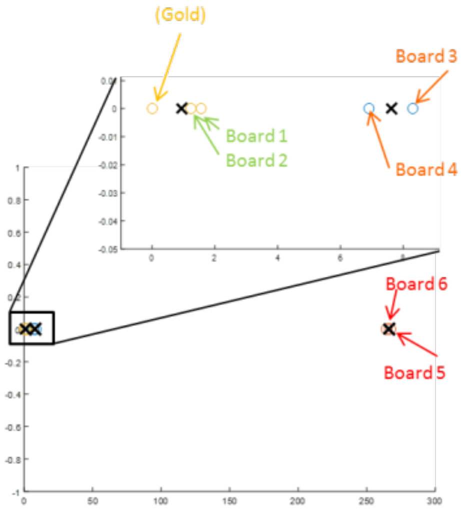


FIG 8. FPGA Tamper Test

Case 4: PCBA with Tampered Firmware

PFP performed an analysis of seven boards provided by an electronics manufacturer to detect changes in firmware in a blind test. Without any prior knowledge of the design specifications or even of the purpose of these boards the PFP analytics were able to correctly classify the boards (running modified PLD firmware). Figure 9 highlights the results of the test with identification of the counterfeit/ modified boards. The center graph depicts the different clusters relative to the Gold sample. The most distant cluster corresponds to blank boards that had not been programmed. These are easy to spot. The PFP analysis, however, was able to identify two additional clusters that were much closer together but still separate enough to determine with high confidence that they came from different systems. The results, shown in the zoomed detail in Figure 9, show the difference between the boards that match the Gold sample and those with a different firmware version. Even though the two firmware versions are functionally very similar, there was enough confidence in the assessment to classify it as a different version, as shown in the table in Figure 9.



Board Number	Result	Confidence
Gold	Gold sample	
1	Match	
2	Match	
3	Not a match	0.9869 %
4	Not a match	0.9836 %
5	Not a match	0.9997 %
6	Not a match	0.9997%

FIG 9. PFP Blind Test of Proprietary Circuit Board

Conclusion

PFP is a proven technology capable of detecting tampering at all levels of the execution stack, from hardware to firmware to software.

PFP can help minimize supply chain risk by providing an agile and effective approach to detect hardware Trojans and counterfeits in electronic parts in real-time and in parallel with standard operational product testing.

PFP performs anomaly detection using physical side channel signals, such as power consumption during execution, which contain tiny patterns unique to the specific hardware and firmware.

PFP has been successfully demonstrated on simple and complex components at the chip level, board level and device level.

PFP can play a key role in ensuring that the integrity and reliability of critical systems is not compromised throughout the entire supply chain life cycle.

References

[1] http://spectrum.ieee.org/semiconductors/design/the-hunt-for-the-kill-switch/0

[2] "Inquiry Into Counterfeit Electronic Parts in the Department of Defense Supply Chain," Committee on Armed Services, United States Senate, May 21, 2012.

[3] ''Winning the Battle Against Counterfeit Semiconductor Products," A report of the SIA Anti-Counterfeiting Task Force, Semiconductor Industry Association, August 2013

[4] http://www.businessinsider.com/counterfeit-parts-from-china-raise-grave-concerns-for-both-us-companies-and-national-security-2012-6

[5] http://defensetech.org/2012/05/30/smoking-gun-proof-that-military-chips-from-china-are-infected/

[6] http://www.businessinsider.com/navy-chinese-microchips-weapons-could-have-been-shut-off-2011-6

[7] http://americanerecycling.org/images/Counterfeiting_position_paper_6_11_14_FINAL.pdf

[8] http://resource-recycling.com/node/4691

[9] http://www.smithsonianmag.com/smart-news/eight-million-tons-illegal-e-waste-smuggled-china-each-year-180949930/?utm_source=twitter.com&no-ist

[10] http://aviationweek.com/awin/chinese-microchips-are-considered-impossible-regulate

[11] http://www.forbes.com/sites/ciocentral/2012/07/11/the-serious-risks-from-counterfeit-electronic-parts/

[12] https://thecounterfeitreport.com/ product/562/FTDI--Chip-FT232RL-Chips.html (for example)

[13]IHS, ‘‘Reports of counterfeit parts quadruple since 2009, challenging U.S. Defence Industry and National Security,’’ Apr. 2012. [Online]. Available: http://www.ihs.com/ images/IHS-iSuppli-Reports-Counterfeit- Parts-Quadruple-Since-2009.pdf.

[14] ‘‘Do engineers use counterfeit components?’’ Jan. 2015 [Online]. Available at http:// www.ecnmag.com/blogs/2015/01/do-engineers-use-counterfeit-components

For more information visit: www.pfpcyber.com
Email: info@pfpcyber.com
PFP Cybersecurity is also known as Power Fingerprinting, Inc.