



Power Analysis of Physical Signals on the Edge

Air-gapped AC, DC, or EMI sensing

P2Scan - PC based software containing PFP's patented power analytics algorithms

pMon 751 - Network-based digitizer for data acquisition and signal processing

Accessories - Probes, amplifier, cables, etc.

Optional Additional Sensors - USB adapter, AC power sensor, rack mount sensor

Accurate and Fast

PFP's PowerIQ technology detects anomalies from trusted baselines in machine time. Using the laws of physics, PowerIQ is nearly impossible to evade or detect.

Fully Customizable

P2Scan provides a user friendly interface with point-and-click simplicity. Monitoring parameters, sensitivity, and metrics are fully customizable by the user.

Complete Solution

The P2Scan kit includes all of the necessary probes, amplifiers, and analysis software to immediately begin using PFP capability.


About Us


PFP Cybersecurity provides an IoT platform for security, safety, and quality.

Copyright © 2018 by Power Fingerprinting. All Rights Reserved.

Contact Us

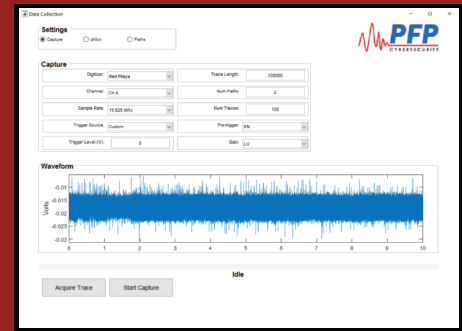
 www.pfpcyber.com

 540 - 200 - 8344

 1577 Spring Hill Road # 405
Vienna, VA 22182

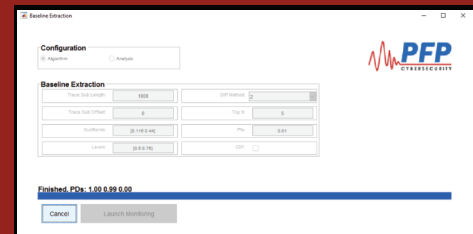
Analog Data Capture

The baseline references, which uniquely identify the execution of a given software routine, are extracted during a controlled "learning" phase before the system is deployed. The included pMon seamlessly integrates with P2Scan to allow easy data capture from the user's devices.



Baseline Extraction with Machine Learning

"Baseline Extraction" guides the user through a series of straightforward steps to create the baseline using PFP algorithms.



Runtime Monitoring

Once the baseline is created, P2Scan monitors the user's system with a simple button push. From that point, P2Scan continuously looks for deviations from the baseline to determine whether an intrusion has occurred.

During Runtime Monitoring, P2Scan provides a number of data views which allow the user to review and interpret the system performance in real time. A persistent graph provides a quick, easy display showing status. For example, a red point indicates an anomaly.



PFP Cybersecurity Overview

PFP provides an IoT platform for security, safety, and quality. PFP detects anomalies caused by hardware and software tampering, such as counterfeits, cloning, implants, and hacking of configuration and data by insiders. PFP's PowerIQ analytics can be on-the-cloud or on-premise for new and legacy Internet of Things.

PFP's physics-based integrity assessment reduces the detection time to mere milliseconds and is capable of detecting malicious intrusions in any device. Even dormant attacks that are simply "listening" can be detected, even if the system is behaving normally from the user's perspective. Easily integrated with existing threat intelligence/management solutions, PFP is complimentary to current cyber security approaches, adding another layer of protection. It has no impact on the performance of monitored systems, and attackers cannot tell they are being monitored.