Time-Centric Modeling of Correct Behaviors for Efficient Non-intrusive Runtime Detection of Unauthorized System Actions

THE UNIVERSITY OF ARIZONA

Challenge:

- Critical need for anomaly detection methods, specifically designed for embedded systems with minimal area and energy overheads

Solution:

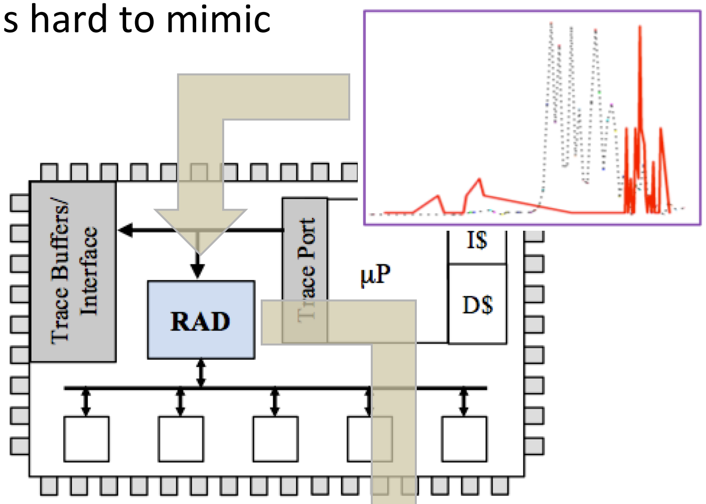
- Combining system-level time constraints and statistical timing models enable novel nominal system behavior models that are resilient to mimicry attacks.
- Secure, non-intrusive, and fast hardware-based identification of runtime deviations from the timing characteristics of embedded systems

Award: CNS-1615890

PIs: Roman Lysecky, Jerzy Rozenblit

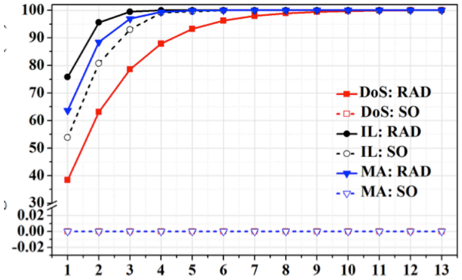
Contact: Roman Lysecky <rlysecky@ece.arizona.edu>

Formal timing models: Fine-grained, subcomponent timing of system events is hard to mimic



Hardware-based: Efficient HW monitors execution with no timing overhead

Better malware detection:



Scientific Impact:

- Time-centric formal models for defining correct system execution behavior with increased resilience
- Systematic methods for evaluating and optimizing tradeoffs between security, area, and energy

Broader Impact:

- Better tools for embedded developers to eliminate/ mitigate malware
- Secure critical systems including medical devices, IoT, automotive, etc.
- Web-native material on security for CS1 programming courses (expected to reach >40,000 students/year)