Cyber Security and Safety for Utilities

A White Paper from PFP Cybersecurity

Summary

Detecting threats to our critical infrastructure has never been more difficult and our nation's security has never been more important. Utilities today face a challenging task of quickly detecting and remediating threats from supply chain to runtime throughout the whole life cycle. This whitepaper provides some of the key challenges facing Utilities today and highlights how a new technique of monitoring utility assets with the lowest possible denominator – power profiling – can solve these challenges. A key PFP technology advantage is that we don't have to know anything about an attack. Through PFP's Security as a Service, Utilities can detect and alert immediately. Zero-day attacks cannot get by PFP protected Utilities.

Cybersecurity Challenges for Utilities

Protecting critical infrastructure has never been more challenging and our nation's security has never been more at risk. Awareness that "cyber vulnerability is real", is no longer an issue within Utilities. Utilities now recognize they are vulnerable – now they want to detect a cyber-anomaly when it happens not days or months later. The changing nature of cyber security attacks has made cyber defense a moving target. Utilities today are constrained on resources – there is a shortage of manpower to configure firewall and deep packet inspection rules, manage events and remediate.

To make matters worse, Utility cyber-attacks can be introduced throughout a device's lifecycle – in the supply chain, during setup or configuration, as well as, traditional operational cyber-attacks during deployment.

Kris Ardis highlights seven smart meter security threats that do not involve hacking the network at all:[1]

1. Replace IC's with fakes
2. Use social engineering to load bad software during manufacturing
3. Steal software or decompile to clone meters
4. Meters replaced with fakes
5. Inside job to recalibrate meters
6. Hackers monitor communications channels
7. Hackers physically attack the meter to change code or retrieve keys

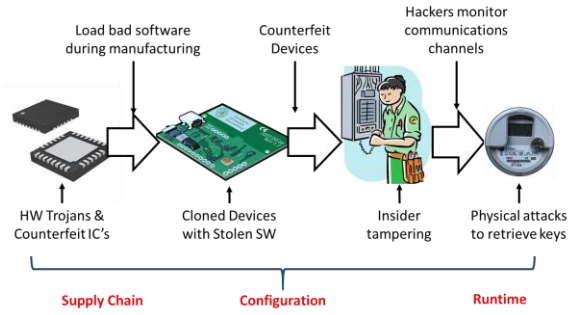

FIG 1. Security threats no longer involve hacking the network[1].

With near 20 billion IoT devices expected in service by the year 2020, most industries, if not all, will face cyber threats throughout the device's life cycle.

Limitations of Traditional Utility Cybersecurity Solutions

Industrial IoT devices used in critical infrastructure present unique challenges that make the application of traditional

cybersecurity solutions difficult or ineffective. Industrial IoT devices used in Industrial Control Systems (ICS), such as PLCs, feeder relay controllers, SCADA systems, phasor measurement units (PMU) for transmission, automated capacitor banks and feeder switching for distribution, are extremely difficult to protect because they have limited processing resources, operate under strict timing constraints, have stringent safety and reliability requirements, are often based on legacy embedded platforms, and they lack the ability to install security software.

The bad guys, using techniques, such as polymorphism and advanced persistence, have made malware detection through signature recognition all but meaningless. As operations networking (frequently called OT systems) become more complex with every device being "connected", the risk for nefarious activity increases daily.

Simultaneously, attacks against Smart meter endpoints are becoming more sophisticated. Highly motivated and well-resourced adversaries are developing complex threats that avoid detection and remain persistent in systems compromised at the endpoints.

The traditional solution, for some time, has been the concept of defense-in-depth. In a nutshell, use many active layers of defense in the belief that one of the layers will always be able to detect an intruder, and hence, if the first layer lets him in, the second or subsequent lines-of-defense will catch him. Although sound in principle, attackers have proven in recent years that holes can always be found to evade the Utility Company's best defenses.

In today's threat environment, Utility Companies must now extend their protective wall even out to the endpoint where the service is provided. In essence, defense-in-depth, a once proven concept, is now one more concept on the scrapheap of history. Modern cyber warfare relies on instantaneous detection and remediation. But doing this with the limited resources of industrial control systems or IoT devices is impossible in practice.

Compounding these problems with using traditional cyber-solutions, are threats embedded in hardware and firmware. Currently undetectable by traditional security tools, these threats are expected to become more prevalent.

Detecting threats to our critical infrastructure has never been more difficult and our nation's security has never been more important.

Consider the existing state of cybersecurity.

- Detecting breaches takes too long; several studies show that breaches routinely go undiscovered for extended periods.
- Unknown unknowns; you cannot stop what you don't know how to defend against. New attacks such as supply chain, implant and memory attacks, etc. are difficult to detect.
- Noise-to-signal; Although cyber 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, will provide long term invisibility. The result is a growing window of opportunity for hackers, criminals and nation states to exploit your critical infrastructure.

What's at Stake

As dependence on smart systems increases with the growing connectivity of equipment in utilities, a successful cyber-attack is capable of causing massive physical, economic, and psychological harm to any population. For critical infrastructure operators, such as electric utilities, dependability is much more than a slogan, it is a mandate.

As highlighted by the recent Ukraine BlackEnergy attacks [2], a successful utility cyber-attack will disrupt operations. The obvious loss of revenue is nothing compared to the damage to the Utility's reputation for reliability and ultimately the government scrutiny and "help" that will follow. The risk of "brand" tarnishing and the additional regulations by policy makers who's perception is one of "infrastructure operators are not doing enough on their own accord" is very real.

Consider the seemingly innocuous Utility "disconnect" command on a smart meter. Under hacker control, this simple command can be used to cause widespread blackouts by destabilizing the entire grid.[3]

What are the Keys to Success

Utility operators need to show a proactive approach and do more than the required minimum measures. Utilities need to show that their unique cybersecurity requirements are being addressed and that future threats are being considered.

In order to address all these cybersecurity challenges, it is necessary to devise trust and protection solutions that address challenges throughout the life cycle, from cradle to grave of all Utility end-point devices. It is necessary to understand that a dedicated adversary will eventually evade preventive measures, and to invest in immediate, reliable detection across networks and endpoints. Solutions need to be deployed without disrupting operation, handle the broad diversity of systems and platforms (including embedded and legacy), and be cost-efficient to fit into the tight margins of the utilities operational budgets.

PFP enables a new capability of detecting tampering regardless of where it occurs – hardware, firmware, or software.

In this whitepaper, we will look at Utility cyber protection across the entire utility ecosystem. Key areas are grid infrastructure protection, utility company supply chains, and smart end-point protection. However, it will be useful to first outline the power fingerprinting technique and why this solution solves the Utility Company's cybersecurity needs.

PFP: A Platform of Trust for Connected Devices, IoT, and End-Points

PFP detects anomalies by power analysis of so-called side-channel signals such as AC, DC, EMI, etc. Leveraging digital signal processing and machine learning, PFP can cluster side channel data at different levels, providing visibility at different scales to detect tampering at layout, manufacturing, firmware load, configuration,

software coding, etc. PFP enables a new capability of detecting alterations regardless of where they occur – hardware, firmware, or software. PFP PowerIQ monitoring can be used without impact to latency or adding overhead. The key elements of the PFP solution, shown in Figure 2, include the PowerIQ analytics, the customized user interface and the optional embedded software if remediation is desired.

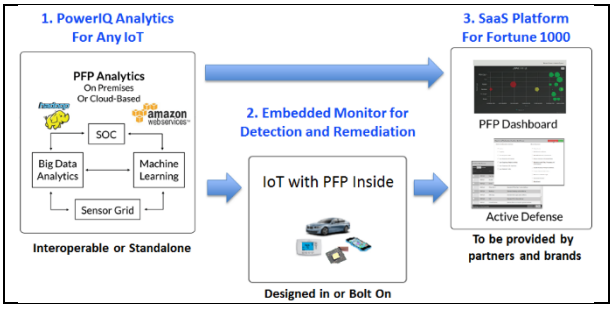

FIG 2. The PFP Solution System Diagram

PFP malware and tamper detection, depicted in Figure 3, performs fine-grained anomaly detection on the Utility's end-point device (e.g. a feeder relay or PMU) by monitoring and profiling power fluctuations (side channels) to determine whether a device has deviated from expected operation. A PFP monitoring system 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 devices to assess the execution integrity of hardware and firmware. An important implementation point is that PFP technology can be applied without bringing down utility operations.

The Department of Energy (DOE) has included the power fingerprinting technology in its 5-year roadmap for grid modernization. PFP is currently working with the DOE's Savannah River National Laboratory (SRNL) and its partner, Clemson University to determine how best to integrate PFP's power fingerprinting technology into grid applications.

PFP power fingerprinting technology provides an analog solution to cybersecurity using the lowest possible denominator –power profiling– making it virtually impossible to evade because PFP looks for the manifestation of anomalous indicators of malicious behavior revealed in the AC, DC and Electromagnetic Interference (EMI) power signals.

For legacy devices, such as controllers, routers and other endpoints, PFP provides the pMon products which perform machine-time monitoring. The PFP solution can be deployed on premise or as a cloud-based SaaS (Security-as-a-Service). The monitoring devices are included in the PFP subscription so additional cost calculations are unnecessary.

PFP Detects Zero-Day Attacks
No threat intelligence required – you don't have to know anything about an attack.

We will now review each of the key Utility areas that must be protected:

(1) infrastructure protection,
(2) company supply chains, and
(3) endpoint protection.

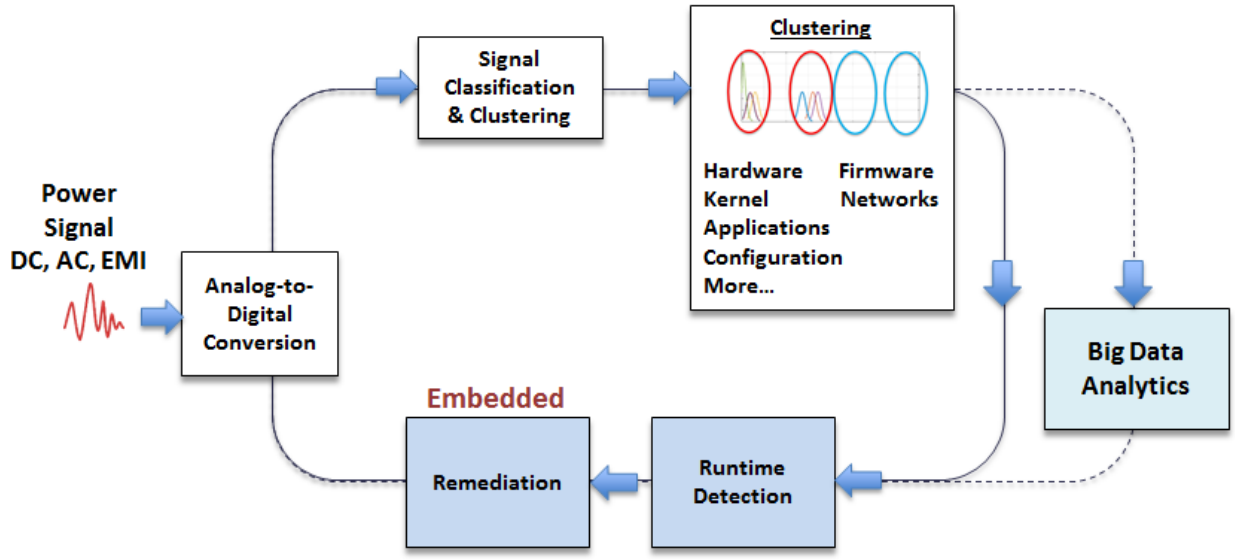

FIG 3. Malware Detection using PFP

Utility Grid Infrastructure Protection

Because intelligent electrical devices (IEDs) often are designed for specific, limited functions, they provide inadequate resources for security functionality. There often is little physical space, low virtual space for memory, limited power and restricted bandwidth. These constraints put a premium on efficiency for any security solution.

For example, a feeder protection relay is a critical portion of the power distribution infrastructure in the United States. A typical feeder relay is the Schweitzer Engineering Laboratories SEL-751A which provides sophisticated grid protection, automation, and control capabilities and yet has no cyber-protection ability. The Department of Energy, Savannah River National Laboratory asked PFP to use its power analytics to detect cyber attacks to the SEL-751A feeder relay. Using both AC monitoring and sensors which monitor radiated RF energy, PFP detects malicious attacks and alerts grid operators of an attack (see Figure 4).

When controlling large-scale processes across large geographic expanses, Utilities incorporate a class of systems called Supervisory, Control, and Data Acquisition (SCADA). SCADA systems

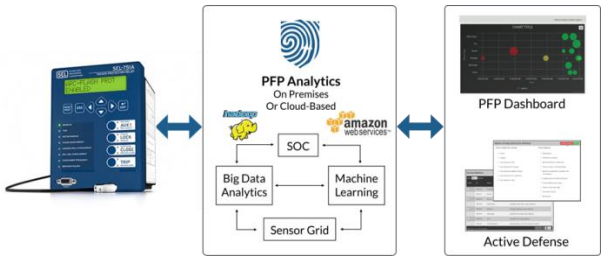

FIG 4. PFP Protects SEL Feeder Relay

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.

Current ICS defensive strategies include updating/patching, strengthening the

periphery, and reusing traditional solutions from the Information Technology world. Unfortunately, these approaches have provided only limited success in the Utility environment and leave critical systems vulnerable to cyber attacks. Traditional approaches include network-based intrusion detection systems (IDS) and signature-based solutions in host computers, such as anti-virus. 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. USB) or simply remain dormant for extended periods of time. Signature-based solutions also have severe shortcomings within Utilities, as they (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).

The Stuxnet worm emerged in 2010 underscoring the vulnerability of ICS to cyber attacks.[4] Even 6 years after the discovery of Stuxnet, commercial solutions that directly monitor the execution of ICS processes are still absent. PFP was tested at SRNL for monitoring ICS processes running on PLCs and detected even minor cyber changes.[5] Other testing has shown the PFP solution detects Stuxnet in milliseconds even when the malware is dormant (gray cluster in Figure 5).

A frequent entry point for attacks in the ICS OT world is, interestingly, the enterprise IT network itself. The underlying router infrastructure has been viewed as safe since enterprise router attacks have been virtually unheard of. FireEye notes, "Router implants, from any vendor in the enterprise space, have been largely believed to be theoretical in nature and especially in use," until recently. In 2015, Mandiant confirmed the existence of "router implants [which] spread

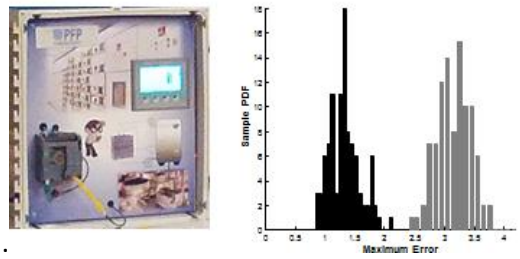

FIG 5. PFP power analytics on Siemens' PLC

across four different countries." [6] This Cisco router implant was called SYNful Knock, and as FireEye notes:[6]

> SYNful Knock is a stealthy modification of the router's firmware image that can be used to maintain persistence within a victim's network. It is customizable and modular in nature and thus can be updated once implanted. Even the presence of the backdoor can be difficult to detect as it uses non-standard packets as a form of pseudo-authentication…
>
> Finding backdoors within your network can be challenging; finding a router implant, even more so. …
>
> The impact of finding this implant on your network is severe and most likely indicates the presence of other footholds or compromised systems. This backdoor provides ample capability for the attacker to propagate and compromise other hosts and critical data using this as a very stealthy beachhead.

PFP power analytics have been proven to detect embedded attacks on router infrastructure, as well. The PFP solution, shown in Figure 6, was independently tested and shown to successfully detect malware router implants including the recent SYNful Knock memory implant on Cisco 3845 routers.

FIG 6. PFP Model 801 detects SYNful Knock implant on Cisco Routers

Utility Supply Chain Protection

The complex, multinational nature of electronics manufacturing in today's world 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.

Counterfeit electronics have become a major challenge in a complex supply chain. (See PFP's Whitepaper[7] for detailed discussion of PFP capability for Supply Chain protection.)

Four of the seven, non-network hacks highlighted by Ardis [1] are supply chain issues. 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.

PFP test equipment uses Commercial Off-The-Shelf (COTS) components providing a low-cost supply chain solution. PFP is much faster compared to other inspection approaches, since PFP can observe and perform its analysis in parallel with routine power-up and functional testing. PFP has been shown effective in a variety of chips, devices and platforms to assess the execution integrity of hardware and firmware.

When PFP is used as part of an acceptance or laboratory test to validate component and subsystem integrity, it can instantly provide a good/no-good assurance signal.

Utility Endpoint Protection

Countering embedded threats in embedded devices requires security that sees what's happening in the embedded processor. This cyber protection can be built in or monitored from outside the device, but it must provide machine-time detection and remediation, be affordable and efficient, and be able to detect otherwise undetectable threats in hardware and firmware.

The National Institute of Standards and Technology, Guidelines for Smart Grid Cybersecurity[8], state:

> "With intelligent electronic devices (IEDs) playing more critical roles in the smart grid, there is an increasing need to ensure that those IEDs are not easily attacked by firmware updates, commandeered by a spoofed remote device, or swapped out by a rogue device. At the same time, because of the unique nature and scale of these devices, protection measures should be cost-effective as to deployment and use, and the protection measures must be mass-producible. … Further, it is important to assume devices will be penetrated, and there must be a method for containment and implementing secure recovery measures using remote means."

PFP power fingerprinting technology can be used to protect any end-point device (including Smart Meters). As shown in Figure 7, a Utility technician can check the cyber-status of any meter in the field with a simple handheld monitoring device.

As a longer term strategy, the Utility can have PFP technology incorporated by the OEM meter supplier, allowing remote monitoring and instantaneous remediation by directly embedding PFP capability in new smart meters.

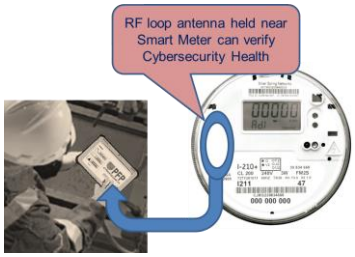

FIG 7. Walk-Around Periodic Cybersecurity Checkup Concept

Conclusions

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 is a proven technology and ecosystem capable of detecting tampering and malware at all levels within the Utility enterprise from hardware to firmware to software.

PFP can help minimize cyber risk by providing an agile and effective approach to detect hardware Trojans and counterfeits in devices in real-time and in parallel with standard operational technology.

PFP has been successfully demonstrated on simple and complex Utility 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 Utility systems is not compromised throughout the entire product life cycle.

PFP for Utility Company Solutions

- PFP can handle the wide of variety of devices – doesn't matter what software it's running, etc.
- "Built-in or bolt-on" – self-monitoring in firmware, or retrofit existing devices
- PFP is transparent to the device – little to no overhead on the CPU
- Detects dormant as well as active attacks
- Does not require threat intelligence
- Requires no additional software
- Cannot be detected or evaded by attackers

References

[1] "7 serious smart meter security threats that do NOT involve hacking the network", July 28, 2014, http://www.smartgridnews.com/story/7- serious-smart-meter-security-threats-do-not-involve-hacking-network/2014-07-28

[2] "Analysis of the Cyber Attack on the Ukrainian Power Grid", SANS ICS, E-ISAC: http://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf

[3] "Industry experts: Hackers can now 'harm human life' through smart meters", K.T. Weaver, Take Back Your Power, 02-01-2015.

[4] "Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon", Kim Zetter, Crown Publishers, 2014.

[5] New Technology Detects Hacks in Milliseconds http://www.bloomberg.com/news/articles/2015-02-03/new-technology-detects-hacks-in-milliseconds

[6] "SYNful Knock - A Cisco router implant - Part I", September 15, 2015, https://www.fireeye.com/blog/threat-research/2015/09/synful_knock_-_acis.html

[7] "Supply Chain Protection White Paper", PFP Cybersecurity, 2015.

[8] "Guidelines for Smart Grid Cybersecurity", NISTIR 7628, The Smart Grid Interoperability Panel –Smart Grid Cybersecurity Committee, http://dx.doi.org/10.6028/NIST.IR.7628r1

For more information visit: www.pfpcyber.com
Email: info@pfpcyber.com
PFP Cybersecurity is also known as Power Fingerprinting, Inc.
utility security white_paper 2016 7.docx