PFP CYBERSECURITY

Protection for Industry Control System with Side Channel

Summary

Power Fingerprinting (PFP) protects OT and IT devices by observing the dynamic power behavior for security, quality and safety. It could detect, remediate and authenticate devices from supply chain to the whole life cycle. PFP could be applied without loading of any software artifacts on the target platform, air-gapped, detects anomaly in operation, patching, and authenticate with the combination of hardware and firmware configuration. PFP is out of band, machine time, could be embedded or cloud based. The solution has received 9 issued patents.

Introduction

Industrial control systems (ICS) are computer-based systems that monitor and control industrial processes, from manufacturing to nuclear reactors. ICS is a comprehensive term which typically encompasses a network of components and systems. When controlling large-scale processes across large geographic expanses, ICS incorporates a class of systems called Supervisory, Control, and Data Acquisition (SCADA). SCADA systems are ubiquitous in ICS critical infrastructure, including water treatment and distribution, transportation systems, oil and gas pipelines, electrical power transmission and distribution, wind farms, defense systems, and large communication systems. An attack to critical infrastructure from a well-funded cyber adversary can have devastating consequences to national security. **The Stuxnet worm emerged in 2010 underscoring the vulnerability of ICS to cyber attacks.**

Current ICS network monitoring defensive strategies include updating/patching, strengthening the periphery, and reusing traditional solutions from the Information Technology world. **Unfortunately, these IT approaches provide limited coverage in ICS environments and leave critical systems vulnerable to cyber attacks especially legacy systems using older communications protocols**. Traditional approaches include network-based Intrusion Detection Systems (IDS) and signature-based solutions in host computers, such as anti-virus. These approaches have severe limitations and are insufficient for critical ICSs. IDS solutions based on traffic analysis are notoriously vulnerable to advanced persistent threats, which are cleverly crafted to avoid signature-based detection, minimize network utilization, and mimic legitimate network traffic. Furthermore, traffic-analysis IDS are incapable of detecting malicious intrusions which do not generate network traffic. Such malicious intrusions could communicate using alternative channels (e.g. RS-232, RS 485, USB), simply remain dormant for extended periods of time or provide the user with false sensor information. Signature-based solutions also have severe shortcomings within ICS: (1) are unable to detect zero-day attacks, (2) must reside on the host system consuming valuable resources that CPU-constrained platforms do not have, and (3) do not support embedded systems such as programmable logic controllers (PLCs). In other words, anti-virus for ICS is wanting. **Even years after the discovery of Stuxnet, commercial solutions that directly monitor the actual execution of ICS processes are still absent.**

Power Fingerprinting (PFP), uses physical measurements from a side channel (dynamic power behavior) to detect malicious intrusion in critical systems **PFP is a physics based Anomaly Detection System capable of directly monitoring the execution of components, analog sensor signals, digital communications signals and systems components.** PFP is the ideal candidate to perform anomaly detection directly in ICS, from sensors, PLC, HMI, networks, edge computers, etc.. PFP provides an extra layer of protection, bridges coverage gaps and is complementary to traditional IDS approaches, as shown in FIG. 1.

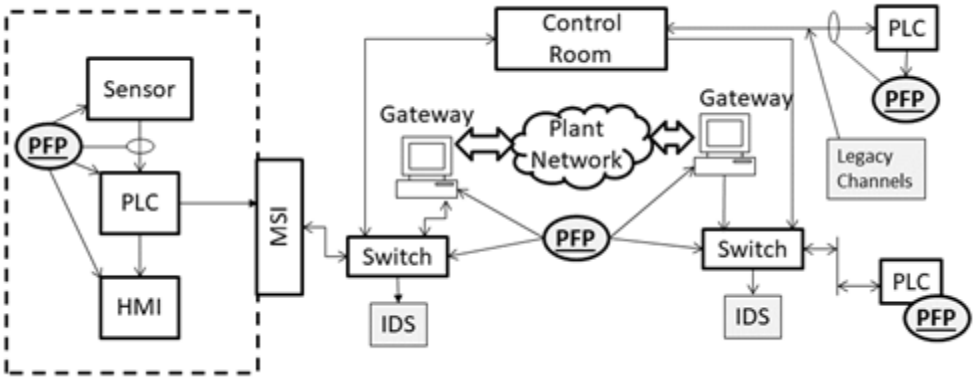

FIG 1. PFP directly monitoring ICS components to detect malicious intrusions

In FIG 1, PFP monitors are shown monitoring the execution of devices in the safety critical zone as well as outside of it. The PFP monitors are deployed in coordination with traditional cyber security solutions, such as anti-virus (AV) and IDS, to provide a comprehensive defense-in-depth for critical systems.

PFP enables the continuous, real-time, direct monitoring of elements of ICS. PFP empowers OT operators with a disruptive capability that did not exist before. PFP is able to detect intrusions at the slightest disruption in execution, even if the malicious intrusion remains dormant or mimics legitimate network traffic. This enhanced detection capability allows the immediate response to neutralize the threat. Furthermore, PFP does not violate the principle of non-interference in terms of safety and security in critical ICS, allowing the monitoring of the most sensitive components. PFP is a dynamic solution to detect quality, safety and security issues such as zero-day threats and adversarial attacks independent of platform, failure scenarios, or attack techniques.

PFP Technology

PFP performs fine-grained anomaly detection on the processor's dynamic power behavior to determine whether its behavior has deviated from and expected response or operational process. A PFP monitor, shown in FIG 2, uses a physical sensor to capture fine-grained electromagnetic signals, also known as "side channels", which contain tiny patterns or "fingerprints" that emerge during the transition from one instruction to another. In PFP, power traces are processed using signal detection and classification techniques on an external device. The observed traces are compared against trusted

references to assess whether the execution has deviated from its expected behavior, e.g. when an attack has managed to install malicious software.

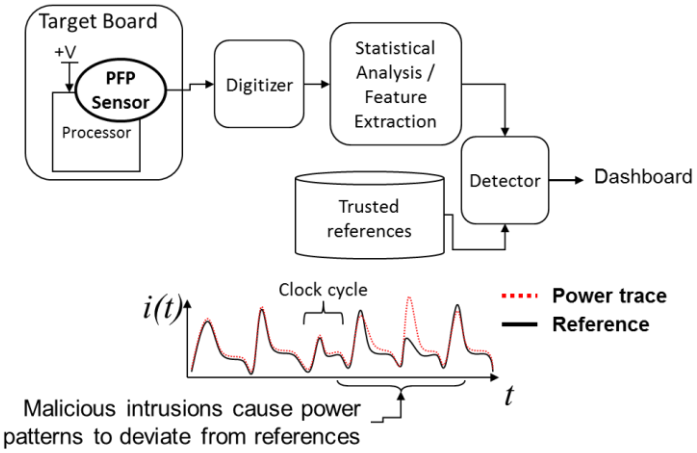

FIG 2. PFP Monitor

Because the monitoring is performed by an external device, the memory and processing overhead on the target is greatly reduced or eliminated. Also, PFP monitors can be built using Commercial off-the-shelf (COTS) components.

PFP can combine traces from multiple instances of the target execution in order to increase accuracy and reduce the chances of making an error**. In other words, it is possible for a PFP monitor to achieve an arbitrary probability of false alarm provided that enough execution instances can be observed.**

Monitors

Monitors capture the signals from the devices . A monitor could be a device resides in close proximity to the target, or it could be embedded in devices such as sensors, PLC, and HMI. Such monitors observe, with fine detail, the instantaneous current drain or emission of the processing element during execution. Example monitors include the Keysight instruments, ARM-based Stem-on-Chip IC with an on-chip digitizer and the PFP DIN railed mount pMonitor Model 751.

FIG. 3. Sample monitors

There are different technical options to implement monitors, including current and electromagnetic probes. Current sensors include current probes and current mirrors that can be introduced into the chip or board design of new systems. **Electromagnetic (EM) sensors include near-field antennas that pick up the changes in the electric or magnetic fields caused by processor execution. EM sensors have the advantage that can be used to retrofit legacy devices without modifications to the target platform.**

PFP Analytics

PFP is based on detecting anomalies and deviations from baseline references. These references describe the expected dynamic power behavior and how much variation is considered normal. PFP references can be extracted using different approaches. One of the most straightforward methods includes having a gold sample of the target platform. In this scenario, PFP baselines are determined by executing the gold sample in a controlled environment while observing its dynamic power behavior. This process, depicted in FIG 4 is very close to automated software testing, thus PFP can leverage existing tools to facilitate the baseline extraction process. While references are unique to a specific target system, the process to extract them is general and can be applied across platforms and applications.

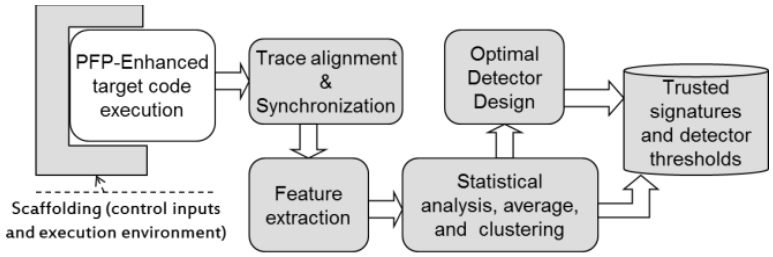

FIG. 4. PFP Characterization Process

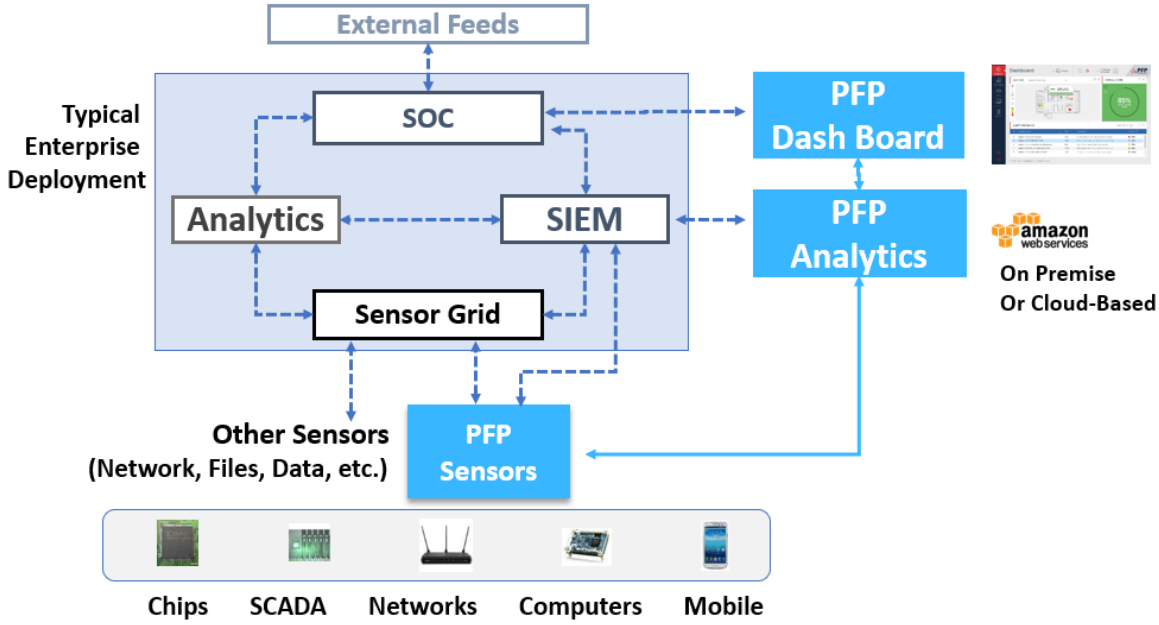

FIG. 5. The PFP solution is compatible with many existing deployment

The PFP solution in FIG 5 is available for PC based and Cloud based. The PC based P2SCAN is intended for use without network and cloud, as a travel kit. The cloud based P3SCAN is available on AWS for enhanced scalability in enterprise environment. The PFP solution could be interoperable with existing implementation.

PFP Results and Examples

PFP is a proven technology which has been successfully applied to simple and complex platforms. The principles behind PFP apply to any digital platform. PFP has been proven on a variety of platforms across all layers of the execution stack – from hardware layers to the application layer.

Siemens S7 PLC

Using COTS components we have successfully detected a malicious intrusion in a Siemens PLC. In this demonstration, the original control logic in a Siemens S7 PLC is characterized and monitored. A malicious intrusion similar in operation to Stuxnet is then introduced. When a trigger condition is present, the intrusion activates and sabotages the operation of the control system while hiding its actions from the operators. Similar to Stuxnet, when the trigger condition is not present the intrusion goes into a dormant state. When dormant, the intrusion has no impact on the logic operation and produces no suspicious network traffic.

PFP successfully detected the malicious intrusion even when the trigger condition is not present. The intrusion's act of checking for the trigger condition is enough for PFP to catch it.

A short video of this demonstration can be seen at: http://youtu.be/-ENkJbUaIvA

Lateral Movement

This example shows PFP's ability to detect lateral movement of attacks in an OT environment which consists of an IP camera, a Cisco router and a Siemens PLC with sensors and HMI (FIG 6).

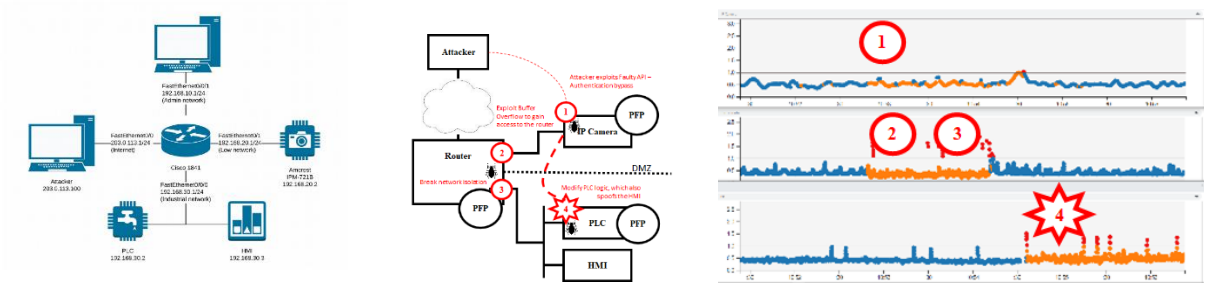

FIG. 6. A sample OT test cell

In this demo scenario attackers perform the following tasks in seconds.

1. From the IP camera, attacker exploits Faulty API – Authentication bypass
2. Exploit Buffer Overflow to gain access to the router
3. Break network isolation
4. Modify PLC logic, which also spoofs the HMI

PFP detects the attackers when they get onto each device in real time and notify the operators. If the attackers could not be detected in real time, they would intrude, attack and disappear without a trace.

Supermicro Servers

Supply chain attack for commercial IT products such as servers received attention after the Bloomberg report about Chinese chip implant. PFP has developed an emulated attack by delivering malware through a backdoor which was loaded after reboot.

In this example, the PFP analytics was able to detect an emulated UEFI attack. PFP could also detect other hardware and firmware tampering such as BMC, TPM, etc. PFP could collect signals from the SETA bay connector, PCIe bus, over the BMC chip, etc. PFP can also be applied to storage and network equipment.

PFP is a signed security partner for Supermicro. *A video of this project can be seen at*: https://youtu.be/PhAim50qeWo

FIG. 7. Emulated UEFI attack on a Supermicro X11

Xilinx FPGA

Another example is the PFP solution assess the integrity of hardware using an FPGA and detect tampering introduced at the supply chain. The target platform is a Xilinx Spartan 3 FPGA. The original design is tampered, introducing potentially harmful functionality, but which is activated only under a specific condition. The tamper hides the malicious functionality, remaining dormant for extended periods of time and then activating when the right conditions are present.

Traditional functional and acceptance testing are unlikely to detect such conditional tamper, as the input conditions that trigger the Trojan are chosen such that they are only activated by very specific inputs, unlikely to ever be present under normal operation. The PFP monitor, however, was able to successfully detect the hardware tampering, even when the trigger condition is not present, because the very act of checking for the condition by the trojan is an anomaly! The PFP analytic could collect data with various monitors such as the Keysight CX3324, Tektronix DSO, Picoscope and the PFP Model 751.

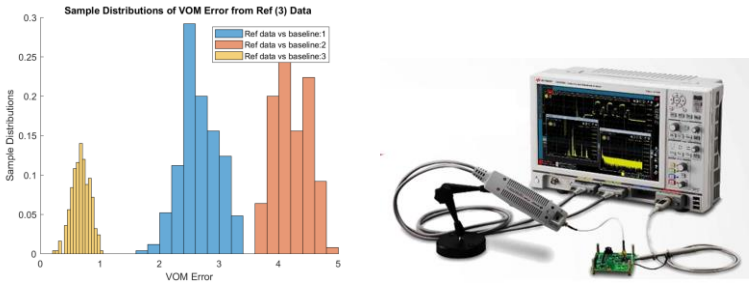

FIG. 8. The PFP Analytics Cloud and PC based

PFP Conclusion

PFP is a proven technology able to monitor directly the execution of devices with constrained resources. PFP has been successfully demonstrated on simple and complex platforms. PFP technology does not require the loading of any software artifacts on the target platform. The principles behind PFP apply to any devices. PFP can detect anomaly in security, quality and safety to OT and IT devices and protect this critical infrastructure. today.

For more information visit: www.pfpcyber.com
Email: info@pfpcyber.com