Detecting Zero-Day Attacks in Real Time on Day Zero

Industrial Device Integrity Assessment – Hardware, OS & Software Malware Detection

© 2014 PFP Cybersecurity
Mr. Brooks is focused on new technologies and solutions for industrial and commercial applications for the protection of critical infrastructure. He has more than 30 years developing and managing a wide variety of solutions for military and industrial applications. Mr. Brooks has engineering degrees from the University of Florida (BS) and the Massachusetts Institute of Technology (MS) with a thesis in Human-Machine Systems and Controls. He also has a University of Chicago MBA. He was a key member of the IEEE/NIST Committee on Smart Sensors (IEEE 1451). Mr. Brooks has published or presented in more than 40 industry journals, symposiums and conferences, and holds two patents. One patented product won 1993 Star Tech Award for Best New Product in Washington Technology magazine.
The Detection Gap

“On any given day, some 50 percent or more of known malware is undetectable.” CounterTack

“Signature-based antivirus is dead” ZDNet

“The Antivirus Era Is Over” MIT Technology Review

“We don’t actually know how to scan for malware. We can’t stop it, because we can’t find it.” Scientific American

- Malware in embedded devices (partial list)
  - SCADA/PLC Attacks: Stuxnet, both dormant and active
  - Router Attacks: Routing table, forced write, etc.
  - Bios Attacks: Root Kits
  - Mobile Device Attacks: RATC

- Supply Chain
  - Trojan Integrated Circuits: Designed in US, produced in China with backdoor
“Software solutions are no longer enough for software attacks”

“The Hardware Assisted Defense”

Improving Critical Infrastructure Cybersecurity Executive Order 13636 Preliminary Cybersecurity Framework (10-22-2013)

− **Anomalous activity** is detected in a timely manner and the potential impact of events is understood.

− **A baseline** of normal operations and procedures is identified and managed.

− **The physical environment** is monitored to detect potential cybersecurity events.
Current Solutions & What we Need

Today The Trend

- Application Layer
- Network Layer
- Physical Layer

Current Vendors

- Hardware Assisted
- Out-of-Band Detection

Software Execution
- OS
- BIOS

Hardware

The Trend
A New Approach using Sideband Analysis – Quantitative and Deterministic

- Detect intrusions by anomaly detection on the processor’s power consumption

Side-Channel Non-Contact

New Power Trace

Compare New Data with the Baseline

Anomaly?

Alert User

yes

no

Evaluate Next Module

Real Time and Near Zero False Positive
How Sideband Cyber Attack Discovery Works

Plant Operator Monitors Plant

SCADA System
- CPU
- Memory
- Power Supply

Current Monitor

Control Valve In Plant

Create Baseline of Instantaneous Power Usage

Monitoring Unit

Create Baseline of Instantaneous Power Usage

Monitoring Unit

Plant Operator Monitors Plant
Cyber Attack Discovery by Monitoring Power Changes

Plant Operator Sees Everything is Good

SCADA System
- CPU
- Memory
- Power Supply

Control Valve In Plant

Match Signature

Monitoring Unit

Current Monitor
Cyber Attack Recognition Thru Power Discrepancies

Only one "bit" is different

Monitoring Electrical Signature allows one to "see" the change

Only one "bit" is different

Control Valve in Plant

Instantly detect Anomaly in baseline

Monitoring Unit

Hacker Injects Malicious Code

Plant Operator is "Alerted" System Compromised

SCADA System

CPU

Memory

Power Supply

Current Monitor

Monitoring Unit

Hacker Injects Malicious Code

Plant Operator is "Alerted" System Compromised
Cyber Attack Recognition Thru Power Discrepancies

- SCADA System
  - CPU
  - Memory
  - Power Supply

- Monitoring Unit

- Control Valve In Plant

- Instantly detect anomaly in baseline

- Monitoring electrical signature allows one to “see” the change

- Only one “bit” is different

- Hacker Injects Malicious Code

- Plant Operator is “Alerted” System Compromised
The End-to-End Approach

- **A disruptive, effective and simple solution**
  - Detect the zero-day attack
  - Detect both Active & Dormant attacks
  - No Added Software Needed
  - Non-intrusive (no electrical contact)
  - Scalable from chips, boards, devices, systems, etc.
  - Nearly impossible to evade
Probes

- COTS probes
- Low-cost custom design with and without connectors
- Traces on boards or chips have no cost impact
The Deployment Process

**Exploration**
- Identify probe requirements
- Identify sampling requirements

**Characterization**
- Extract PFP baseline feature sets

**Integration**
- Set user-defined parameters
- Create Response policy
- Develop Dashboard / UI / API

**Monitoring**
- Assess integrity
- Initiate response
- Update UI

**Maintenance**
- New version characterization
- System updates
A Sample Deployment

1. Identify the target device
2. Establish the baseline with a Scanner
3. Verify the monitoring solution
4. Set up a Monitor with the verified solution
5. In-Field baseline update?
6. Maintenance and ongoing monitoring

- Devices to be monitored
- Baseline
- Anomaly

Enable new baseline with software update or on demand

Cloud-based and third-party monitoring solutions

Testing at Savannah River National Lab
Threats in Semiconductor

- Detecting tampering (kill switch or back door) in chips and modules
- An emulated backdoor
  - Invert output only when cond_1 is true

Cond_1: True
DORMANT
Kill switch loaded

Cond_1: False
ACTIVE
Kill switch Activated

Clear separation = no false positive

Deterministic, no false positive

FPGA Short Video
http://youtu.be/3VVuUG7z1go
Threats in Android

- Android OS running on the Motorola Droid Processor
- Malware distributed in the Official Android Market
  - Used by DroidDream, DroidKungFu, and other malware
- RageAgainstTheCage (RATC) Privilege Escalation Attack
- Monitored Kernel integrity

Proven for sophisticated CPUs and Operating Systems
Threats in PLCs (Stuxnet)

• On a Siemens PLC (SIMATIC S7-1200) in both Dormant and Active Modes, targeted by Stuxnet (similar to the Iranian setup)

• PLC Logic: Tank level control

---

![PLC Diagram](image)

**Real-Time, Continuous Monitoring**

---

PLC Short Video
http://youtu.be/biRAIt7VbPk
• Initial step, sample the RF emissions given off by the PLC’s processor for each execution path.

• The sampled time series of an execution path is referred to as a trace
• Compute the statistical characteristics of the execution path.
• Ideally each cycle of the execution path will be identical within a reasonable amount of uncertainty.

Clear Separation on Deviation from Normal
VISIT US IN
BOOTH #409
FOR A DEMO

Thurston Brooks
tbrooks@powerfingerprinting.com
240-750-9154
2014-2015 Products

- **P2Scan** – kit for users to evaluate and monitor their devices for corruption.

- **eMonitor** – standalone unit and probe. Available in convenient DIN-rail mountable form-factors

- **CoreCloud** – a SaaS solution that provides cloud-based analytics

- **SIEM API** – a software API for interfacing to 3rd-party Security Information and Event Management
# Product Development

- Reducing size, weight, power, and cost

<table>
<thead>
<tr>
<th>Product</th>
<th>Description</th>
</tr>
</thead>
</table>
| **P2Scan-L** (Laboratory ID System) | • COTS  
• Bench-top  
• High-end |
| **P2Scan-P** (Production System) | • COTS  
• Compact  
• Portable |
| **eMonitor**          | • COTS  
• Small Form Factor  
• DIN Rail Mount |
| **Embedded Board-Level** | • PFP embedded on Customer board |
| **Chip**              | • FPGA  
• Stand-alone silicone, or  
• Integrated IP |
| **Laboratory Probe**  | • COTS |
| **Production Probe**  | • COTS  
• $25 with connector |
| **Low-Cost Probe**    | • <$1  
• No connector |
| **Embedded Probe**    | • Traces on board  
• Free |
| **Chip Level**        | • Traces or active circuits on chip  
• Free |
Proofs of Concept

• **Network - Wireless**
  – Attacks such as kernel, routing table, forced write to storage, etc.

• **Semiconductor**
  – Detecting tampering (kill switch or back door) in chips and modules

• **SCADA**
  – Siemens PLC (SIMATIC S7-1200) in both Dormant and Active Modes, targeted by Stuxnet

• **Android OS Kernel integrity**
  – RageAgainstTheCage (RATC) Privilege Escalation Attack

• **Others – Medical, Mobile**