I/UCRC: CARFS
Center for Advanced Research in Forensic Science

On-Device Detection via Anomalous Environmental Factors

PI: Dr. Todd Andel

Computer Science/SoC

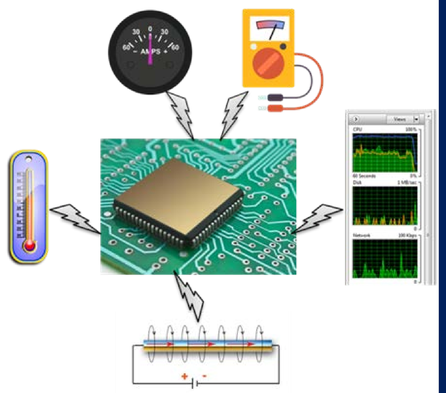
UNIVERSITY OF SOUTH ALABAMA

DFII: Digital Forensics Information Intelligence

RELEVANCE / OBJECTIVES

Relevance

- Physical indicators from attacker activity can be statistically distinguished
  - Temperature, power usage, resource utilization
  - Provide an unsubvertible correlation source

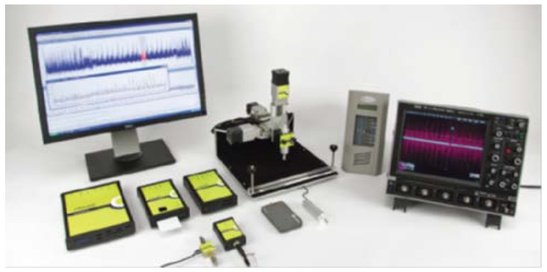


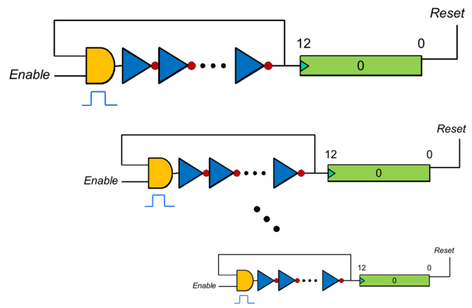
Objectives

- Develop real-time attacker detection capabilities using device level measurements of environmental factors
  - Use of multiple sensors to provide correlation
  - Transition high fidelity side-channel correlation low cost on-chip implementation

APPROACH / TECHNIQUES

- Develop correlation algorithms for baseline signatures in multiple non-malicious environments (“biomes”)
- Evaluate and tune correlation engine against active attacker
- Investigate sensor combinations, including multiple redundant sensors, for systems reporting false information





MILESTONES / DELIVERABLES

Deliverables

- Baseline signature dataset for non-malicious systems
- Analysis & identification techniques of maliciously activity
  - Techniques to detect zero-day exploits and hardware implants

Milestones

- **4 m**: Develop correlation algorithms for baseline signatures from on-device environmental factor sensors & side-channels
- **8 m**: Tune correlation engine to detect anomalous activity.
- **12 m**: Develop redundant sensors with out-of-band reporting. Incorporate low-fidelity capture capabilities in place of high-level requirements

INDUSTRY BENEFITS

Economics

- Advanced persistent threats can routinely subvert a system and provide false readings to cover their activity. The ability to determine such activity using on-device sensor correlations provides a cost effective detection capability

Potential Member Benefits

- Providing away to identify potential zero-day exploits and undiscovered rootkits, or even maliciously implanted hardware
- Identification of exploits from an external side-channel other correlated environmental factor vantage point may lead to detection algorithms that can be integrated without subsequent need for high fidelity side-channel capabilities