PFP
CYBERSECURITY

Power Fingerprinting (PFP): Intrusion Detection in Critical Infrastructure using Unintended Analog Emissions

More Situational Awareness for Industrial Control Systems (MOSAICS) Industry Day

4-5 November 2020

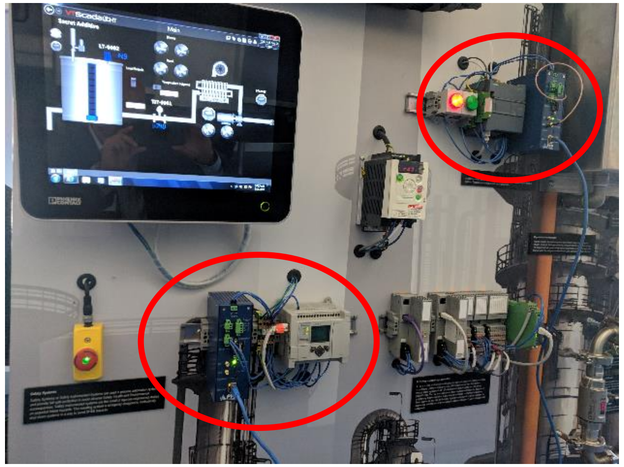
MOSAICS 2020 INDUSTRY DAY

Bottom Line Up Front

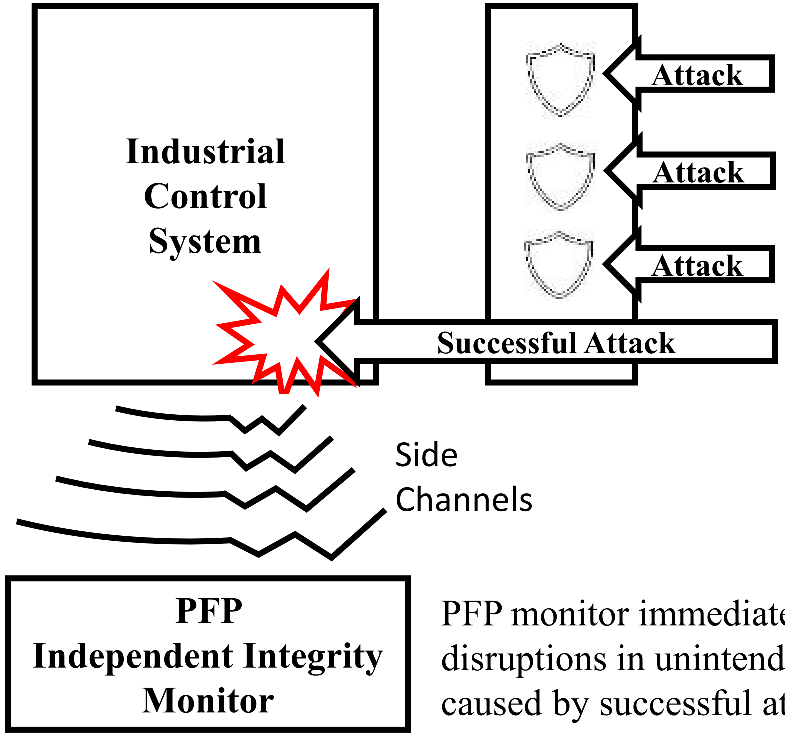
PFP CYBERSECURITY

Power Fingerprinting (PFP) enhances situational awareness in critical ICS by using unintended analog emissions to assess the integrity of devices and detect intrusions

- Create baselines using machine learning and detect anomalies in machine time
- Suitable for resource-constrained platforms
- Effective against zero-day attacks
- Logically and physically isolated operation from target platform



Traditional security measures stop a large variety of attack vectors, but eventually an attack will succeed



PFP monitor immediately detects disruptions in unintended emissions caused by successful attack

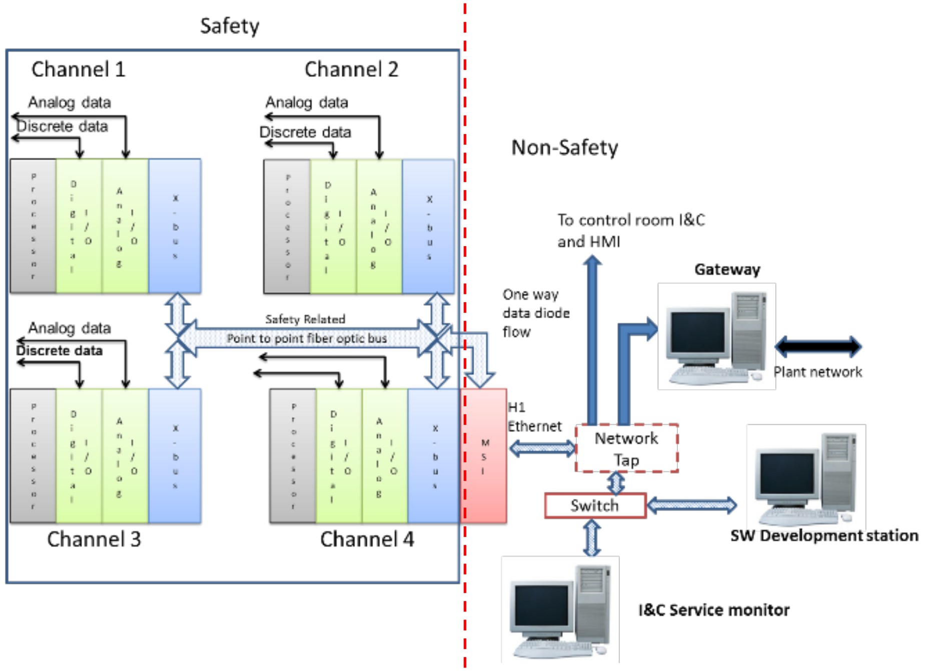
MOSAICS

2020 INDUSTRY DAY

Cybersecurity in Mission-Critical Systems

PFP CYBERSECURITY

- Traditional solutions have limitations for emerging threats in ICS
  - Beyond server and desktops – control, weapons/navigation, and critical systems are at risk, whether they are connected to the Internet or not
- Untrusted supply chain: hardware/firmware tampering
  - Software only solutions cannot reliably detect HW tamper

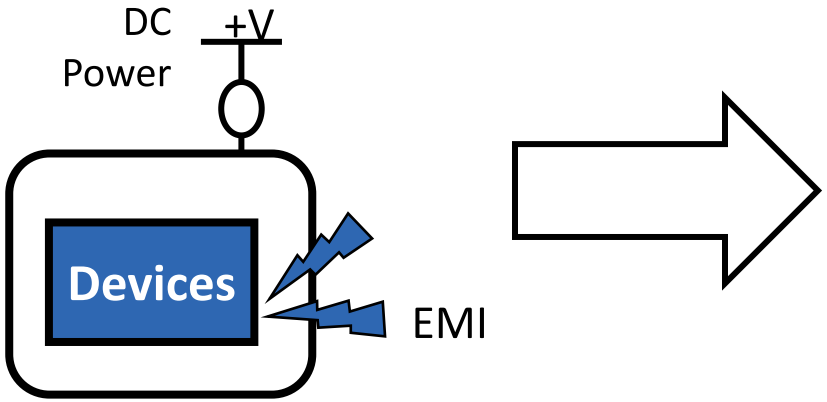


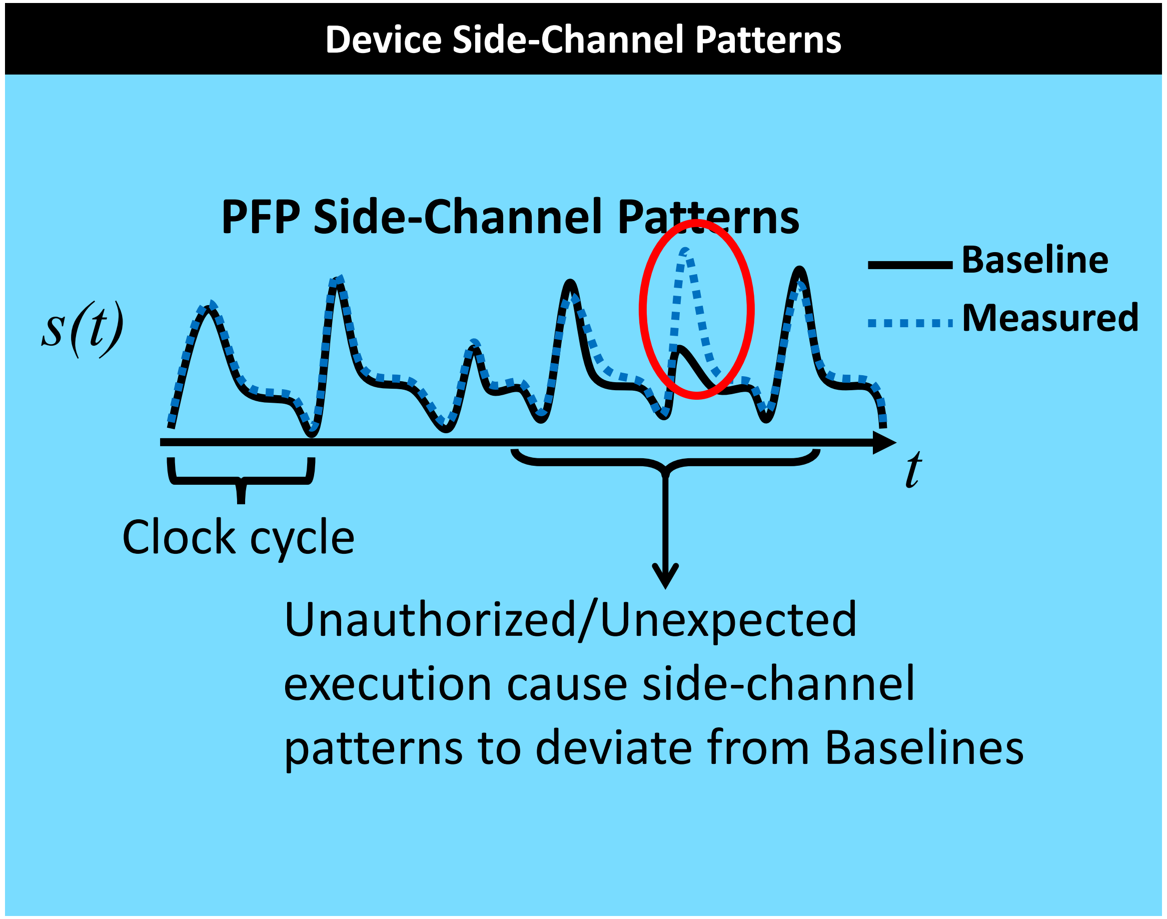
- Strict safety, reliability, & timing requirements
- Legacy systems
- Platform and protocol diversity

Integrity Assessment using Unintended Emissions and Machine Learning

Side channels are unintended analog signals which depend on hardware & firmware and are intrinsic to digital devices

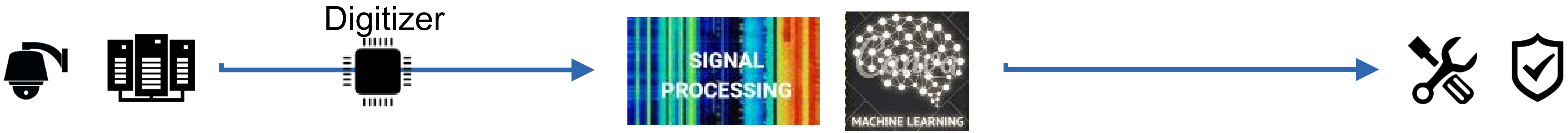
E.g. Power behavior, electromagnetic emissions, temperature, etc.





Unauthorized/Unexpected execution cause side-channel patterns to deviate from Baselines

How PFP's Technology Works



Many Devices

Servers, IoT, Industrial
Control, Analog Power

PFP Analytics

Cloud, On Premise,
PC, or Embedded

Detect & Remediate

Stuxnet, BleedingBIT,
MIRAI, Trojan, etc.

PFP System: COTS sensors, Monitors, Analytics

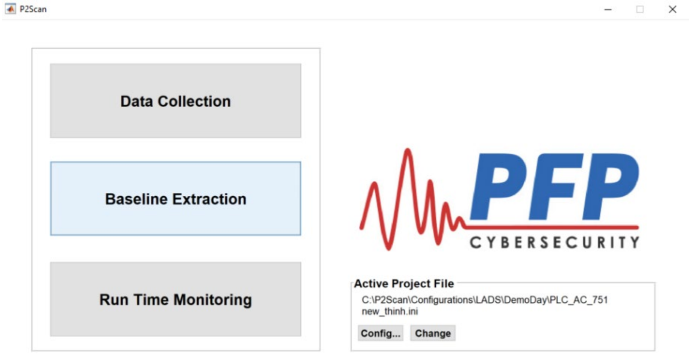
EM Sensors

Current Sensors

pMon-751

Low-cost flexible PFP monitor

- EM and DC sensors
- Collect sensor data
- Local processing evaluation with trained models (reduce bandwidth requirements)



P2Scan

Data Collection

Baseline Extraction

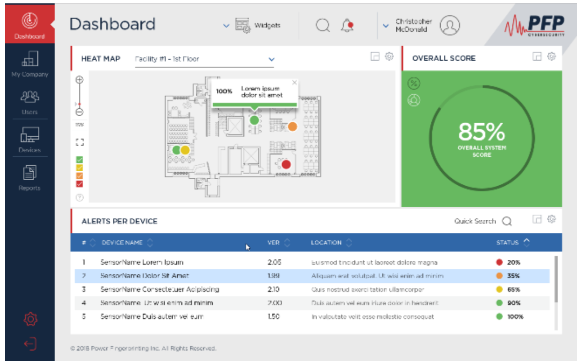
Run Time Monitoring

PFP CYBERSECURITY

Active Project File
C:\P2Scan\Configurations\LADS\DemoDay\PLC_AC_751
new_thinh.ini

Config... Change

P2Scan – Analytics, Mobile, disconnected



Dashboard

HEAT MAP Facility #1 - 1st Floor

100% Lorem ipsum dolor sit amet

OVERALL SCORE

85% OVERALL SYSTEM SCORE

ALERTS PER DEVICE Quick Search

#	DEVICE NAME	VER	LOCATION	STATUS
1	SensorName Lorem Ipsum	2.05	Euismod tincidunt ut laoreet dolore magna	● 20%
2	SensorName Dolor Sit Amet	1.99	Aliquam erat volutpat. Ut wisi enim ad minim	● 35%
3	SensorName Consectetuer Adipiscing	2.10	Quis nostrud exerci tation ullamcorper	● 65%
4	SensorName Ut wisi enim ad minim	2.00	Duis autem vel eum iriure dolor in hendrerit	● 90%
5	SensorName Duis autem vel eum	1.50	In vulputate velit esse molestie consequat	● 100%

© 2018 Power Fingerprinting Inc. All Rights Reserved.

P3Scan – Enterprise Analytics

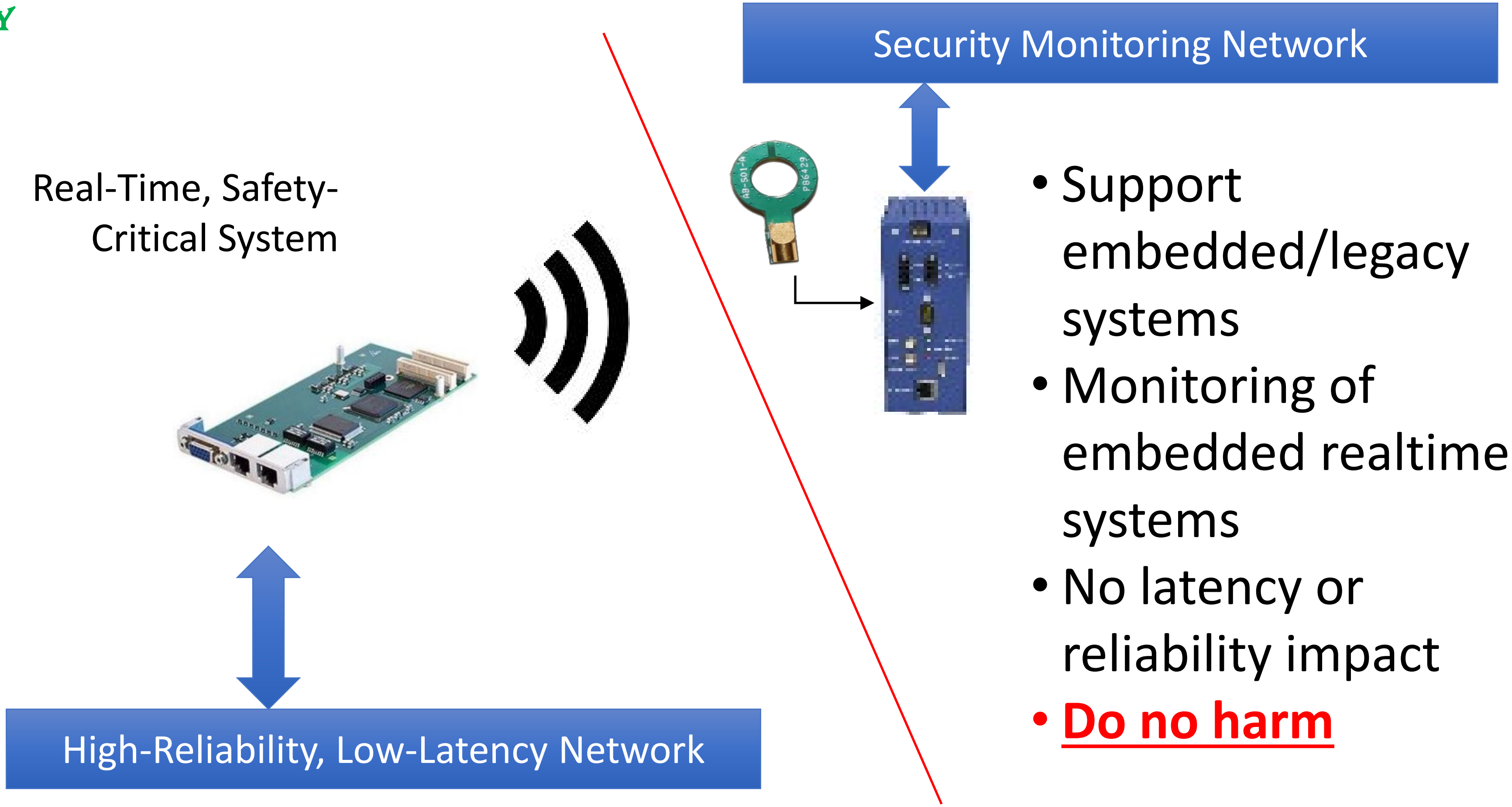
Third-party sensors

Raspberry Pi

In progress: M.2 form-factor monitor for rugged servers

arm

PFP Impact on Safety-Critical Systems


Security Monitoring Network
Real-Time, Safety-Critical System
High-Reliability, Low-Latency Network

- Support embedded/legacy systems
- Monitoring of embedded realtime systems
- No latency or reliability impact
- **Do no harm**

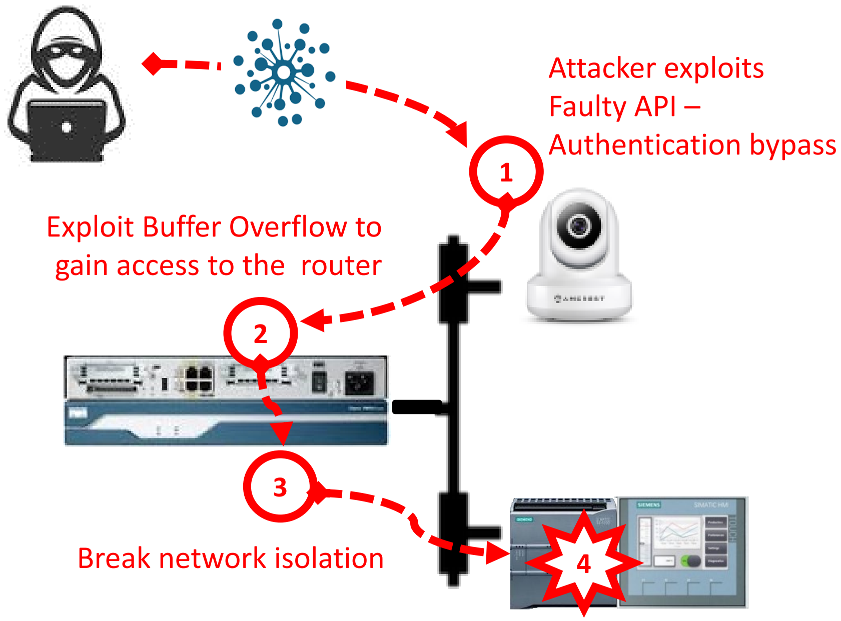
- No need for recertification
- Does not introduce additional vulnerabilities
- Immediate attack detection

PFP MOSAICS Fit

MOSAICS Solution Requirements	PFP Integrity Assessment Technology	
Cyber vulnerability baselining	Baseline execution/logic behavior of ICS devices based on physical unintended emissions and Machine Learning	✓
Enhanced asymmetric threat indications and warnings	Provide threat indicators about the integrity and operational status of ICS Devices being monitored	✓
Anomaly detection	Anomaly detection to detect deviations from the baseline e.g. malicious intrusions, etc.	✓
Information sharing capabilities within an automation framework	Scalable analytics framework to collect and aggregate PFP indicators and share with SIEMs	✓
Enables real-time response actions to disrupt attacker kill chains	Detect violations in machine time (milliseconds)	✓
Timely recovery to restore normal operations	Options for automated response and mitigation	✓
Degrade adversary re-use of attacks	Robust detection capabilities regardless of evasion measures implemented by attacks such as stealth and polymorphism	✓

Real-time Cyber Kill Chain Tracking in Critical Infrastructure

- Simultaneously monitor multiple devices in a critical infrastructure setup and detect attacks in real time to track adversaries’ lateral movement.

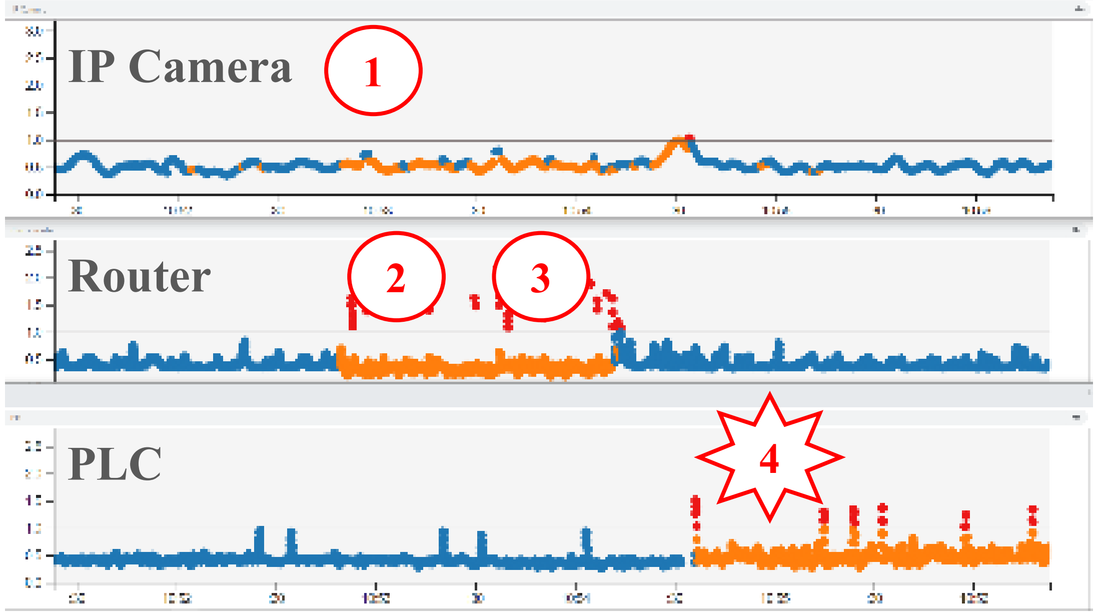


Attacker exploits Faulty API – Authentication bypass

Exploit Buffer Overflow to gain access to the router

Break network isolation

Modify PLC logic, which also spoofs the HMI



PFP Real-time detection results: Independent PFP monitors detect the individual intrusions and track adversary’s lateral movements

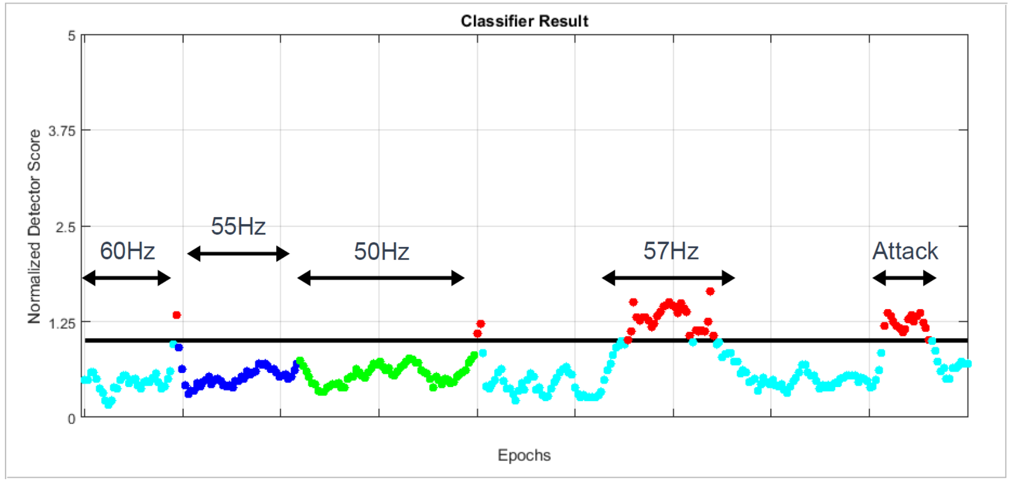
MOSAICS
2020 INDUSTRY DAY

OT Evaluation Testbed: Analog Attacks

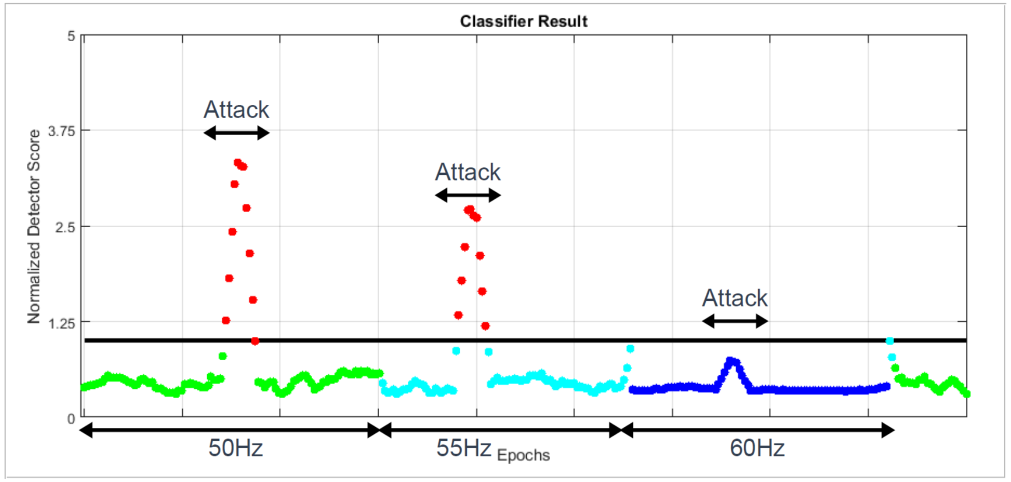
PFP CYBERSECURITY

- Evaluation setup: multiple attacks on Variable Frequency Drive (VFD)
  - Evaluation performed completely by 3rd party

Attack: Rapid Speed Change



Attack: Rapid Switching frequency Change



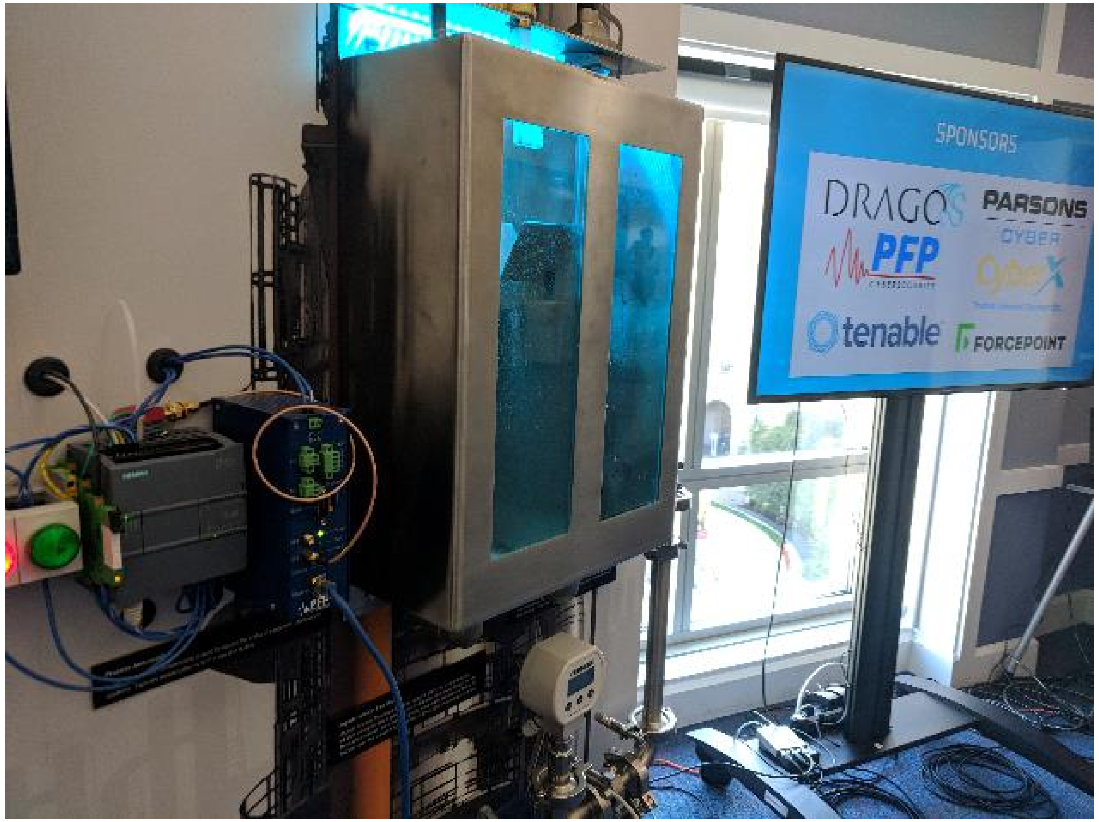
MOSAICS

2020 INDUSTRY DAY

DefCon ICS Village: CTF Monitoring

PFP CYBERSECURITY

DefCon ICS Village: CTF Monitoring

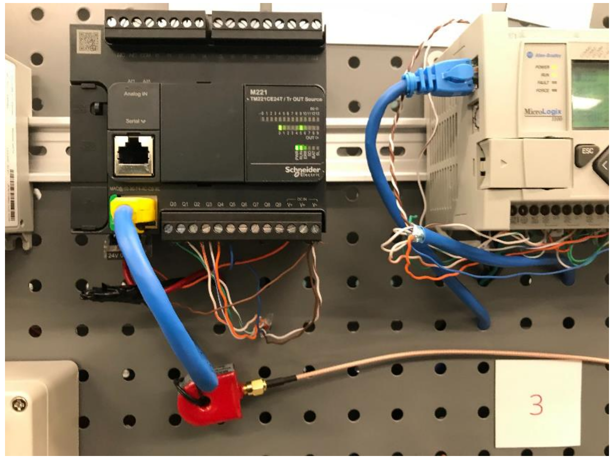


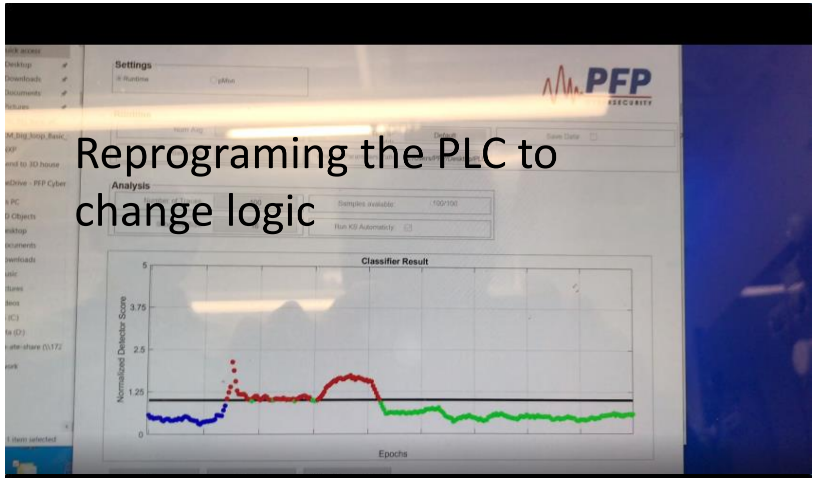
MOSAICS
2020
INDUSTRY
DAY

DreamPort DreamValley RPE: Traffic Controller Real-Time Attack Detection

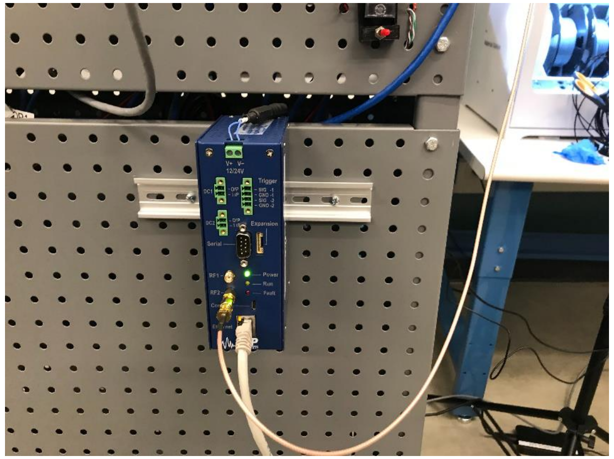
PFP CYBERSECURITY

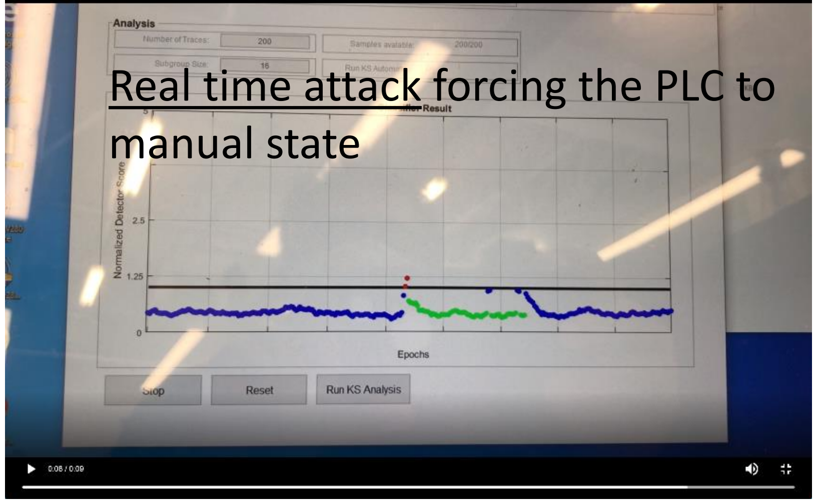
- Defense (BLUE) vs Offense (RED)
- IT and OT solutions to monitor DreamValley infrastructure
- Red Team conduct a coordinated assault against the city





Reprograming the PLC to change logic

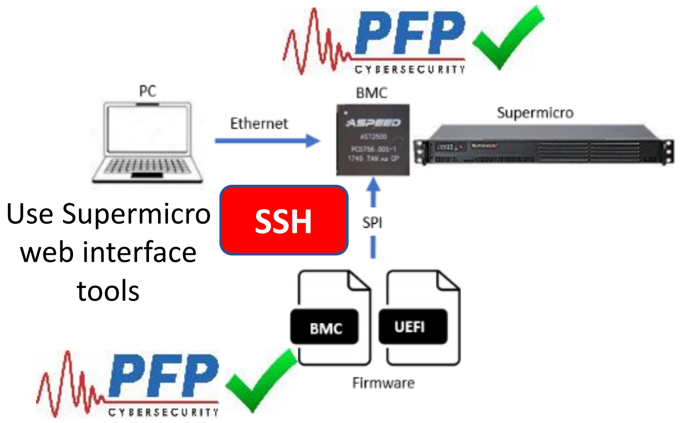




Real time attack forcing the PLC to manual state

Evaluation BMC Attack

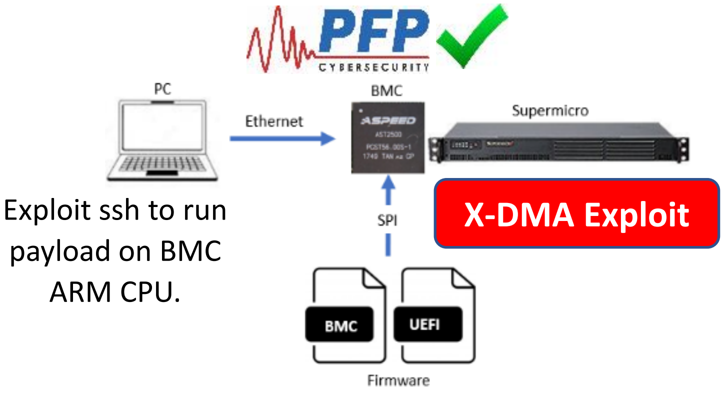
- A sample BMC exploit will attack in three steps, the first is loading a modified firmware, use X-DMA to inject shellcode in CPU kernel, then install backdoor



Use Supermicro web interface tools

Step 1: Modifies BMC firmware

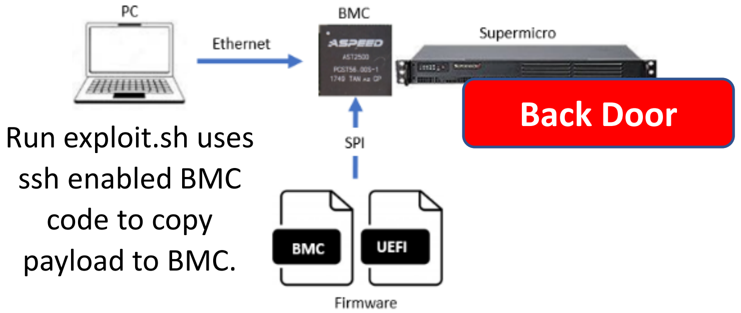
- Modifies BMC firmware to enable ssh
  - This process is done on a Local PC
  - Enable ssh then copy over the Backdoor exploit
- The modified BMC code is updated on the BMC using Supermicro web interface tools on the Local PC



Exploit ssh to run payload on BMC ARM CPU.

Step 2: Run exploit script on Local PC

- PFP runs exploit.sh on Local PC
- Exploit.sh copies payload from the Local PC to BMC (using ssh) and executes the payload on the BMC.
- Payload uses X-DMA to inject shellcode into the kernel code



Run exploit.sh uses ssh enabled BMC code to copy payload to BMC.

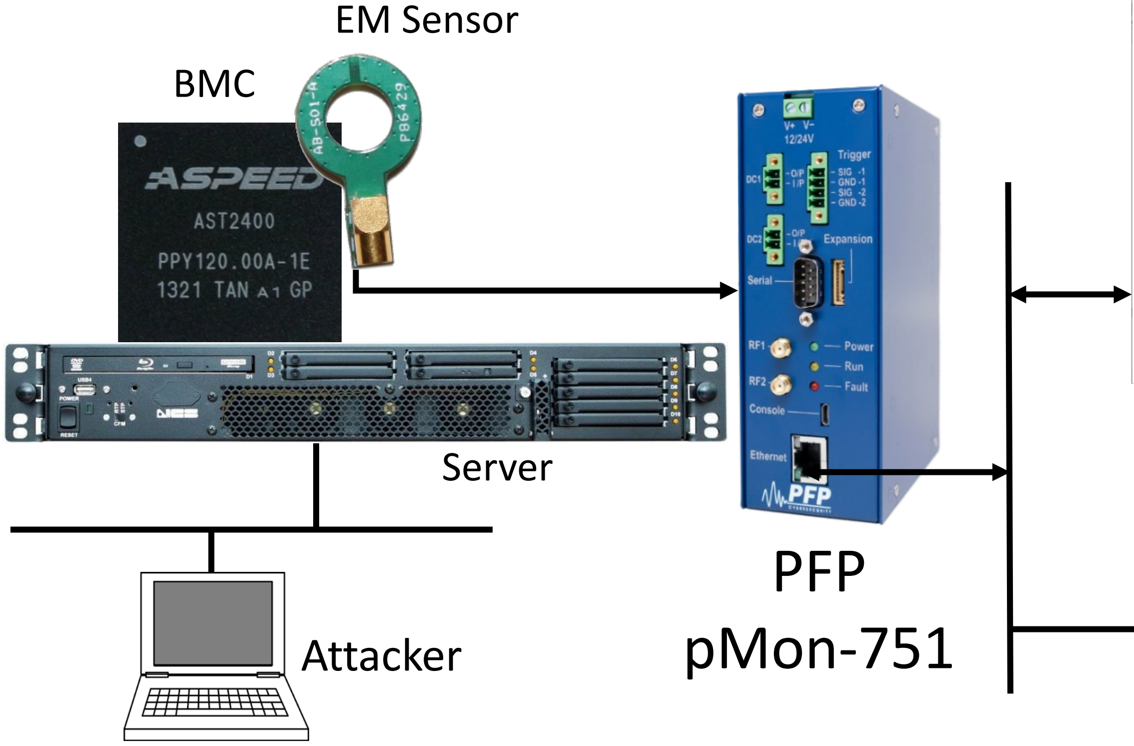
Step 3: Install Backdoor

- Kernel shellcode runs Python with a backdoor command
- Python backdoor connects back to the attacker, providing a shell

BMC exploit in Data Center Server

MOSAICS 2020 INDUSTRY DAY

- Detect Supermicro X10 BMC attack: Load a modified firmware, use X-DMA exploit to inject shellcode in CPU kernel, install backdoor.



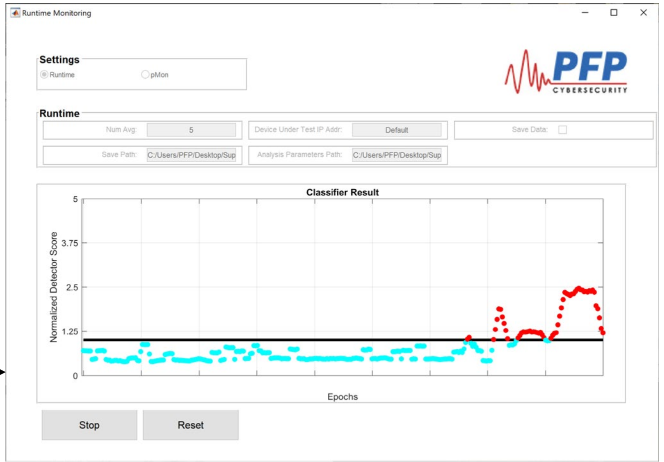
EM Sensor

BMC

Server

Attacker

PFP
pMon-751



Runtime Monitoring

Settings

● Runtime ○ pMon

Runtime

Num Avg: 5

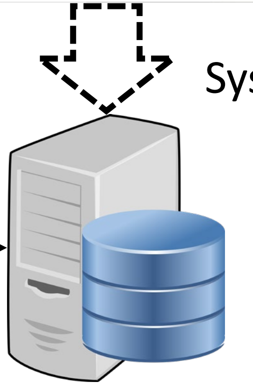
Device Under Test IP Addr: Default

Save Data: □

Save Path: C:/Users/PFP/Desktop/Sup

Analysis Parameters Path: C:/Users/PFP/Desktop/Sup

PFP P2Scan
/P3Scan



Syslog Notifications

Syslog
Server

©2020 Power Fingerprinting Inc.

PFP
CYBERSECURITY

Questions?

Carlos R. Aguayo Gonzalez
caguayog@pfpcyber.com