Protecting 5G Systems Using Side-Channel Information

NSF Workshop on Next-G Security

Oct 15th, 2020

PFP CYBERSECURITY

VT | WIRELESS @ VIRGINIA TECH

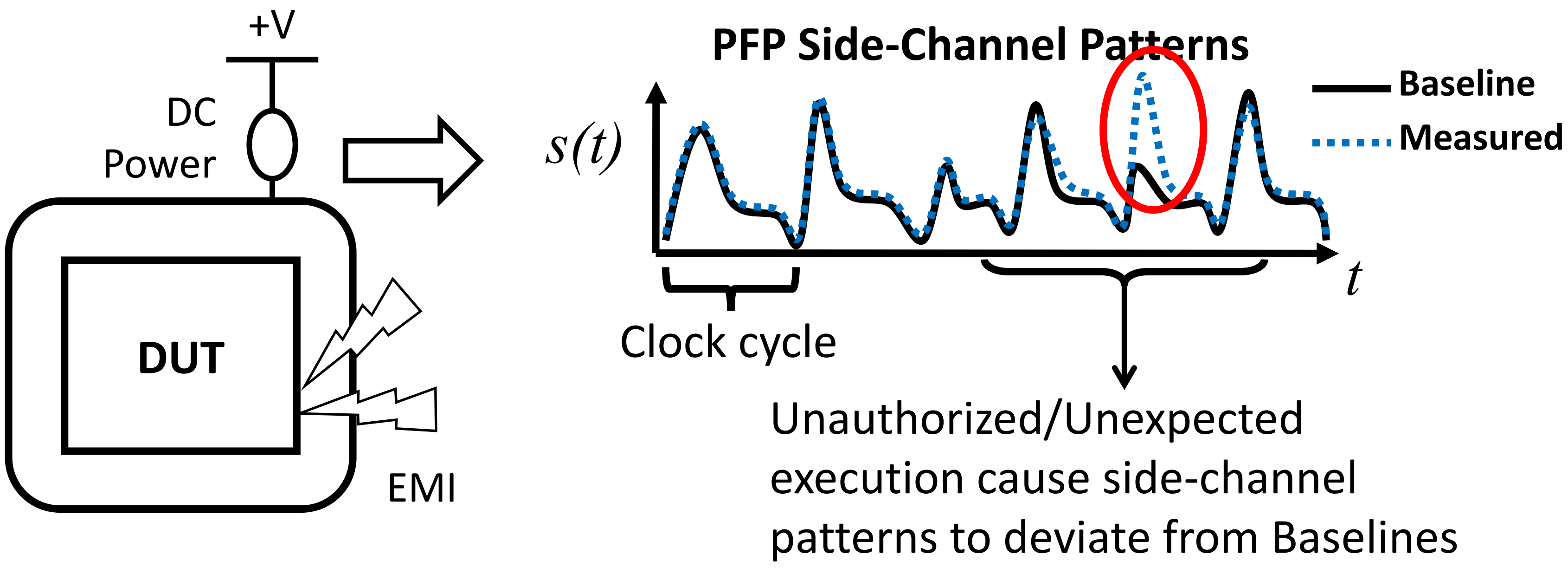
Some Background Info.

- PFP Cybersecurity is a spin-off of Wireless@VT
- Use side channels (e.g., power, EM, heat, …) to validate hardware and software.
- Started from research in validating software to a hardware radio platform
- All systems (small or large) use power and malware or Trojans can't escape from using power.
- Initial seed funding though NSF SBIR and STTR Program, Phase I and Phase II.
- **Biggest hurdle – think non-traditional physical cybersecurity to those in the field.**

THANK YOU NSF !

General Approach

- Signal detection/classification/anomaly detection of analog signals (side-channels).
  - Baseline characterization from “gold product” or crowd-sourcing
- New application is for malware and hardware Trojan detection (supply chain).



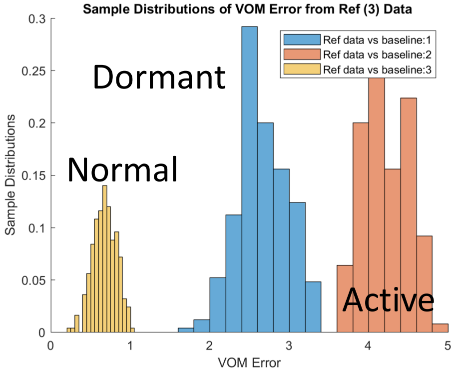
PFP Zero Trust Monitoring: Supply Chain Screening and Cyber Kill Chain Disruption

Supply Chain Screening

- Detect counterfeit/banned hardware and firmware tampering

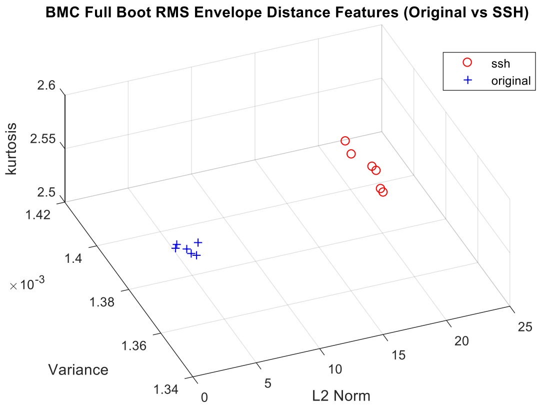
Operational Monitoring

- Detect stealth attacks in machine time and disrupt the attack cyber kill chain



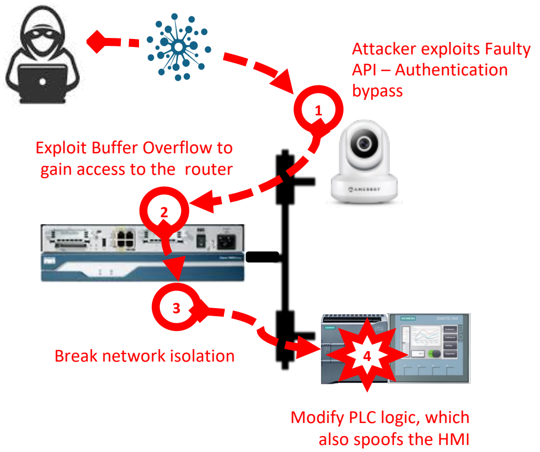
HW Trojan Detection in Xilinx FPGA

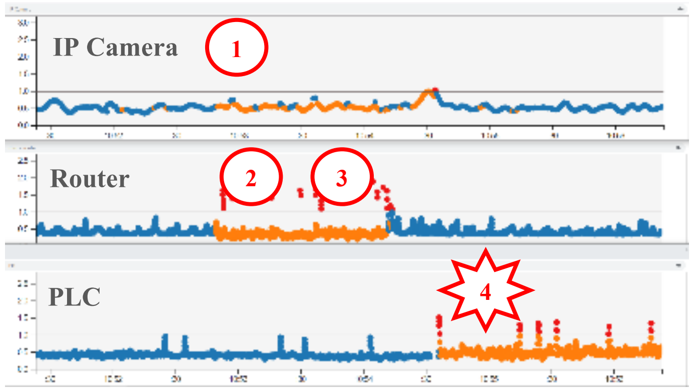
- DC Current Sensor and Keysight Digitizer
- Time/Frequency Feature Extraction
- Bayes Classifier



Server BMC Firmware Tamper Detection

- Loading additional modules at boot
- EM Sensor and pMon 751
- Envelope Analysis and HOS features



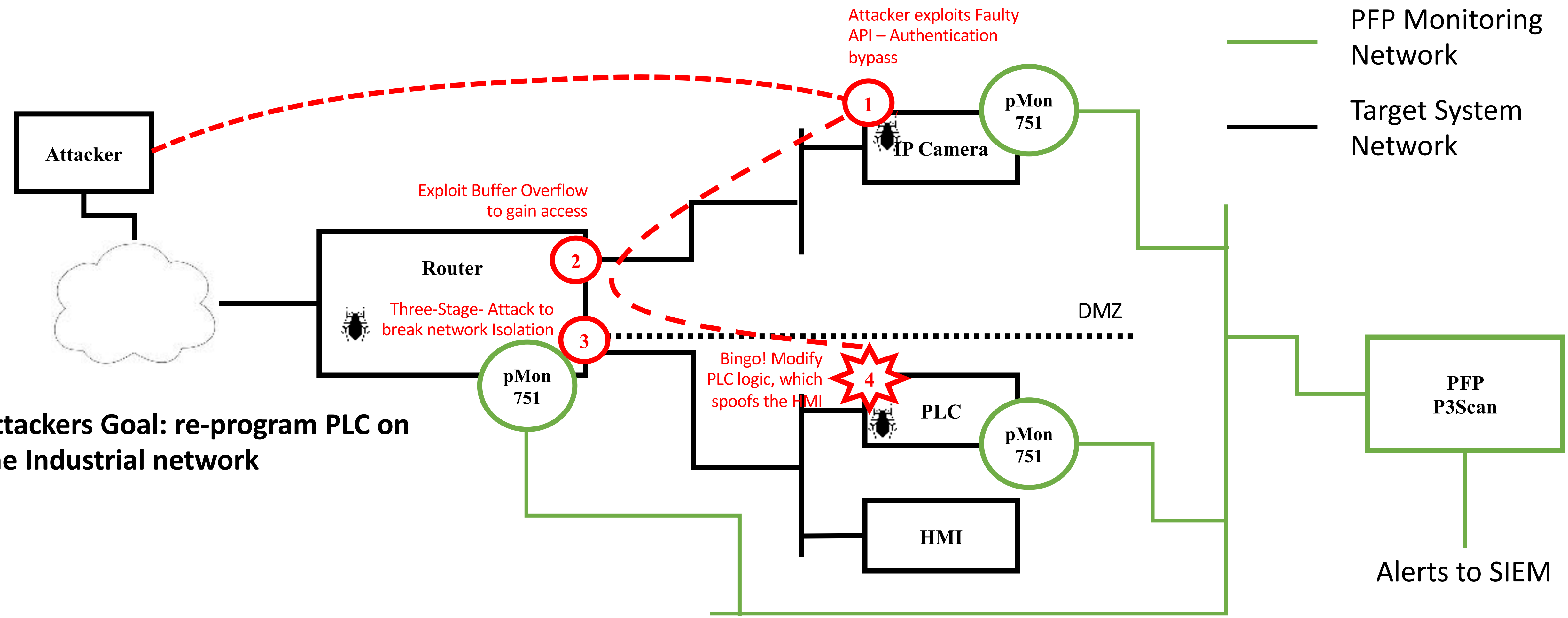


PFP Real-time detection results: Independent PFP monitors detect the individual intrusions and track adversary's lateral movements

Intrusion Detection & Adversary Lateral Movements Tracking

- Adversary moves from one target to the next
- Each device being monitored real-time by PFP (EM and DC)

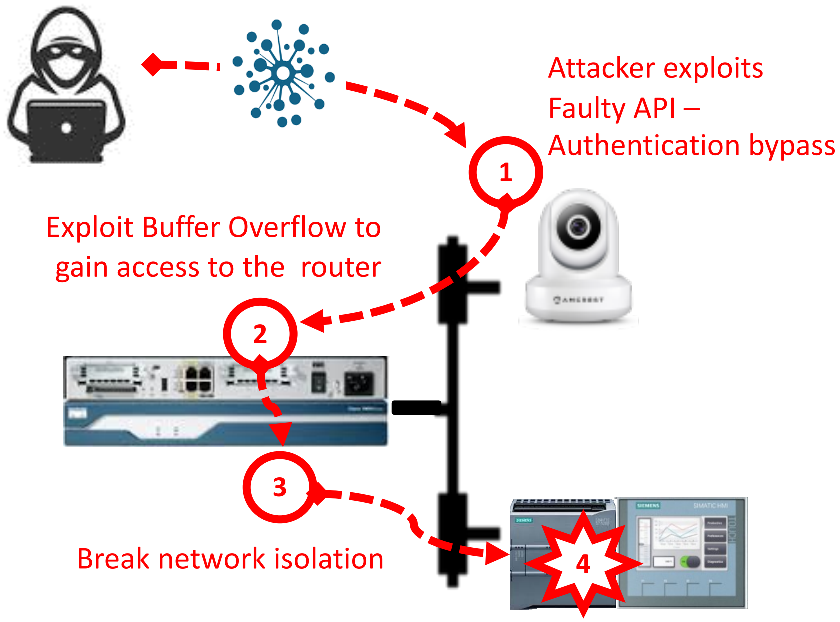
Cyber Kill Chain/Lateral Movement Attack Description

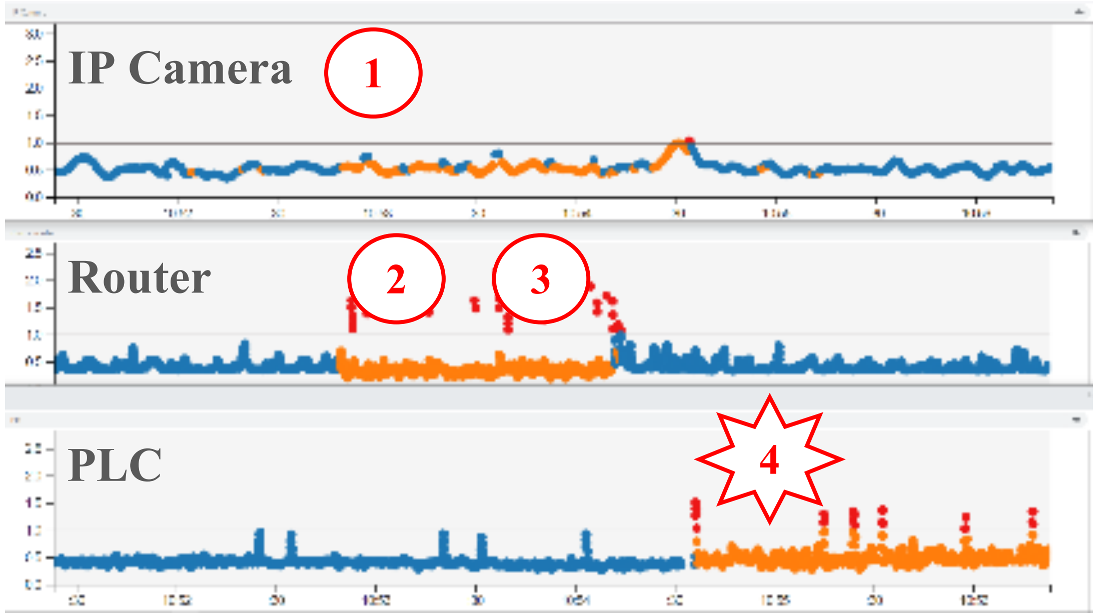


Attackers Goal: re-program PLC on the Industrial network

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.





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

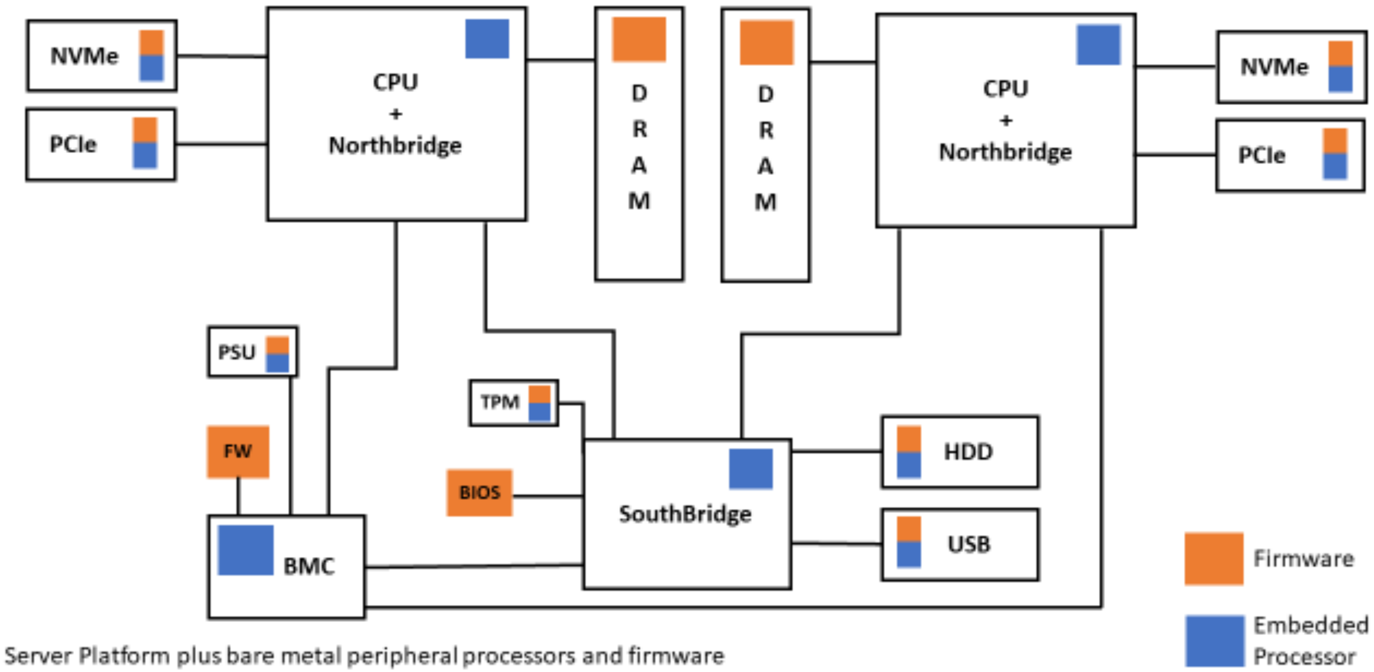
General thoughts

- Some tough problems.
  - Security for low power and cheap IoT devices.
  - Physical layer disruption for mission critical systems.
  - Knowing the integrity of the hardware/software.
  - Recognizing zero-day attacks
  - Insuring integrity of the encryption.
  - Certificate management.
- 6G will be AI centric
  - Starts with 5G, but outsanding issues.
  - Assuring integrity of AI – lots of issues with security and validation.
- We need to “think out of the box”

Backup Slides

Supermicro Server Attack: Exploiting BMC to Install Backdoor

Broad Attack Surface in a Server – Bare Metal



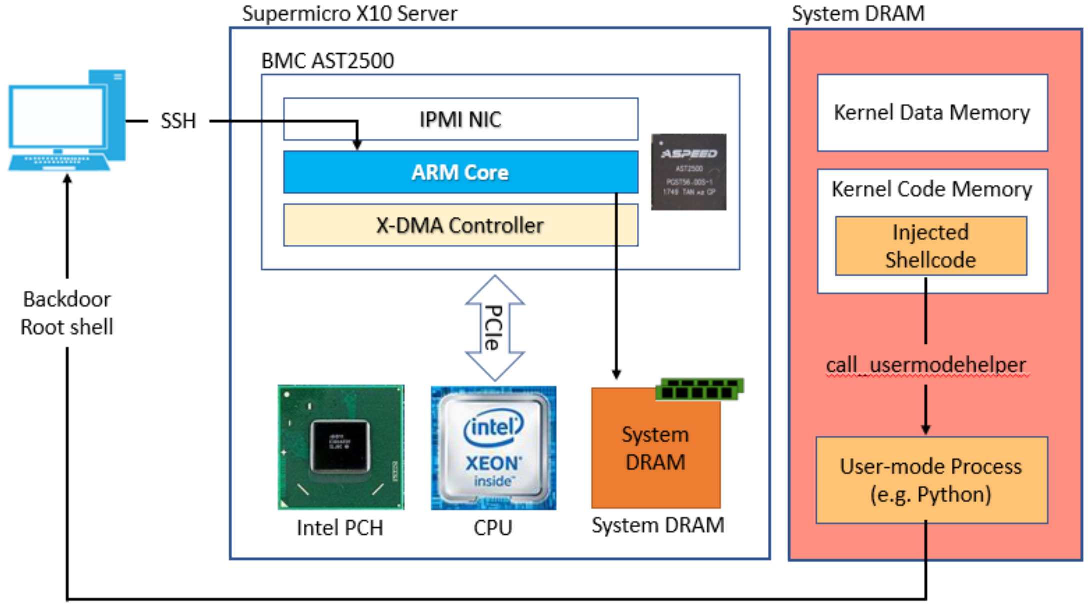
Server Platform plus bare metal peripheral processors and firmware

- Adversaries target much more than CPUs
- Several bare metal components difficult to protect
- Hidden memory/processors can be used to launch attacks on the main CPU or Exfiltrate information as covert channels

Evaluation Attack on Supermicro X10 Motherboard -> used in SWFTS TI20

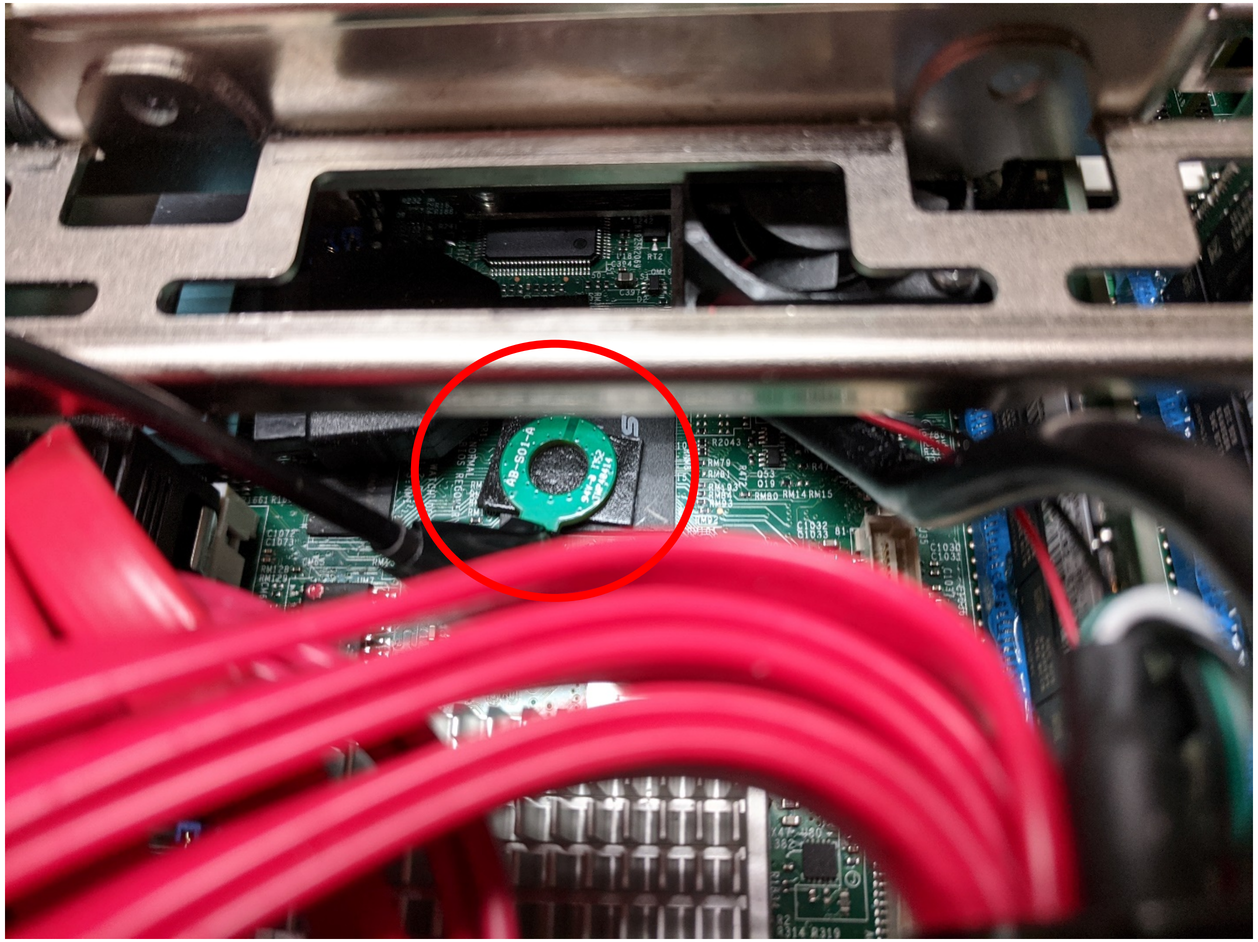
Step by step attack break down:

- Attacker modifies BMC firmware to enable ssh
- Attacker accesses BMC over SSH using IPMI network with admin credentials
- Attacker exploits SSH service to run payload on BMC ARM core
- Payload uses X-DMA to find kernel code memory
- Payload uses X-DMA to inject shellcode into the kernel code
- Kernel shellcode runs Python with a backdoor command
- Python backdoor connects back to the attacker, providing a shell

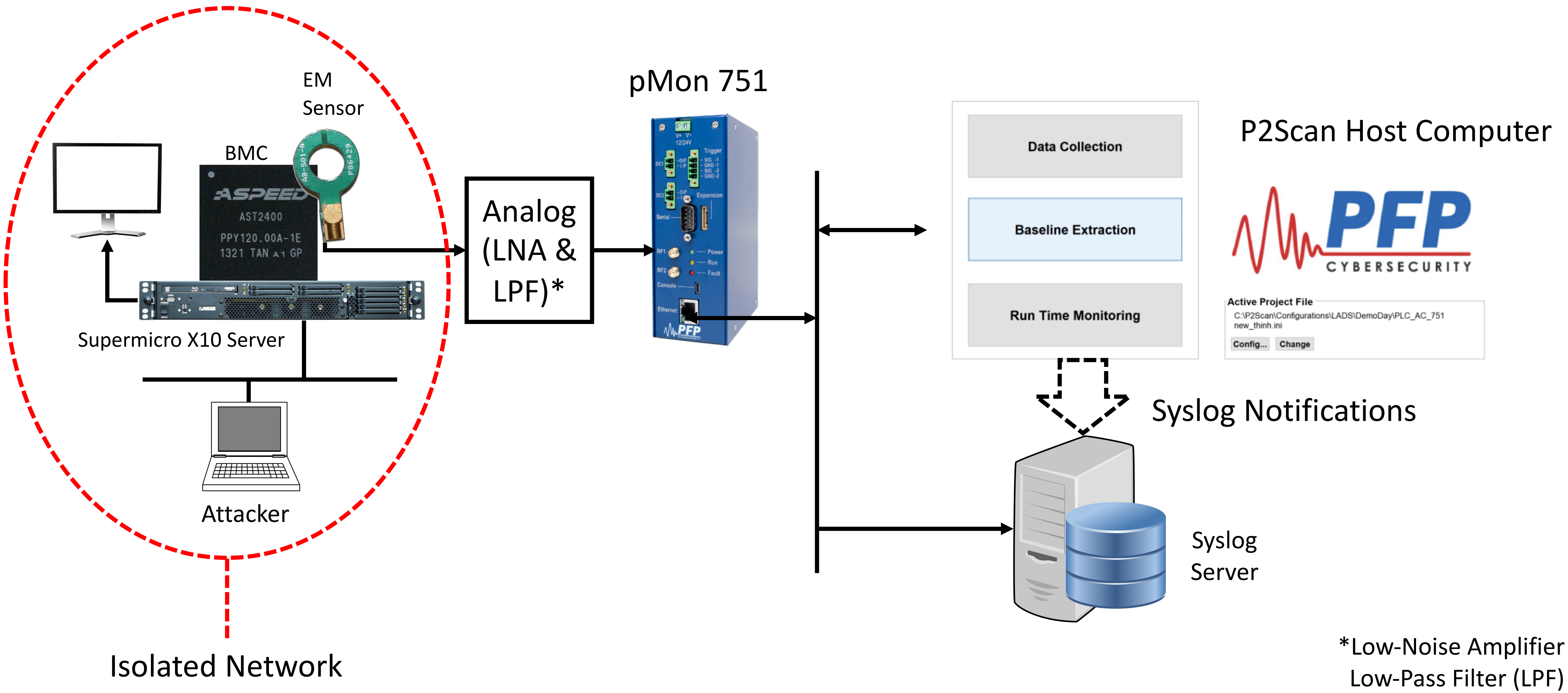


IPMI NIC -> BMC CPU -> PCIe bus -> CPU

Instrumenting Server BMC with EM Probe



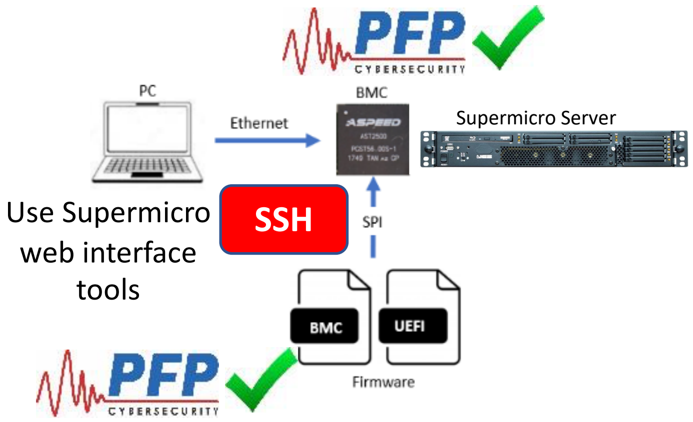
Complete Demo Block Diagram

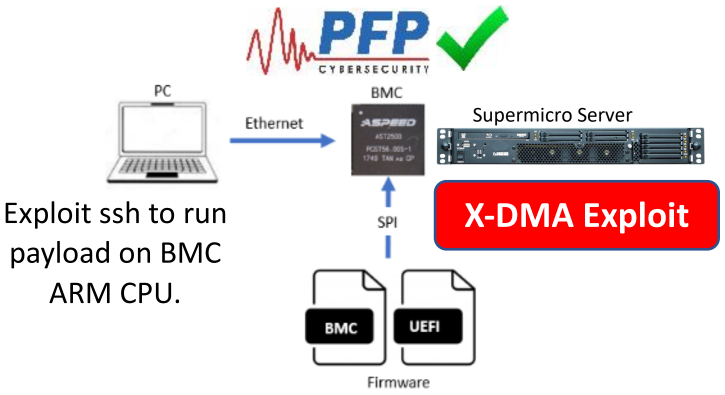


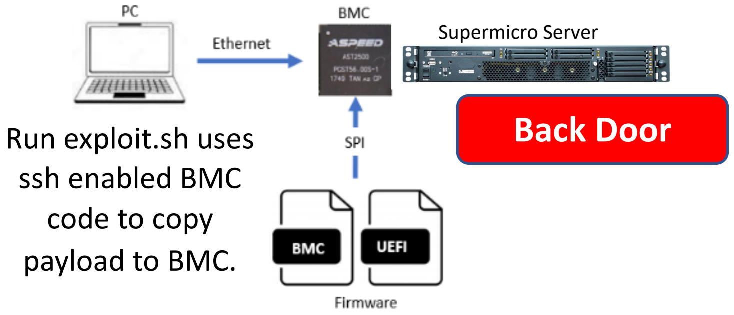
*Low-Noise Amplifier (LNA)
Low-Pass Filter (LPF)

BMC Attack Description

BMC attack's three steps: 1) load a modified firmware, 2) use X-DMA to inject shellcode in CPU kernel, 3) install backdoor







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

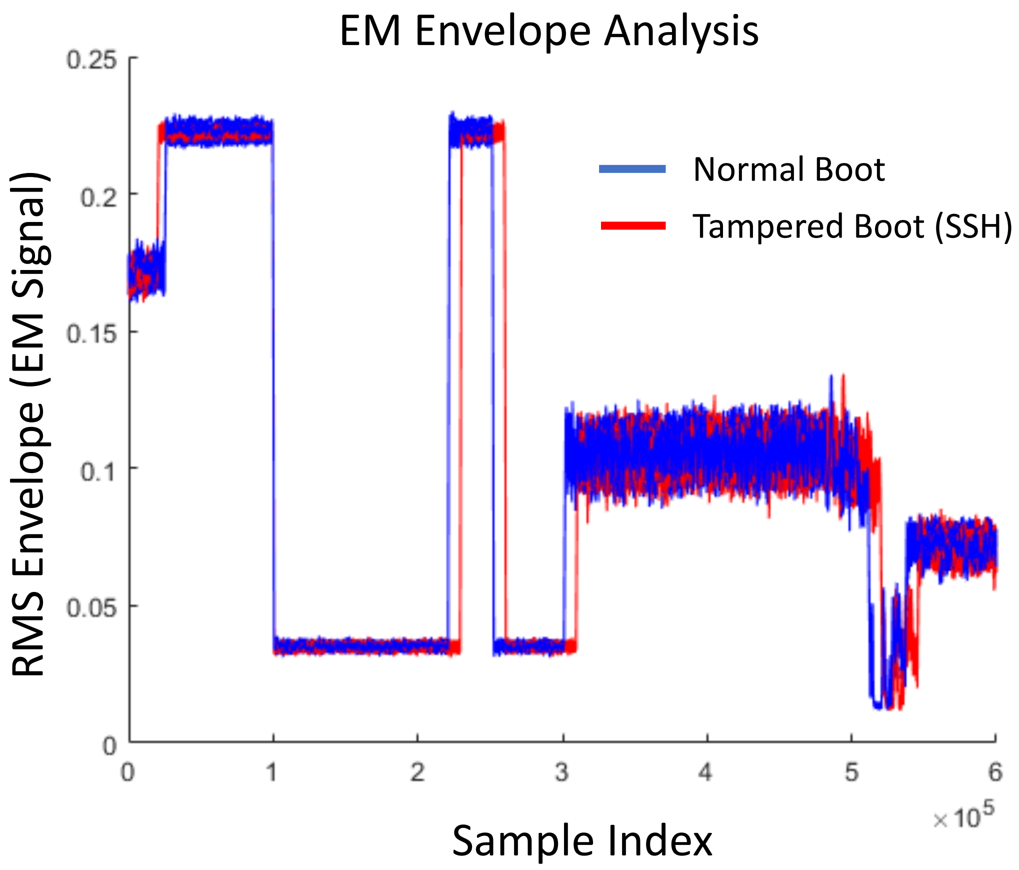
Step 2: Run exploit script on Local PC

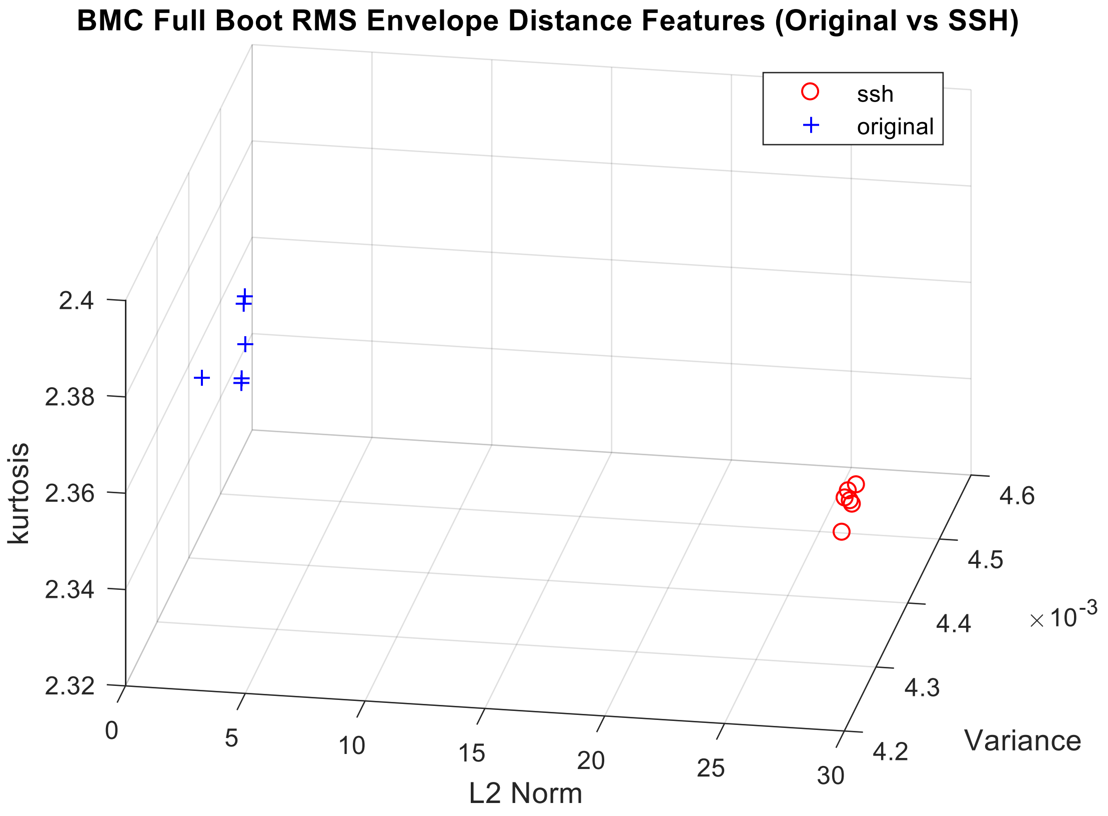
- PFP runs exploit.sh on Local PC
- Exploit.sh copies payload from the Local PC to BMC (using ssh) and executes the payload on the BMC.
- Payload uses X-DMA to inject shellcode into the kernel code

Step 3: Install Backdoor

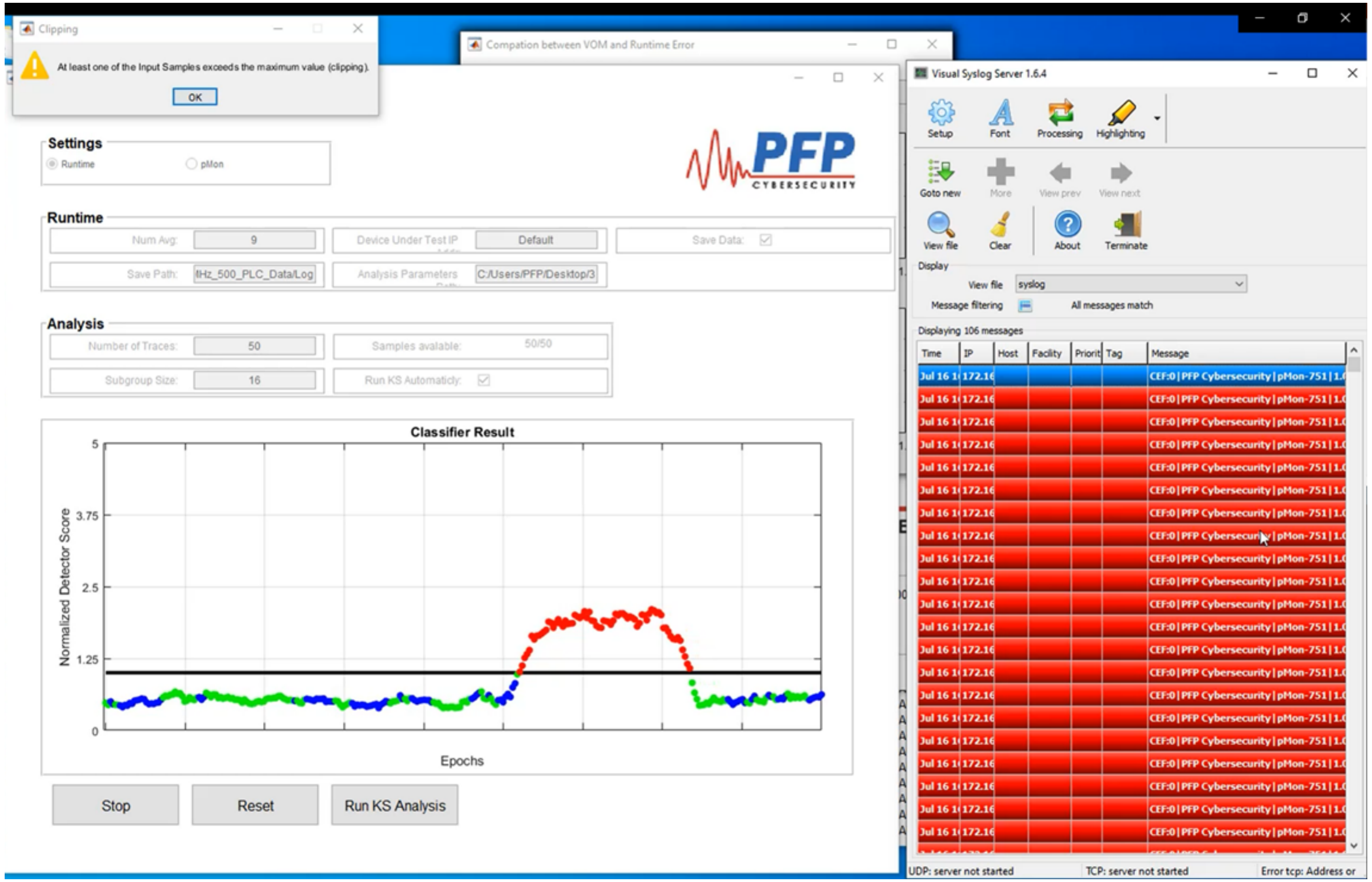
- Kernel shellcode runs Python with a backdoor command
- Python backdoor connects back to the attacker, providing a shell

BMC Attack 1st Stage Detection: Firmware Implant



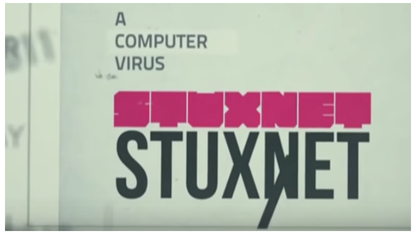


BMC Attack 2nd Stage Detection: X-DMA Exploit



Cybersecurity in 5G Mission-Critical Systems

- Traditional solutions are inadequate for emerging threats
  - Beyond desktops – control, weapons, and navigation systems are at risk,
- Untrusted supply chain – hardware/firmware tampering
  - Software only solutions cannot reliably detect HW tamper
- Zero-Trust requires independent assessment/verification for security



abc NEWS
Operation Cisco Raider,

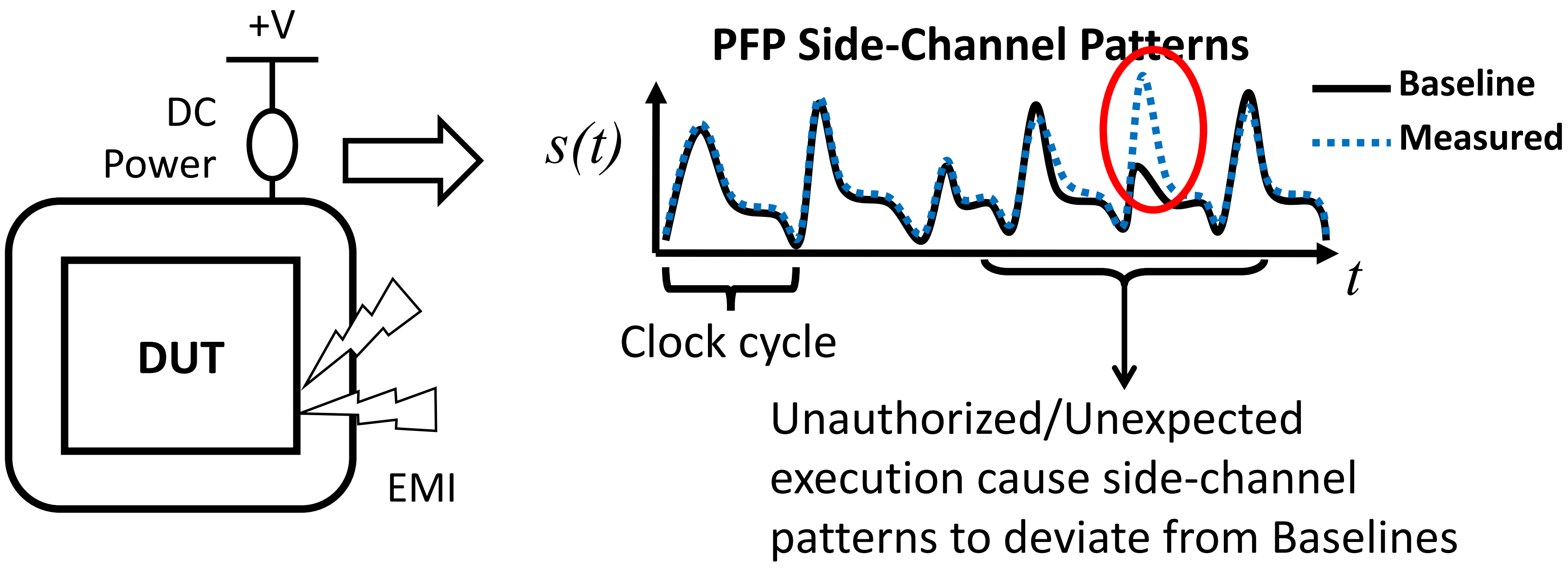
In total, authorities around the world, including in the United States, Canada and China, made more than 400 seizures with an estimated value of $76 million. In one instance, the Royal Canadian Mounted Police seized 1,600 pieces of counterfeit Cisco routers.

Aug 14, 2015

Cisco warning: Attackers hijacking networking hardware via malicious firmware

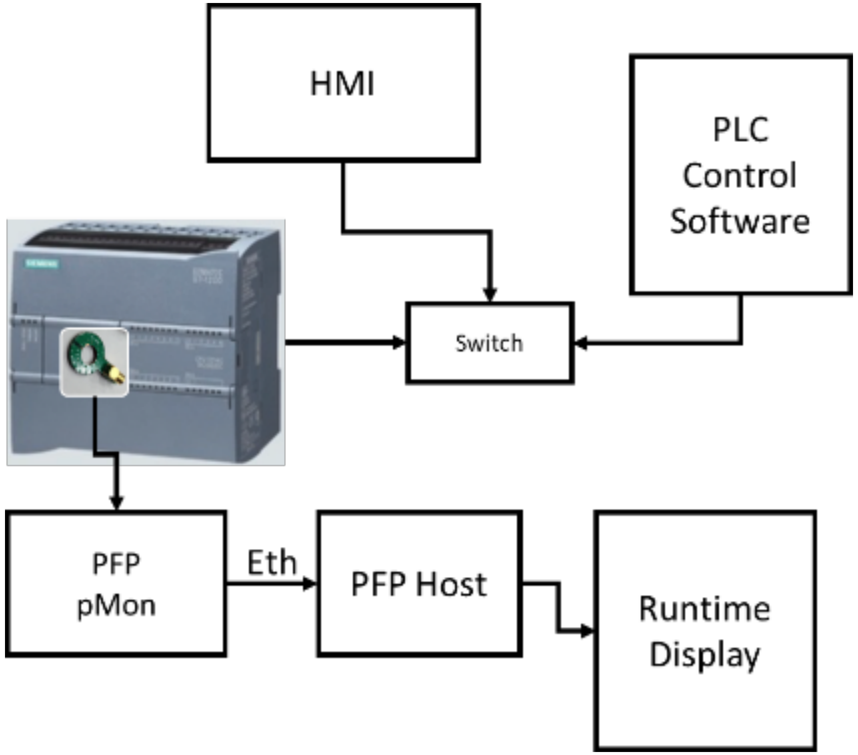
Unintended Emissions and Machine Learning: Independent Assessment and Zero Trust

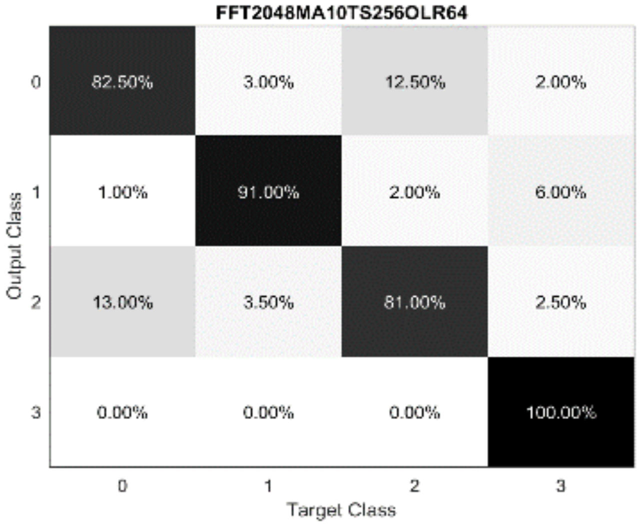
- Side channels, e.g. power behavior or electromagnetic emissions, used to perform nondestructive, unobtrusive evaluation of 5G systems to assess the integrity of hardware/firmware and detect tampering
- Support Zero Trust Architecture with independent monitoring

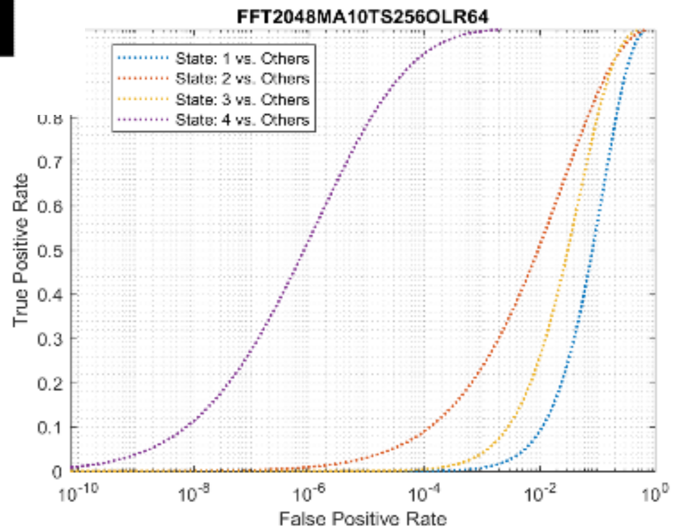


Other Examples

PLC Control Flow Tracking



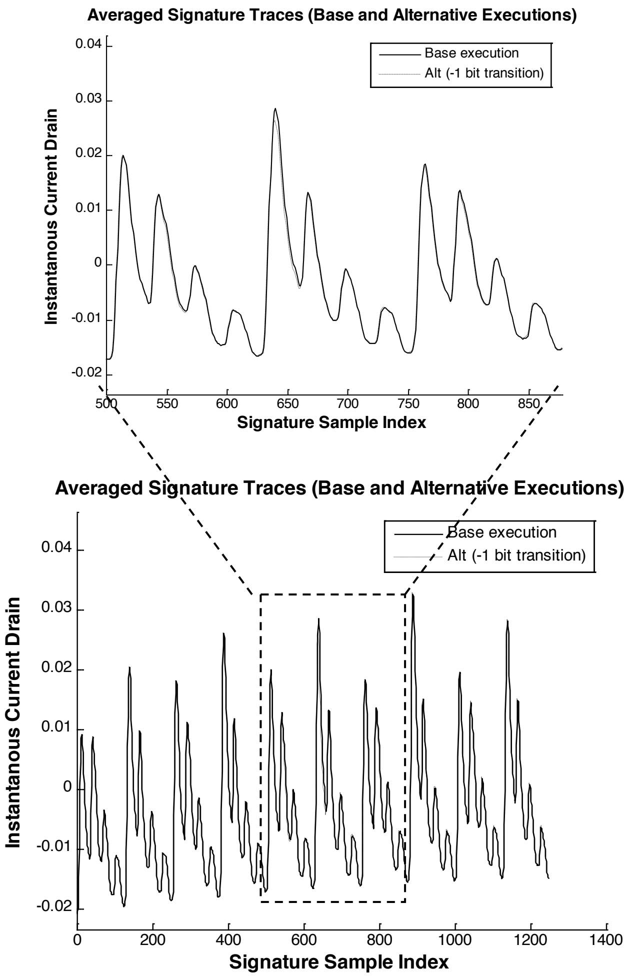


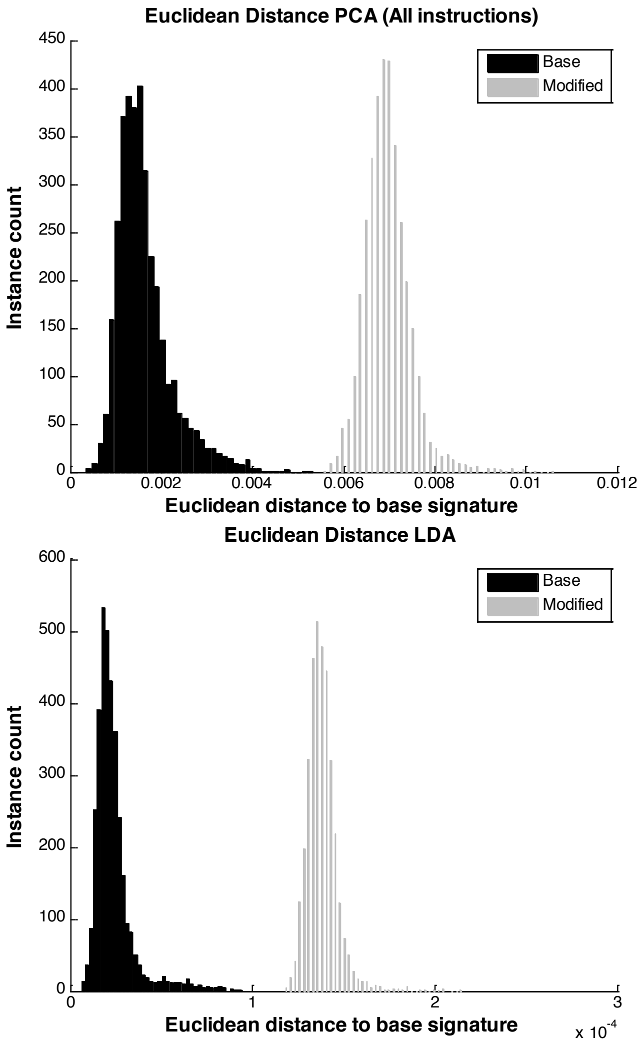


History: Minimum Sensitivity Evaluation

- Introduce the smallest possible execution deviation (one bit)

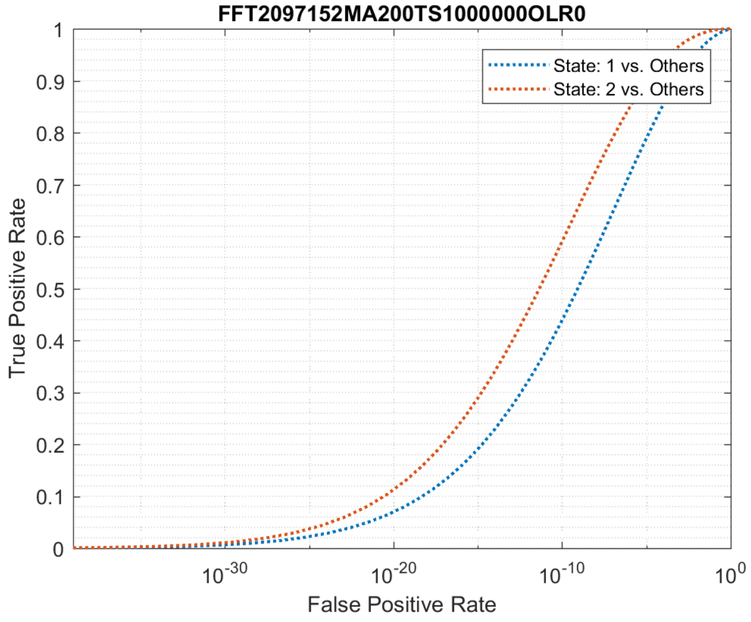
```
//Target code infinite loop
while(1){
    //Restart TIM0
    //Trigger
_asm
    nop
    iorwf   j, 0, 0   //w = 0f
    andlw   0x00      //w = 00
    movf    j, 0, 0   //w = 0f
    andlw   0x00      //w = 00
    movf    k, 0, 0   //Change k 1 bit
    movlw   0x00      //w = 00
    xorwf   j, 0, 0   //w = 0f
    movlw   0x00      //w = 00
    iorwf   j, 0, 0   //w = 0f
    xorlw   0x00      //w = 00
    nop
    ... x 10
    nop
_endasm
}
```

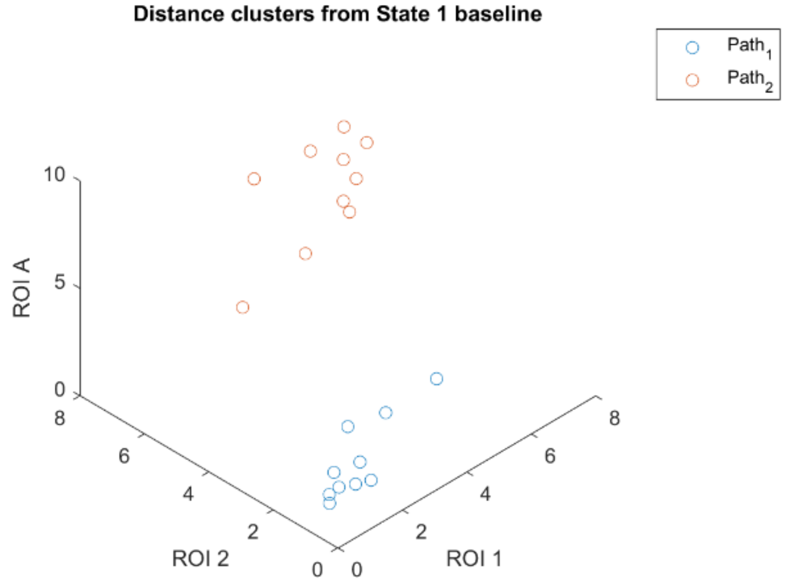


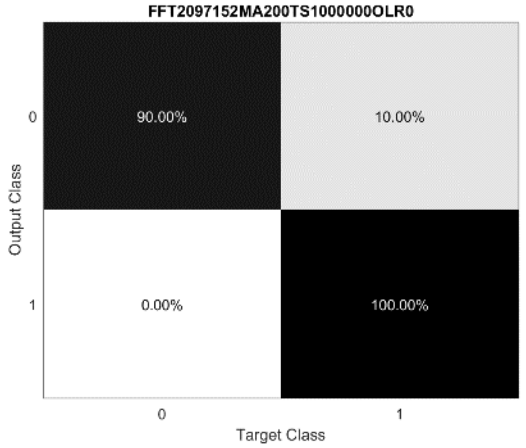


3rd Party Evaluation Samsung Galaxy S5

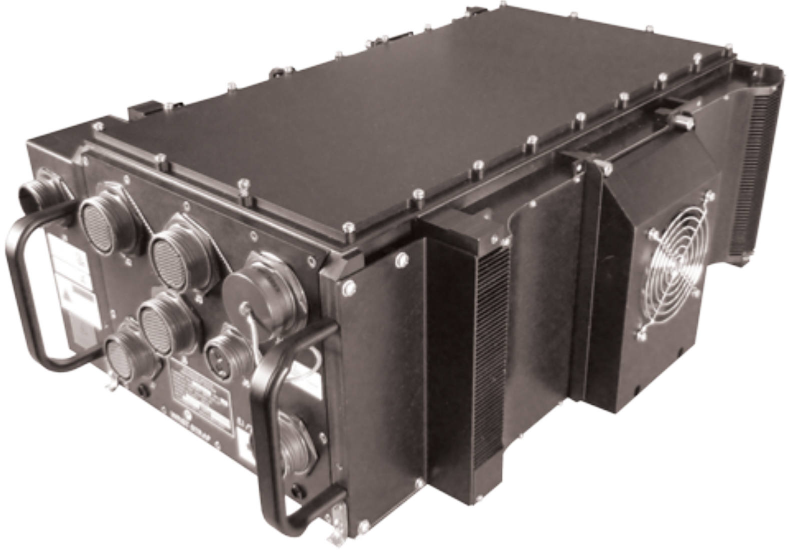
- Disabling App Signature Verifications

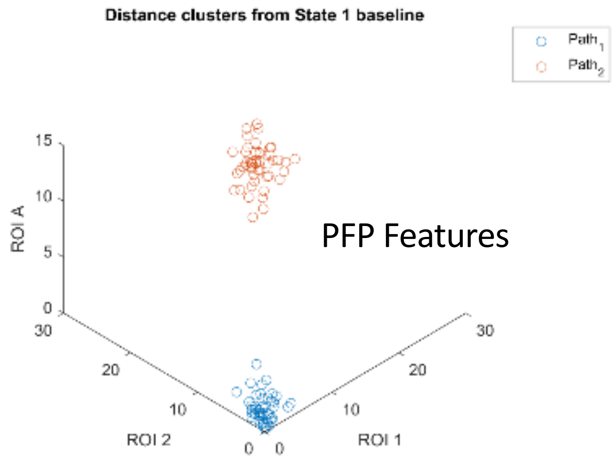


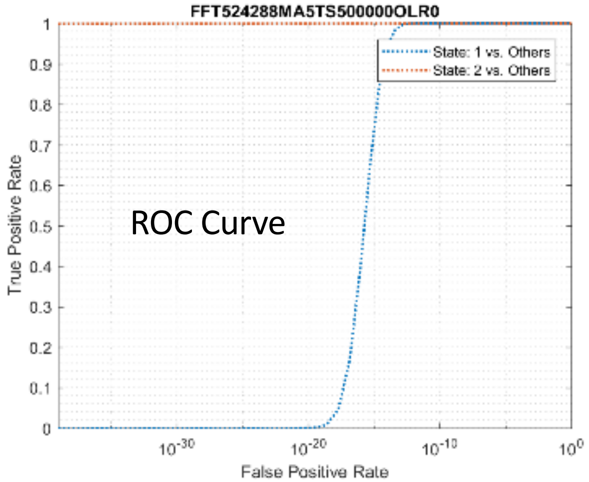


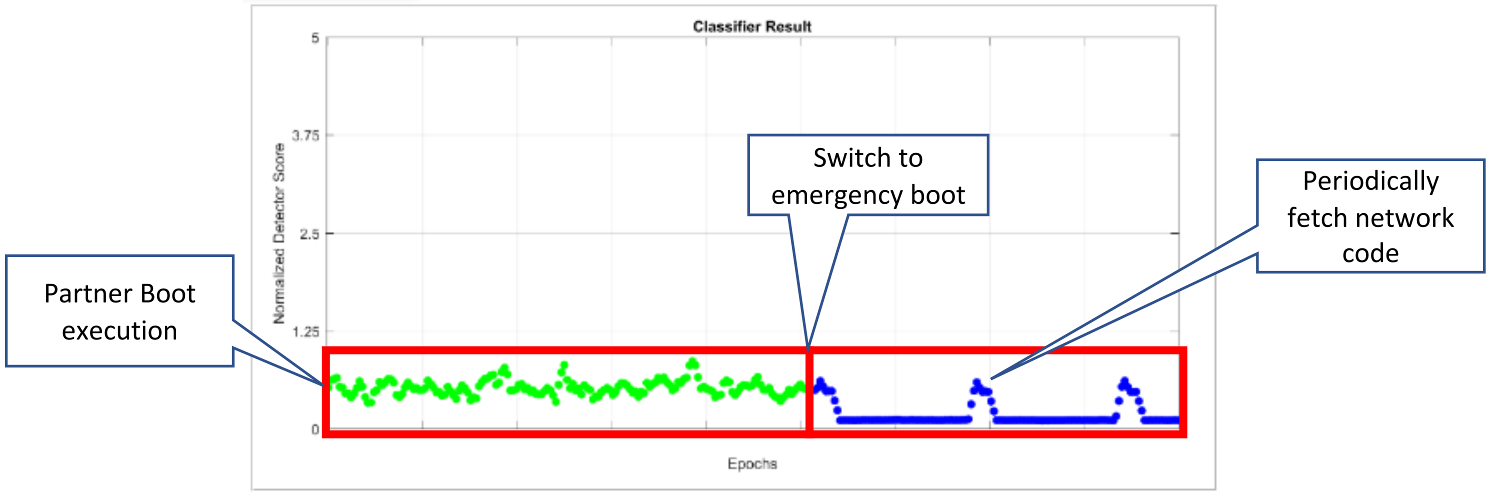


UAV Flight Computer 3rd Party Blind Evaluation



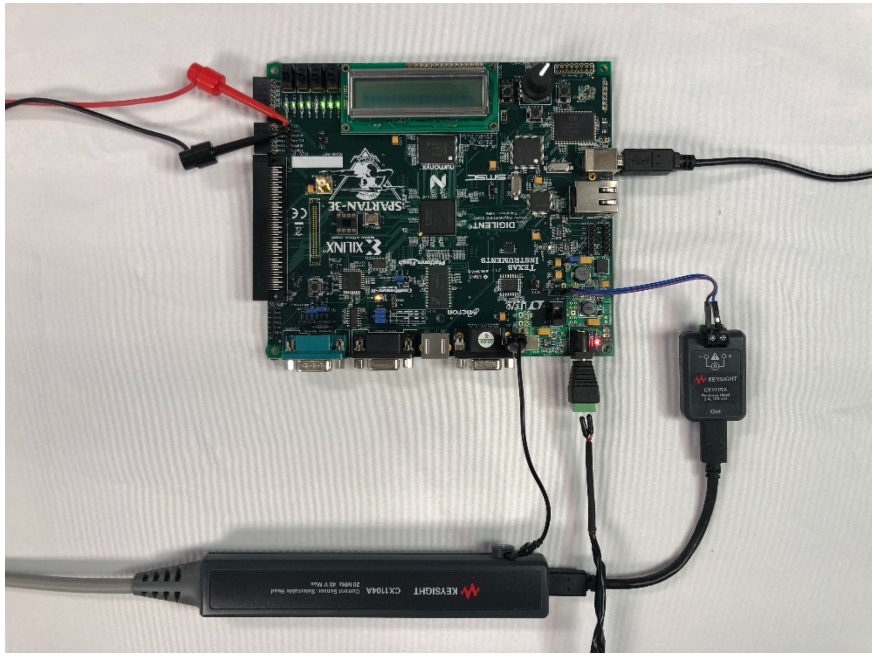






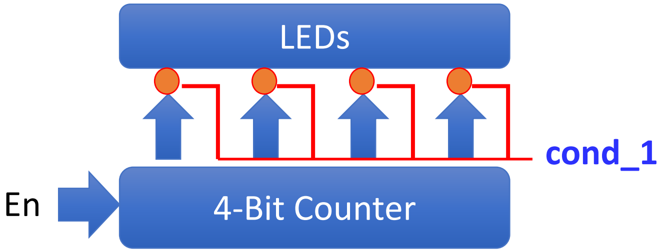
FPGA Hardware Trojan Detection Details

Target and Measurement Setup



Target: Xilinx Spartan 3e FPGA

Digitizer: Keysight CX3300



Tamper: Emulated backdoor

- Invert output only when cond_1 is true

PFP VOM HW Trojan Detection Results