PFP CYBERSECURITY

Embedding Security in the Internet of Things

A PFP Cybersecurity Whitepaper

Embedding Security in the Internet of Things

A White Paper from PFP Cybersecurity

Summary

Threats embedded in hardware and firmware complicate the already challenging task of quickly detecting and remediating threats. The emerging Internet of Things, with billions of new devices that have embedded network connectivity, is increasing both the urgency and the challenge of securing our information infrastructure. Embedded threats require embedded security. PFP Cybersecurity addresses threats to the Internet of Things with analog monitoring of power signals and in-device remediation. Power fingerprinting detects electrical patterns in chips and uses proprietary analytics to detect compromises in hardware and firmware.

Introduction

The task of protecting our information infrastructure has never been more difficult, and its security has never been more important to our national security and economy. As IT systems become more complex and more devices are being networked, more of our global economy is moving online. The distinction between the virtual and physical worlds also is becoming less clear. At the same time, attacks against these systems are becoming more sophisticated. Highly motivated and well-resourced adversaries are developing complex threats that avoid detection and remain persistent in compromised systems.

The result is a growing window of opportunity for hackers, criminals and nation states to exploit breaches in critical information systems.

The emergence of the Internet of Things (IoT), with billions of unmonitored devices that have embedded network connectivity, is bringing a quantum leap in the complexity of our IT systems and in the challenge of defending them. Compounding this problem are threats embedded in hardware and firmware. Currently undetectable by traditional security tools, these threats are expected to become more prevalent in this era of machine-to-machine networking.

Consider the existing state of cybersecurity.

- Detecting breaches takes too long: Definitive numbers are difficult to come by, but several studies show that breaches and other compromises routinely go undiscovered for extended periods. According to the Trustwave Global Security Report, [1] more than 80 percent of breaches were discovered by someone outside the victim organization, and the median time for discovery was 126 days. A survey for Arbor Networks by the Ponemon Institute [2] found that it took financial services companies 98 days on average to detect advanced threats, and retail companies took 197 days. And, of course, Mandiant's yearly cyber threat assessment puts the overall detection gap at 205 days on average and highlights that the longest undetected presence was 2,982 days[3].
- Unknown unknowns: According to a 2013-2014 evaluation of antivirus tools by Lastline Labs, [4] on any given day as many as half of the products being

tested failed to identify newly discovered malware.

- Noise to signal: Although threat intelligence can be valuable in discovering and removing advanced threats through traditional means, analysts first must sift through huge volumes of data from network and system sensors to identify the needle they are looking for.

Hackers realize that burrowing deep into the hardware and firmware where traditional security tools cannot see affords long term invisibility.

IoT and the "problem from hell"

Former NSA director USAF Gen. Michael Hayden (retd.) famously called hardware hacking the "problem from hell" during a 2011 cybersecurity discussion at the Aspen Institute. A backdoor placed on a chip or other device, or in its firmware, is practically undetectable by today's tools that look for malicious code.

The opportunity for hardware tampering grows with the expansion of our global economy and the lengthening of international supply chains. Components from around the world are integrated into products and systems, and it can be difficult if not impossible to ensure that third-party components have not been compromised. Tales have emerged of backdoors inserted in the manufacturing process of chips for use by the U.S. military. It is difficult to accurately attribute the source or even the purpose of backdoors in complex devices such as FPGA chips, but they present serious vulnerabilities. Threats include the risk of data being extracted for cloning products, which can lead to introduction of counterfeit components in critical systems. Back doors also can compromise devices, resulting in damage to equipment, the theft of sensitive data or intellectual property, or tampering with devices and information.

The growth of the Internet of Things provides fertile new fields for hardware hacking as new devices with embedded functionality from manufacturers around the world are integrated into our networks.

The IoT is not new. It is a continuation of the Internet's constant expansion in size and functionality. But the expected addition of billions of new devices with embedded connectivity in the coming years, often communicating directly with each other without human supervision, will present a new scale in security challenges. The potential for intentional tampering as well as for flaws in both off-the-shelf commodity products and purpose-built hardware raise the specter of wholesale threats.

Devices incorporated in the IoT range from single chips to complex sensors and distributed systems such as control platforms for modern smart automobiles. The sheer number of these devices is staggering. Cisco Chief Futurist Dave Evans [5] said the IoT was born between 2008 and 2009 when the number of Internet-connected devices exceeded the number of humans on the planet. He predicted the number of connected devices would double every five years to 25 billion by 2015 and to 50 billion by 2020. These devices will be scattered throughout the world and unlike the servers, PCs and laptops that have made up the Internet to date, many will operate without direct human supervision. Each of these devices

represents a potential vector for attacks, from the application layer to the hardware.

Unlike computers and servers, many of the nontraditional devices in the IoT are not owned and operated by IT departments and fall outside traditional security programs for patching, updating, monitoring and remediation. They also fall outside the IT refresh cycle, which typically is from three to five years for conventional IT equipment. Because they often operate remotely, IoT devices are designed for long lifetimes and can remain in place for decades. Undetected threats are not eliminated through regular replacement.

The IoT is not new. ... But the expected addition of billions of new devices with embedded connectivity in the coming years, often communicating directly with each other without human supervision, will present a new scale in security challenges.

How can the IoT be So Big

These risks are simultaneously created and compounded by the adoption of a new generation of Internet Protocols.

The Internet is in the early stages of a major shift from the original version of the Internet Protocols—known as IPv4—to IPv6. The new version offers multiple improvements in security and functionality over the original, but the main driver for the adoption of IPv6 is that it offers a greatly expanded number of IP addresses to identify networked devices.

Although the pool of available new IPv4 addresses is shrinking, there is still plenty of life left in the original protocols. IPv4 continues to dominate the Internet and will continue to be with us for the foreseeable future. But the rapid growth of the IoT will come in the IPv6 space. The two protocols are not interoperable, which means that enterprises and network providers will essentially be operating dual infrastructures. This alone can create more security problems.

Most security products today support IPv6. But they do not have the decades of experience in working with it that they have with IPv4. It is difficult to say now whether security products will operate as efficiently on IPv6 as on IPv4 when traffic volumes in the new protocols increase.

Also, IPv6 traffic is not now being actively monitored on many networks. IPv6 comes enabled by default on much networking equipment, but because of the relatively small amount of IPv6 traffic today it often is ignored by administrators. This means that IPv6 can provide a backchannel for malicious activity. As the IoT expands, devices using IPv6 could provide an additional channels for unobserved communications.

Not all threats are equal

Some threats posed by the IoT potentially are obviously serious. The ability to interfere with medical devices or onboard systems in ever more sophisticated smart cars could be disastrous. Samsung makes a smart refrigerator that incorporates Google Calendar as a kind of high-tech alternative to the refrigerator magnet and hand-written notes. At first glance this does not appear to be a high-risk application. But the

threats are not always obvious. A compromise of the calendar could provide adversaries with system access, as well as, a user's activities. Even the millions of smart thermostats being installed in homes across the country could, if compromised, provide intelligence that could be exploited.

Regardless of the apparent severity of the risk from any single device, the IoT represents a vast expansion of the Internet's attack surface. Any enterprise or individual linked to this growing array of sensors and controllers faces a growing risk. The security of the IoT cannot be ignored without risk to the critical infrastructures underlying the global economy. Because the IoT includes many sensors and controllers, cyberattacks against the physical domain will become more feasible through this vector. Not only is our information at risk, but physical systems from individual devices to power grids could be damaged.

As early as 2008, the National Intelligence Council [6] recognized the "future … risks that will arise when people can remotely control, locate, and monitor everyday things" through the Internet of Things. "If the United States executes wisely, the IoT could work to the long-term advantage of the domestic economy and to the US military," the authors wrote. "On the other hand, we may be unable to deny access to networks of sensors and remotely-controlled objects by enemies of the United States, criminals, and mischief makers."

In addition to the challenges presented by threats embedded in hardware and firmware, securing the IoT presents other serious challenges as well. A distinguishing characteristic of the IoT is its diversity. Aside from the sheer number of devices being connected, there is a wide variety of designs and functionality from a large number of vendors. Some systems are proprietary, and some are built from widely available off-the-shelf technology. Some comprise individual chips and sensors, others larger complex systems. Some gather public information and are intended for public use, others handle sensitive or classified data and are intended for restricted access.

> *Countering **embedded** threats in **embedded** devices requires security that is **embedded**. … When there is only one chip, security has to be in the chip.*

The IoT solution

Because IoT devices often are designed for specific, limited functions, they often provide limited resources for security functionality. There often is little physical space, little virtual space for memory, limited power and limited bandwidth. These constraints put a premium on efficiency for any IoT security solution.

Countering embedded threats in embedded devices requires security that is embedded. It must be built in, provide machine-time detection and remediation, be affordable and efficient, and able to detect otherwise undetectable threats in hardware and firmware. When there is only one chip, security has to be in the chip.

An analog solution to a digital problem

Fortunately, there is a technology that meets all of these requirements. Power fingerprinting technology is used by PFP Cybersecurity to monitor, analyze and identify otherwise undetectable threats in hardware and firmware.

Either bolted-on for legacy equipment or embedded in new chips as shown in Figure 1, power fingerprinting technology provides an analog solution to cybersecurity. It looks for anomalies that could be indicators of malicious behavior which are manifested in AC, DC and Electromagnetic Interference (EMI) power signals. Because PFP can be embedded in the chip, it operates within the resource constraints of the IoT.

Power fingerprinting:

- Detects dormant as well as active attacks
- Does not require threat intelligence
- Requires no additional software
- Cannot be detected or evaded by attackers

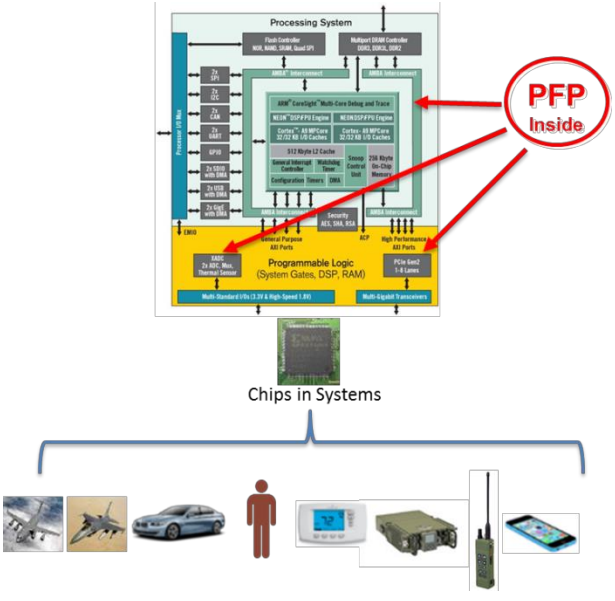

FIG 1. PFP embedded into IoT Chip

How PFP Technology Works

Power fingerprinting (PFP) is a novel approach that utilizes side channels to assess the integrity of an electronic device. Side channels are 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. Power consumption and electromagnetic emissions, depend on the circuit layout, semiconductor technology, and manufacturing process, and therefore, are unique for a given hardware/firmware combination.

PFP is capable of detecting, with extreme accuracy, whenever unauthorized modifications, such as hardware Trojans or counterfeit parts, have compromised the integrity of an electronic system.

PFP does this by performing fine-grained anomaly detection on the device's side channels to determine whether it has deviated from expected operation (Figure 2). 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 has been shown to be effective in a variety of chips, devices and platforms to assess the execution integrity of hardware and firmware.

PFP's tamper detection performance is determined by the availability and quality of the reference baselines. The most straightforward way to produce the necessary baselines is by collecting them directly from a gold (trusted) sample. IoT devices frequently (but not always)

are static applications that always provide the same functionality and hence are quite consistent in execution. For these types of applications a baseline easily can be formed by the OEM as part of the code update. This "known-good signature" can then be loaded for all devices in the field when the new update is applied by the user. For more sophisticated IoT devices, for example an industrial PLC, the professional user of the IoT device "personalizes" the execution of the code to achieve the desired functionality. In this case, there is a baseline associated with the universal firmware, but there also needs to be created a user specific baseline for the tasks/functions the device performs. Side channel signals can be measured directly from the devices using web-based PFP tools and stored using the PFP ecosystem shown in Figure 3.

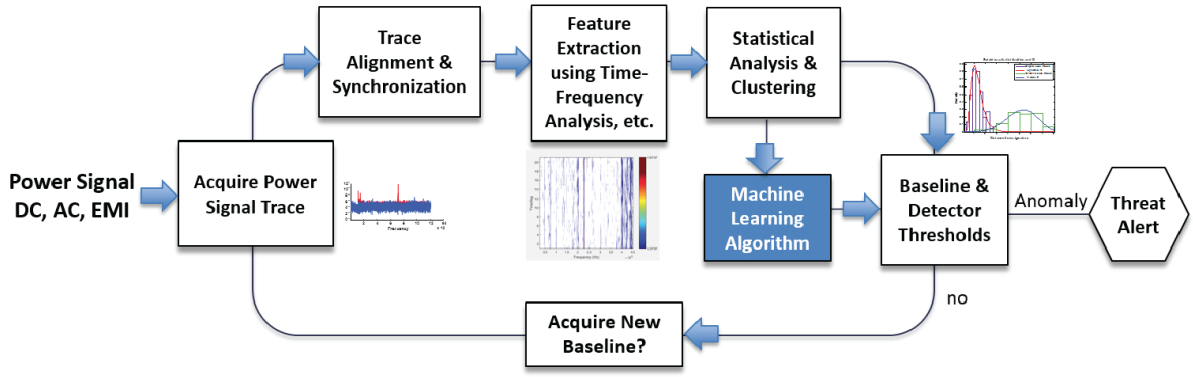

FIG 2. Malware Detection using PFP

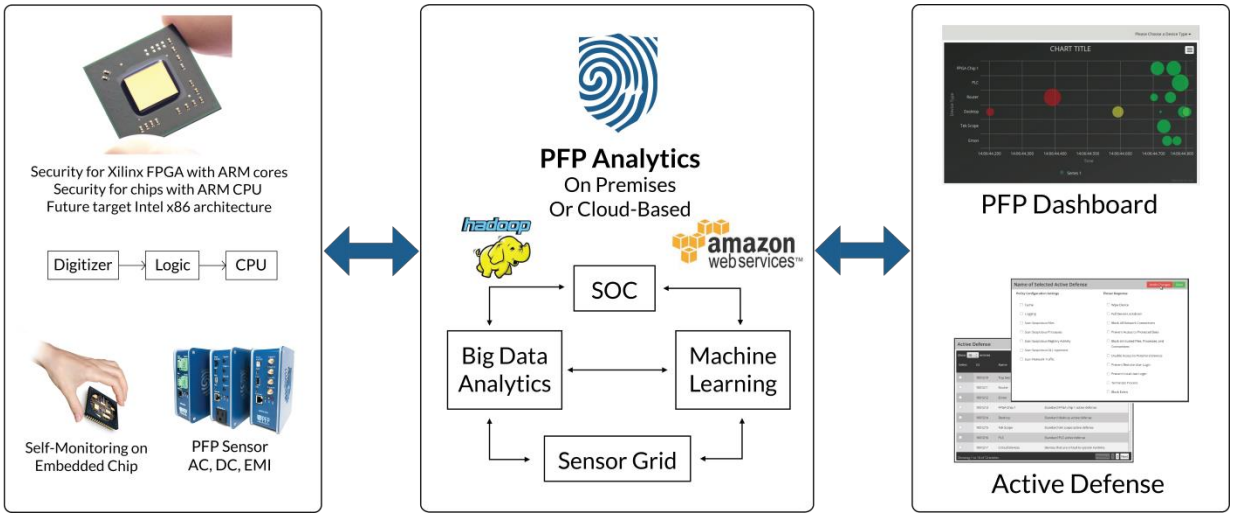

FIG 3. PFP Ecosystem Components

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 IoT risk by providing an agile and effective approach to detect hardware Trojans and counterfeits in IoT devices in real-time and in parallel with standard operational product operation.

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 devices 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 product life cycle.

PFP for IoT

- PFP can handle the wide of variety in IoT devices – doesn't matter what software its running, etc
- "Built-in or bolt-on" – self-monitoring in firmware, or retrofit existing devices
- PFP is transparent to the IoT device – little to no overhead on the CPU
- Deployable at $1 or less per thing in volume

References

[1] [https://www2.trustwave.com/GSR2015.html?utm_source=redirect&utm_medium=web&utm_campaign=GSR2015]

[2] [http://www.arbornetworks.com/news-and-events/press-releases/2015-press-releases/5428-new-ponemon-institute-survey-reveals-time-to-identify-advanced-threats-is-98-days-for-financial-services-firms-197-days-for-retail]

[3] M-Trends® 2015: A View from the Front Lines, Mandiant Threat Report, 2015

[4] [http://labs.lastline.com/lastline-labs-av-isnt-dead-it-just-cant-keep-up]

[5] The Internet of Things, How the Next Evolution of the Internet Is Changing Everything, Cisco Whitepaper, April 2011.

[6] [http://fas.org/irp/nic/disruptive.pdf]

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