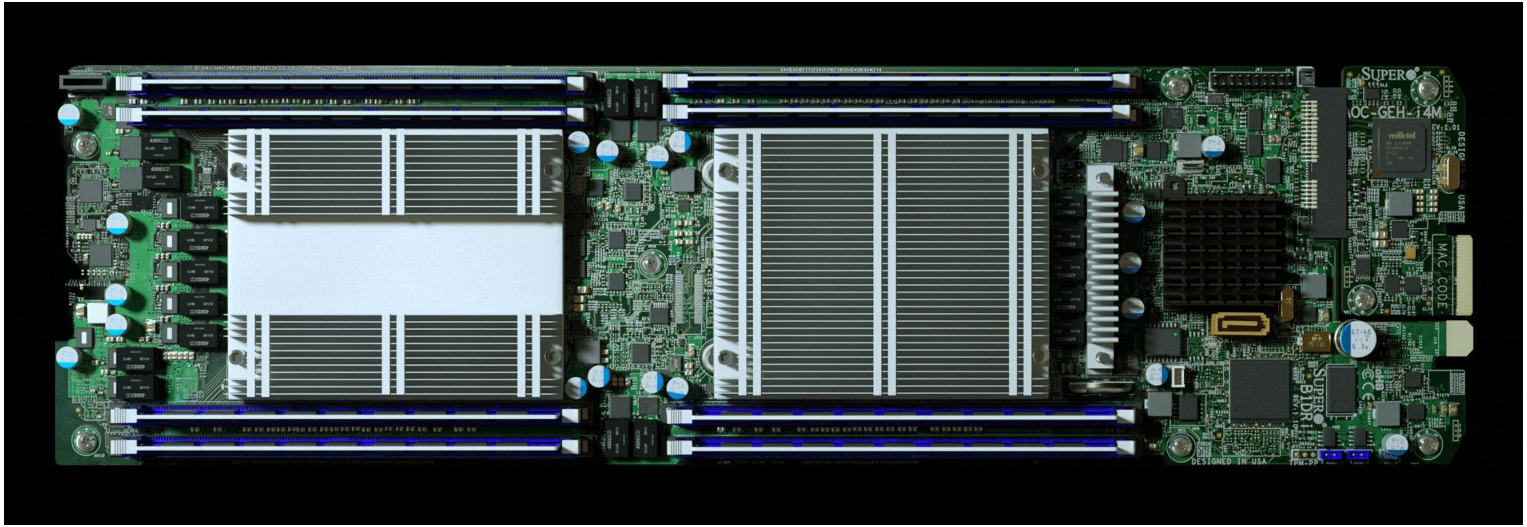
Supply Chain Protection & Verification Through EM Side-Channel Signature Analysis

Alenka Zajic

Georgia Institute of Technology

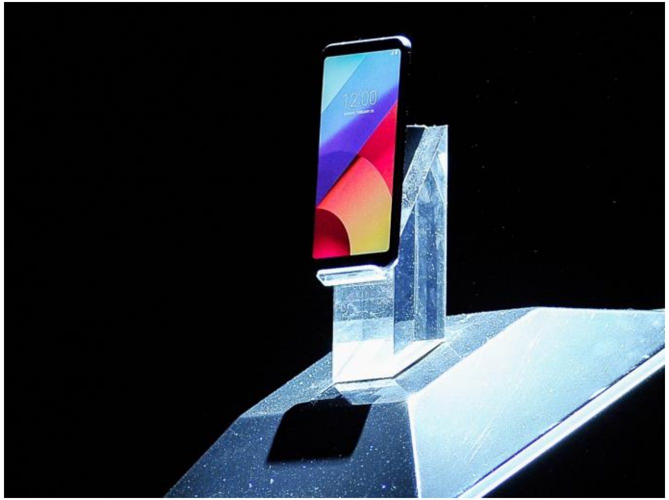
August 2020

The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies – Bloomberg Businessweek 2018



Millions of Android Devices Are Vulnerable Right Out of the Box

Firmware bugs introduced by manufacturers and carriers put Android smartphones at risk - WIRED 2018



The Untold Story of NotPetya, the Most Devastating Cyberattack in History

Crippled ports. Paralyzed corporations. Frozen government agencies. How a single piece of code crashed the world. – WIRED 2018

❖Side Channels

- A side channel is a means of obtaining information about software execution outside of the program’s intended communication
  - Is X a side channel?
  - Depends on what we consider “intended”
- Boils down to “you were not supposed to consider X as a source of information” (YWNS)

❖Categories of Side Channels

- Timing
  - YWNS performance
- Cache, BPred, etc.
  - YWNS microarchitecture
- Power, EM, acoustics, etc.
  - YWNS physical (analog) aspects of the implementation
- Bus snooping, DRAM-freezing, etc.
  - YWNS open the computer!

❖TEMPEST: A Signal Problem

- Bell Labs discovered first wireless side-channel in 1943.

- Cryptography community is concerned about this problem because private-public key encryption can be broken via side-channels.

- Focus on simple hardware such as microcontrollers

❖EM Emanations From Computer Systems

- EM emanations from modern systems (laptops, desktops, cellphones, IoT) exist
  - Can they leak any “interesting” information? (yes)
  - From how far away can they be received? (several meters)

[1] A. Zajic and M. Prvulovic, “Experimental demonstration of electromagnetic information leakage from modern processor-memory systems,” *IEEE Transactions on Electromagnetic Compatibility*, vol. 56, no. 4, pp. 885-893, August 2014.

[2] D. Genkin, I. Pipman, and E. Tromer, “Get Your Hands Off My Laptop: Physical Side-Channel Key-Extraction Attacks on PCs,” in Proc. Crypto. HW and Emb. Sys. (CHES), 2014.

[3] D. Genkin, L. Pachmanov, I. Pipman, and E. Tromer, “Stealing Keys from PCs using a Radio: Cheap Electromagnetic Attacks on Windowed Exponentiation,” in Proc. Crypto. HW and Emb. Sys. (CHES), 2015.

[4] Mordechai Guri, Assaf Kachlon, Ofer Hasson, Gabi Kedma, Yisroel Mirsky, and Yuval Elovici, “GSMem: Data Exfiltration from Air-Gapped Computers over GSM Frequencies,” Usenix Security Symposium 2015.

[6] R. Callan, A. Zajic, and M. Prvulovic, “FASE: Finding Amplitude-modulated side-channel emanations *Proceedings of the 42nd International Symposium on Computer Architecture (ISCA)*, pp. 592-603, June 2015.

[7] R. Callan, A. Zajic, and M. Prvulovic, “A practical methodology for measuring the side-channel signal available to the attacker for instruction level events,” *IEEE MICRO 14*, pp.1-12, Cambridge, UK, December 2014.

Pre-Deployment Verification

Continuous Verification

RFB-Based IC Verification and RF Anomaly RFIC Verification

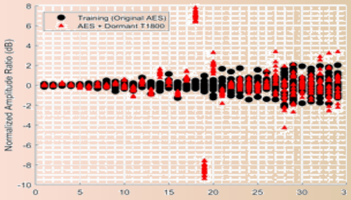
EME-Based Firmware Verification

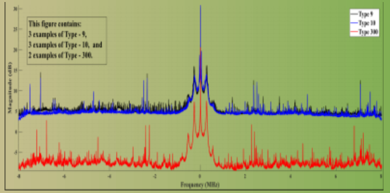
EME-Based Software and Firmware Verification

RFB Analysis

RX

EME Analysis





TX

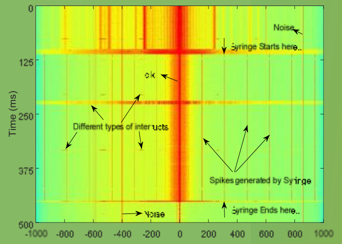
XYZ Positioning

Functional Testing

Acquire

Deploy

Real-Time EME Analysis

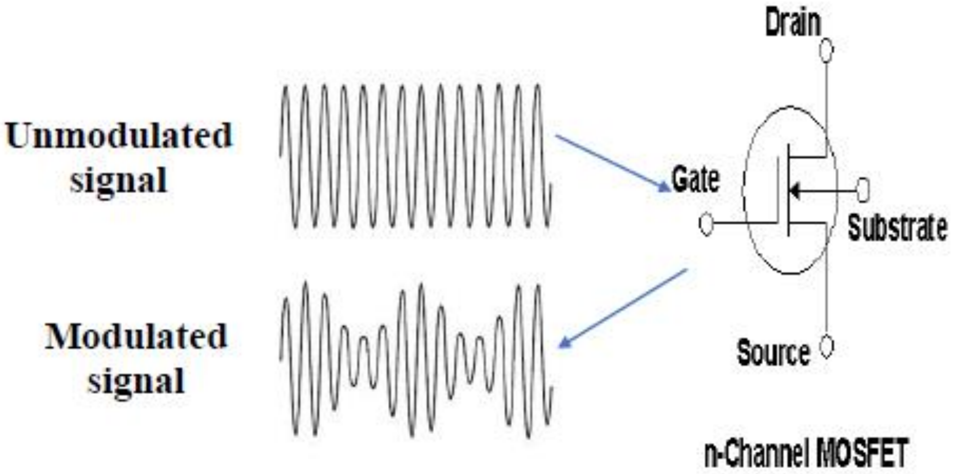


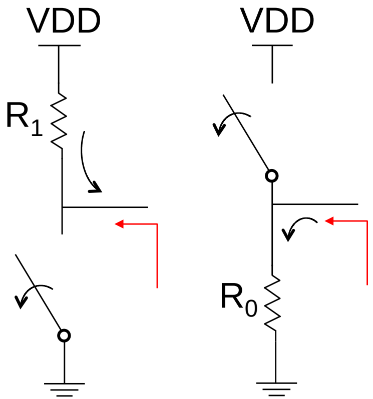
Low-Cost RX

Compact Probe

Normal Operation

❖Impedance Based Side-Channel?





❖Detecting HW Trojans via Backscattering Signals?

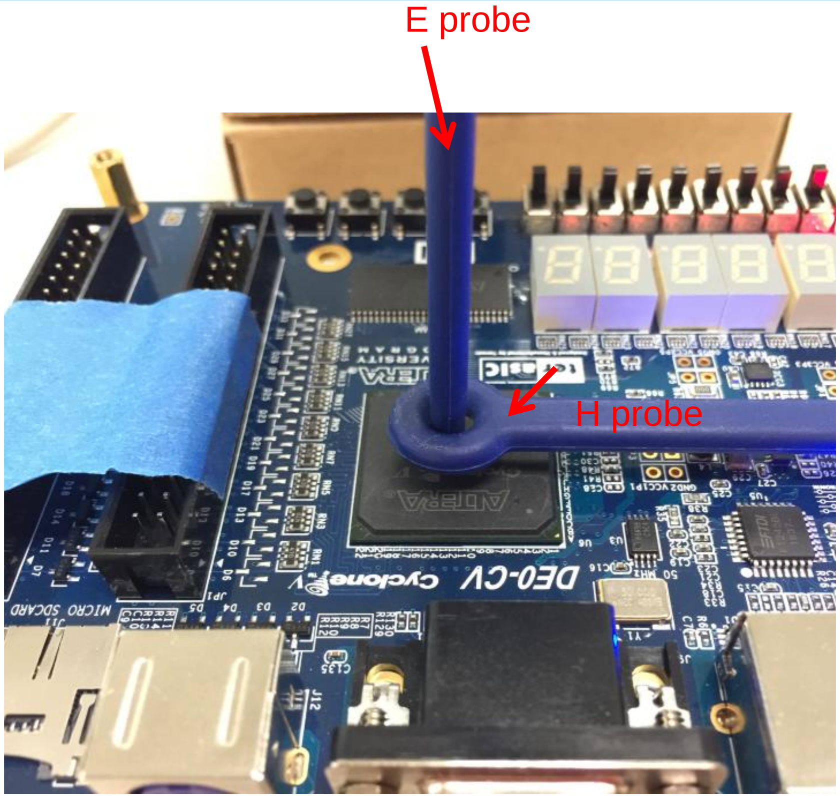
- Synthesized AES-128 crypto-processor on FPGA
  - 11-cycle AES pipeline, new 128-bit data block begun every cycle
- We implemented the hardware Trojan T1800 from trust-hub (http://trust-hub.org/).
  - Activated by a specific 128-bit input value
  - Trojan’s payload circuitry dormant (no switching) until activated
  - Once activated, payloads circuitry toggles a lot (to drain battery)
  - Overall size ~**1.7% of AES circuit**
  - Added to layout while preserving place/route of AES circuit

[8] L. N. Nguyen, C.-L. Cheng, M. Prvulovic, and A. Zajic, “Creating a backscattering side channel to enable detection of dormant hardware Trojans," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, 2019.

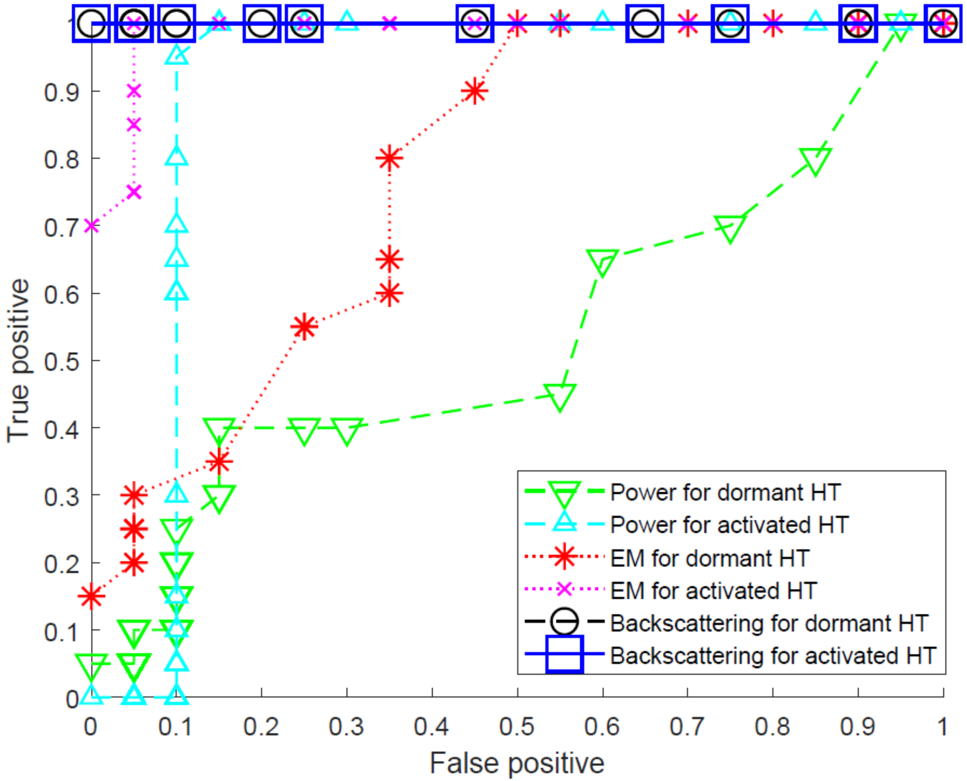
❖Idea for Detection

- Trojan’s “trigger” circuitry is small but active
- Trojan’s connection to AES circuit changes impedances in the original circuit, changing its EM behavior
- Sub-cycle temporal granularity, need BW that is many times the clock rate to capture such rapid changes

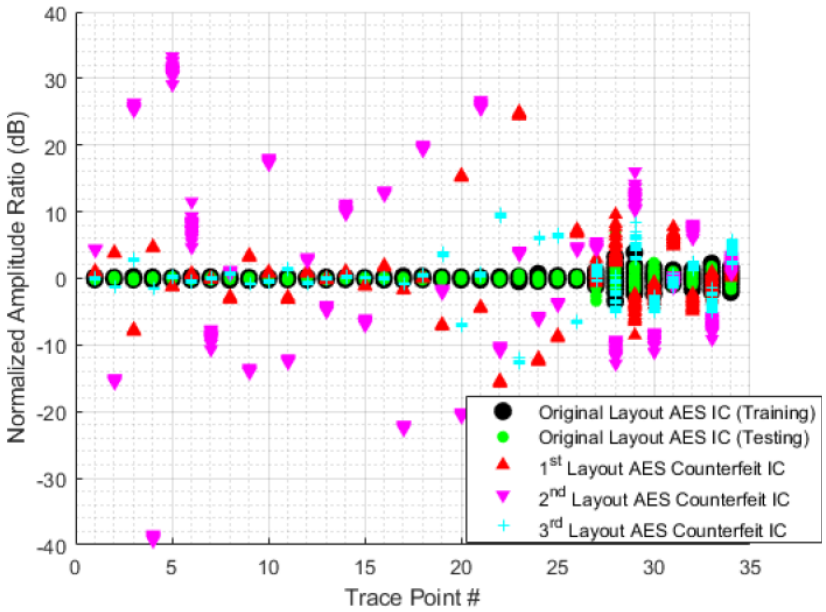
❖Measurement Setup for RFB

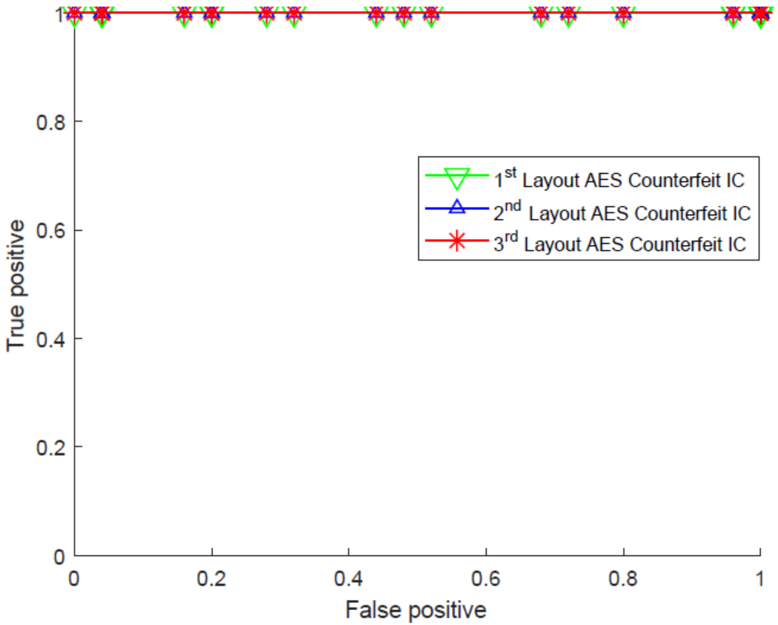


❖Comparison with EM and Power Side-Channels



❖Detection of Counterfeit Designs



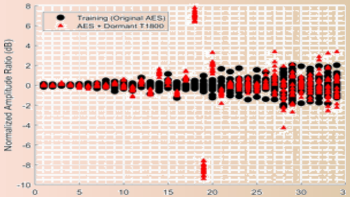


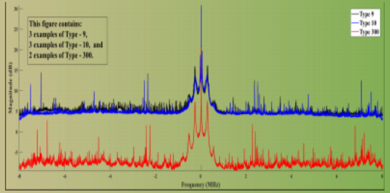
Pre-Deployment Verification

RFB-Based IC Verification and RF Anomaly RFIC Verification

EME-Based Firmware Verification

RFB Analysis ← RX → EME Analysis





TX

XYZ Positioning

Functional Testing

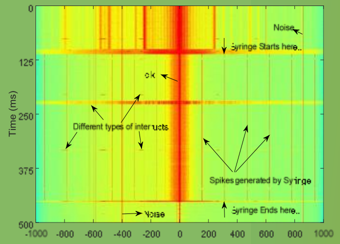
Acquire

Deploy

Continuous Verification

EME-Based Software and Firmware Verification

Real-Time EME Analysis

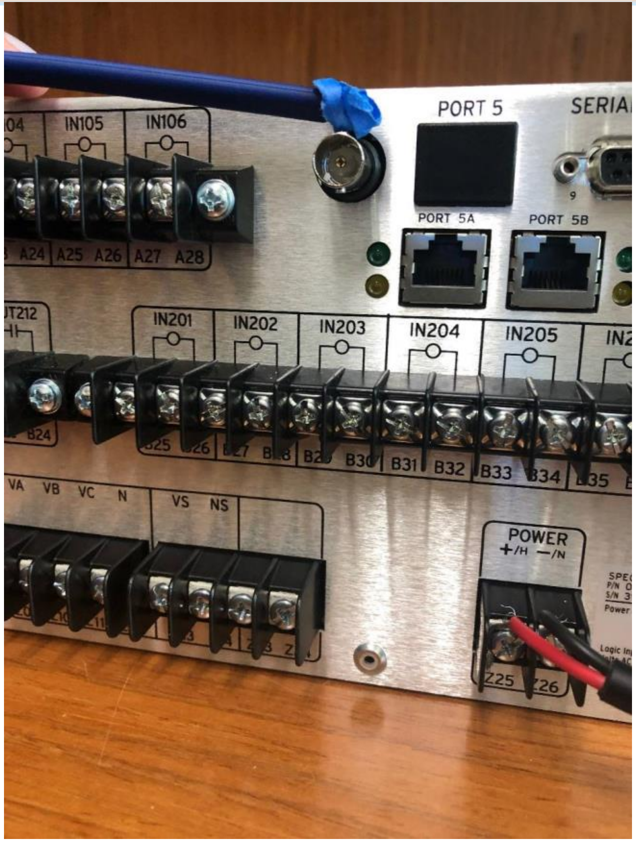


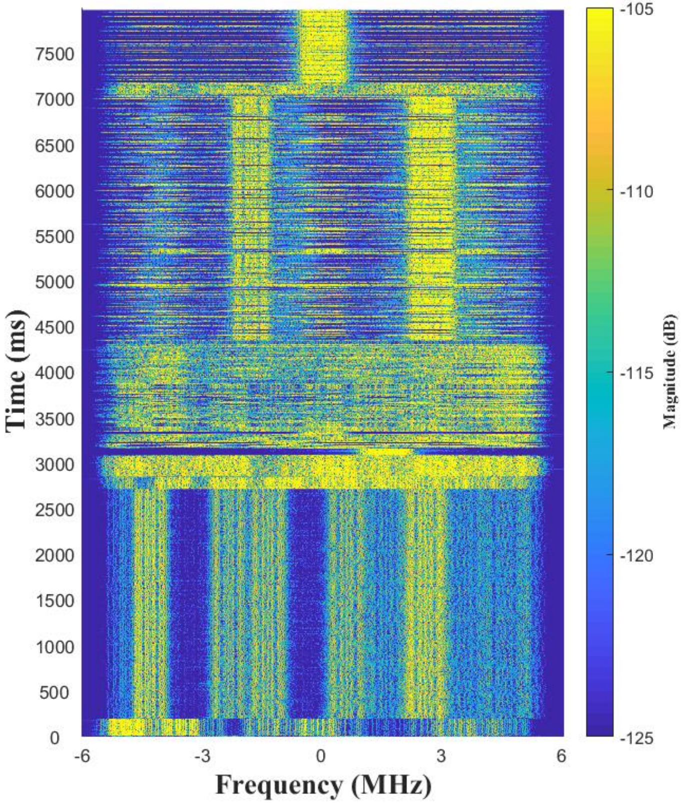
Low-Cost RX

Compact Probe

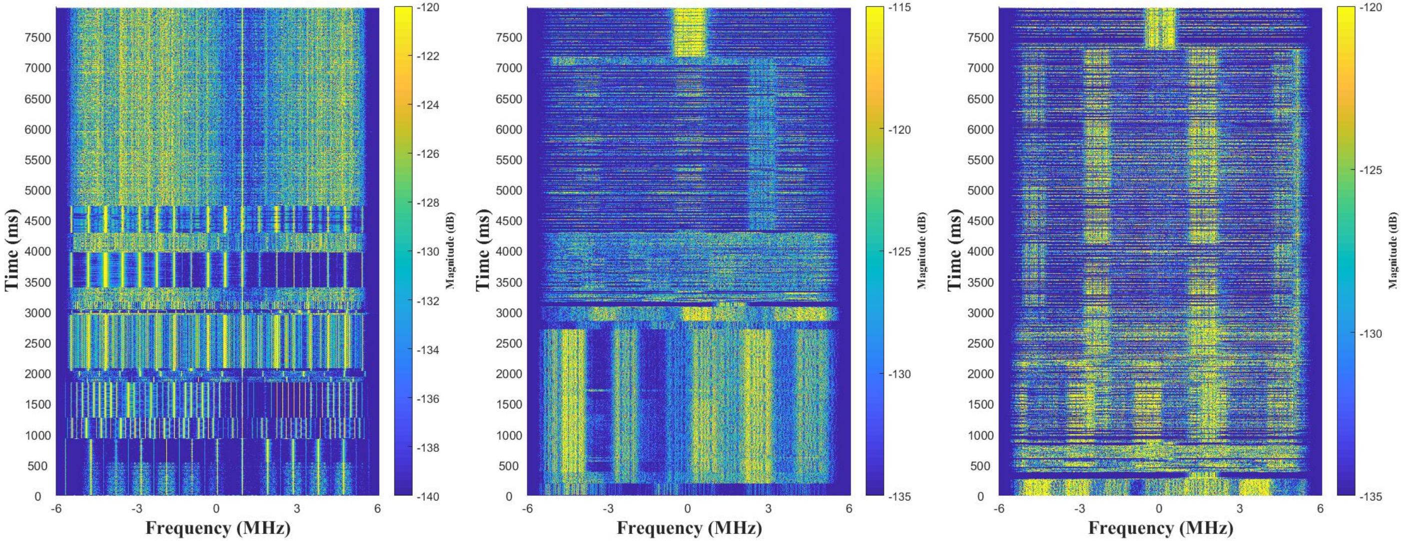
Normal Operation

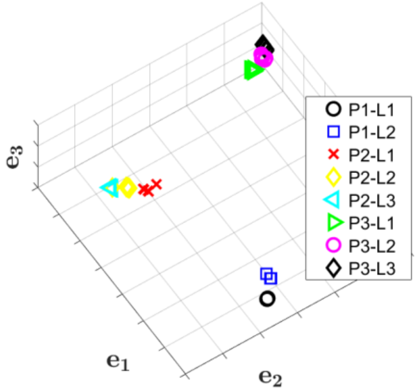
Firmware of SEL-351S Protection System for Power Systems





Different Firmware of SEL-351S Protection System





Pre-Deployment Verification

Continuous Verification

RFB-Based IC Verification and RF Anomaly RFIC Verification

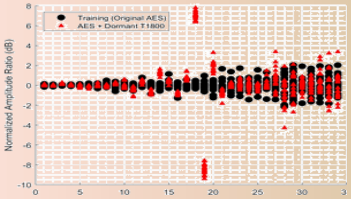
EME-Based Firmware Verification

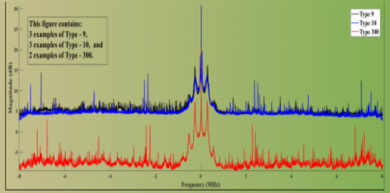
EME-Based Software and Firmware Verification

RFB Analysis

RX

EME Analysis





TX

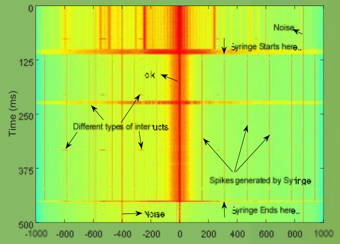
XYZ Positioning

Functional Testing

Acquire

Deploy

Real-Time EME Analysis

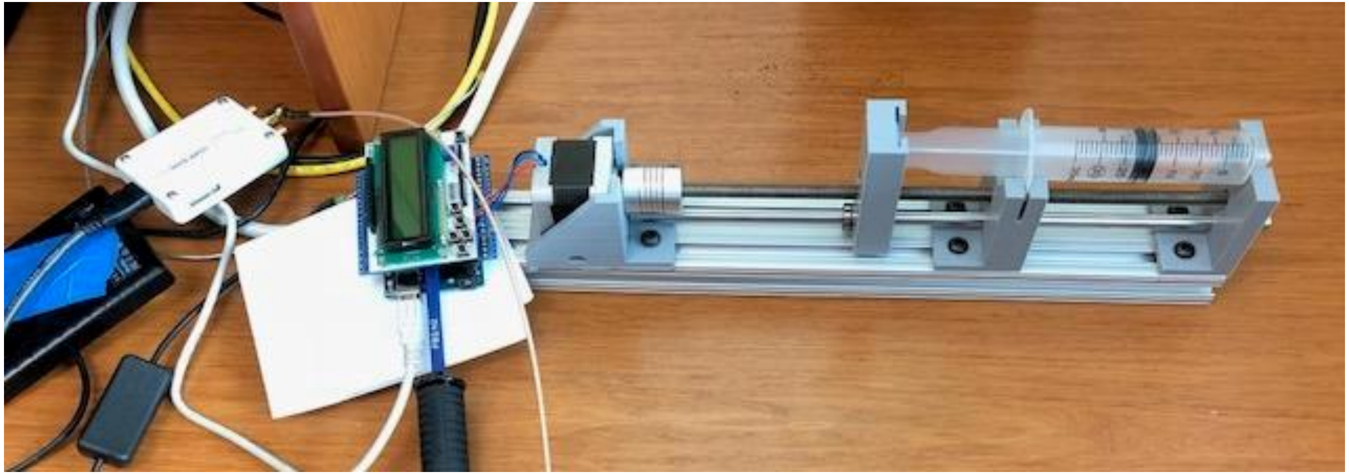


Low-Cost RX

Compact Probe

Normal Operation

❖Syringe Pump

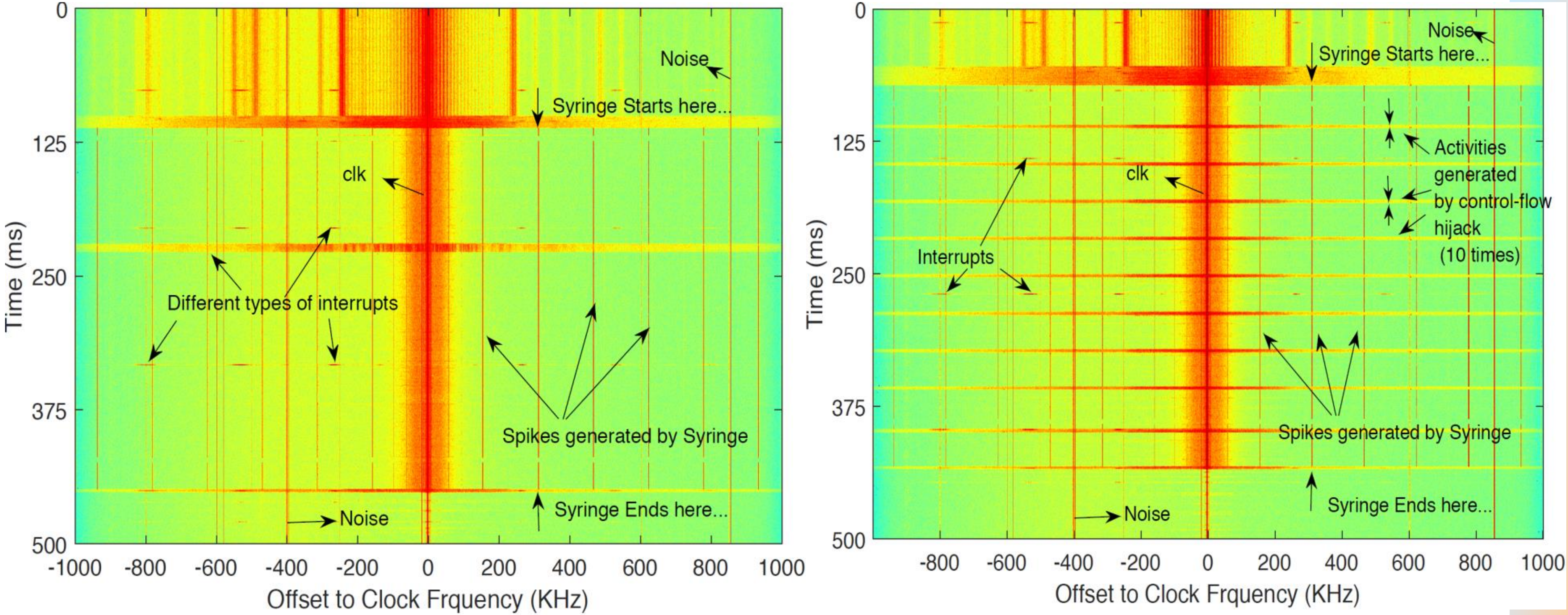


- The buffer overflow overwrites the return address, causing it to jump to the function that is responsible for syringe movement.

[9] A. Nazari, N. Sehatbakhsh, M. Alam, A. Zajic, and M. Prvulovic, "EDDIE: EM-Based Detection of Deviations in Program Execution," *Proceedings of the 44th International Symposium on Computer Architecture (ISCA)*, June2017.

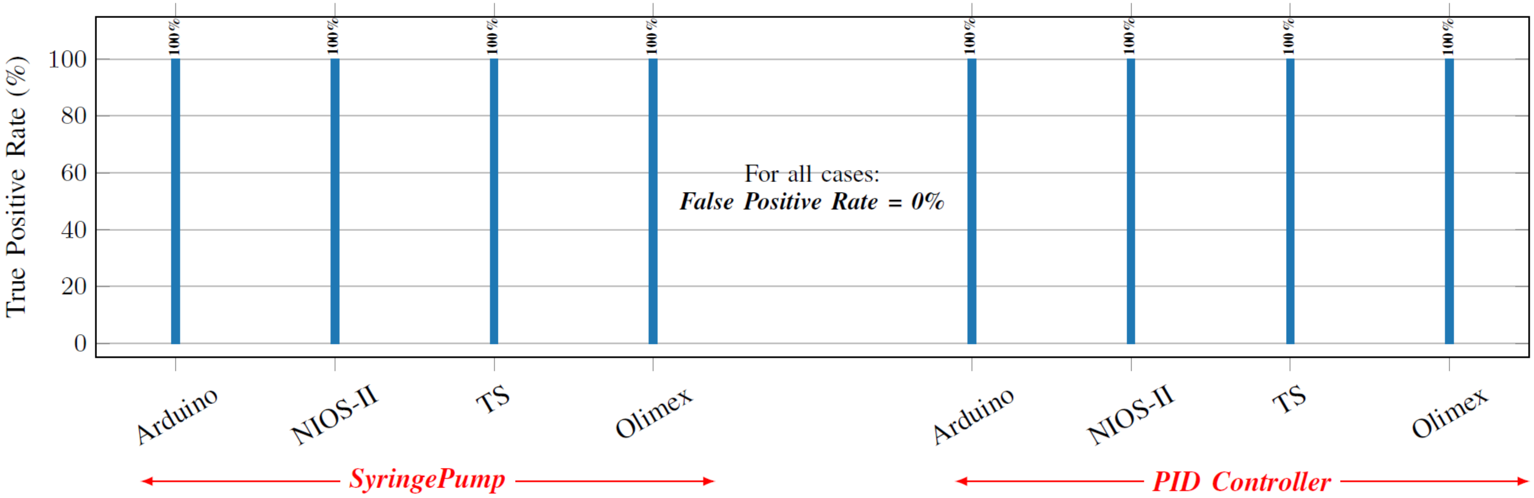
[10] N. Sehatbakshsh, R. Callan, M. Alam, M. Prvulovic, and A. Zajic, "Leveraging Electromagnetic Emanations for IoT Security, " Hardware Demo at IEEE International Symposium on Hardware Oriented Security and Trust (HOST) May 1-5, 2017.

❖Syringe Pump



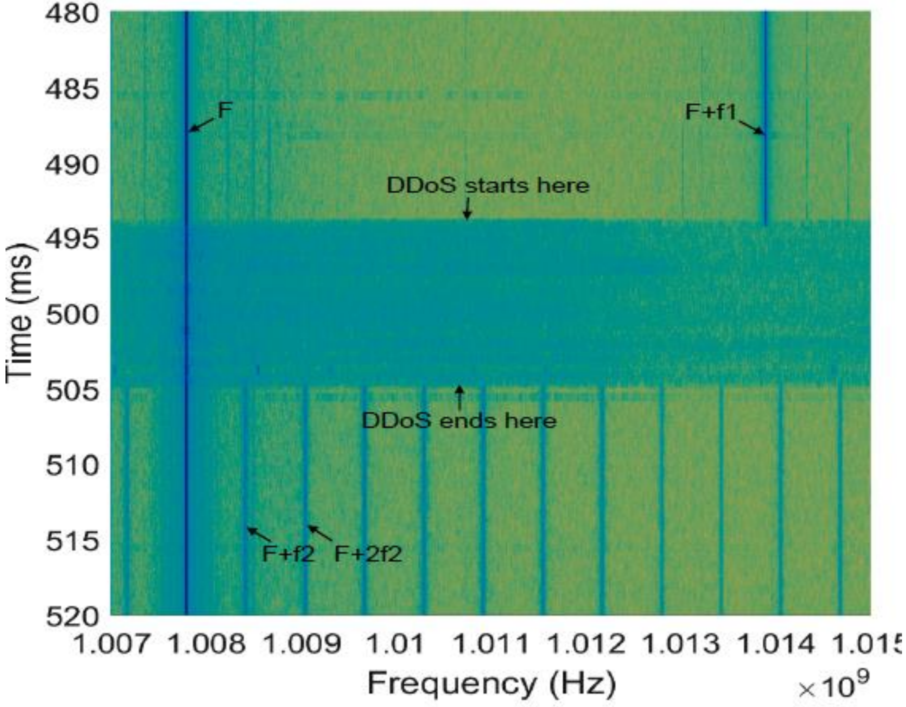
Spectrogram of the Syringe pump application in malware free (left) and malware-afflicted (right) runs

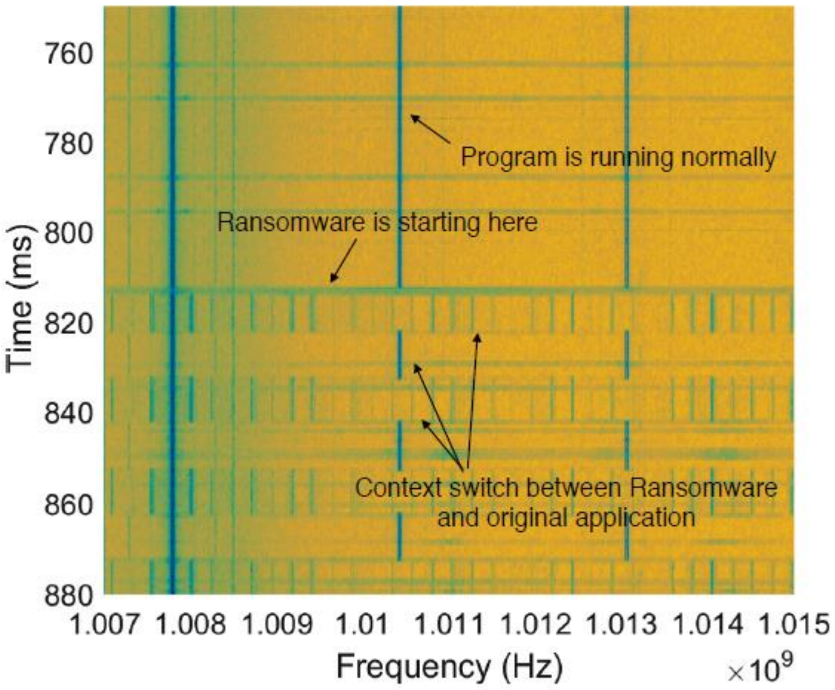
❖Various Devices and Applications



Device	Detection Latency
Arduino	250 µs
Nios-II	250 µs
TS	750 µs
Olimex	1500 µs

❖Syringe Pump infected with Ransomware





❖Conclusions

- Analog side-channels are not always bad, understanding physics behind it makes it powerful tool.
- New side-channel: Impedance-based side channel
- Leveraging EM side channels for firmware verification and malware intrusion detection
- Leveraging impedance-based side channel for hardware Trojan detection

THANK YOU

Questions?