TCIPG

Trustworthy Cyber Infrastructure for the Power Grid

Hardware-based IDS for AMI Devices

tcipg.org

Overview and Problem Statement

A major challenge is that many embedded system devices used in critical infrastructure applications are easily accessible in the supply chain and can be tampered with or altered such that the authentication of the devices cannot be assured. The installation of a hardware-based backdoor gives a cyber-attacker unlimited eavesdropping access to logic-level communication within a Smart Grid device and is virtually undetectable by state-of-the art intrusion detection systems. In addition, a hardware-based backdoor can be inserted during the manufacturing processes or deployment lifecycle. A one-time verification is insufficient. This research activity looks at ways to identify that kind of attack at the embedded system board level, while keeping in mind the constraints of manufacturing cost and normal system performance. This research also looks at the supply chain as a cybersecurity system-level problem, looking for ways to bridge manufacturing practices and lifecycle information assurance.

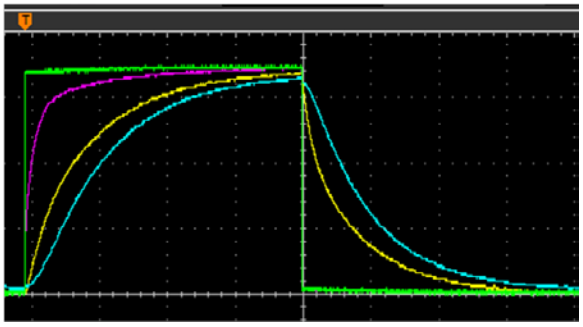
Research Objectives

- Identify the electrical characteristics of a hardware-based, logic-level attack.
- Derive a hardware detection algorithm that can be scaled to different communication bus speeds.
- Determine design considerations with regard to IDS sensitivity and accuracy.
- Identify nonlinear circuits that provide a differential comparison between normal inter-chip communication and unauthorized use during a hardware-based attack, without the use of stored “secret” values.
- Study the analog characteristics of low-cost circuit components to determine if normal manufacturing process variance is enough to create unique hardware signatures that are very difficult to replicate.
- **Smart Grid Application Area:** AMI, SCADA, any embedded system Smart Grid device.

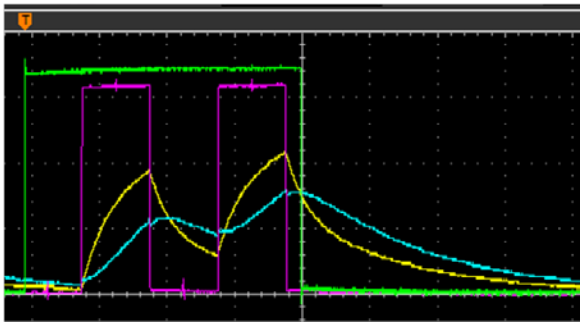
Technical Description and Solution Approach

- Use low-cost, resistive-capacitive circuits connected to an inter-chip communication bus that causes a temporary transfer in system energy; presents a physics-based challenge to the system.
- Synchronously measure the dynamic analog responses to the challenge and derive several IDS metrics: discrete values, voltage, time, interval slopes, and area under curves.
- An intruder attached to the communication bus causes a perturbation of waveform and response characteristics.
- Use statistical analysis to build effective IDS models to distinguish between intruder types.

Normal IDS Circuit Response

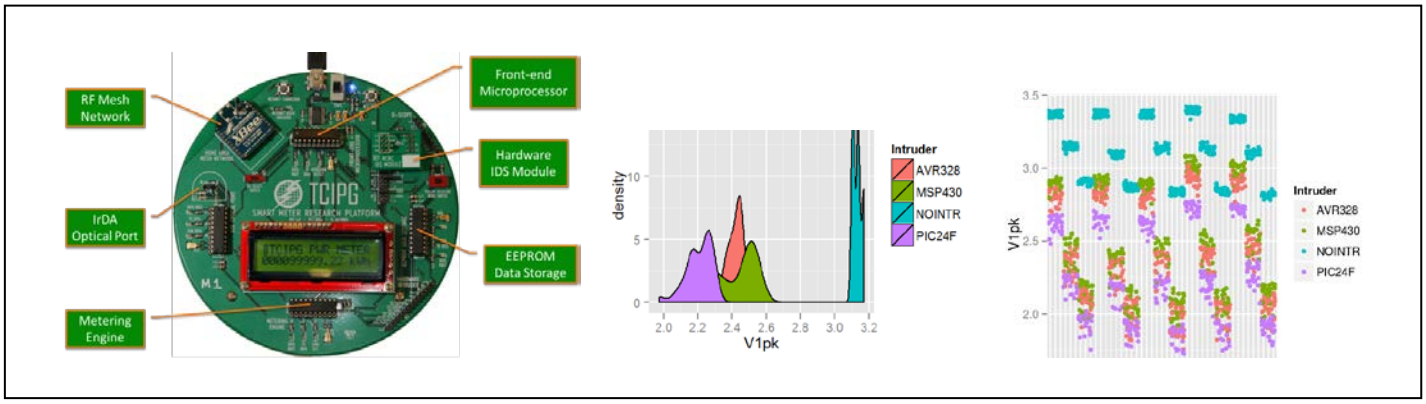


IDS Circuit Response with Intruder



Results and Benefits

- Created the Smart Meter Research Platform to enable embedded system security research.
- Completed empirical model of hardware-intruder electrical characteristics from 80 million measured data points.
- Signatures of various intruders are distinct.
- Intrusion Detection System can accurately distinguish among several varieties of hardware intruders at 89% accuracy with non-optimized algorithm (i.e., the accuracy can easily be improved).
- Provides a high-resolution view of the security status of AMI devices and systems.
- Low impact on system performance.
- Low-cost and easily integrated into new Smart Grid devices.
- **Partnerships and External Interactions:** Sandia National Laboratories (DOE).
- **Technology Readiness Level:** Proof-of-concept complete, 3 provisional patent applications from this activity.



Researchers

- Nathan J. Edwards, njedwar@sandia.gov (recent TCIPG graduate)

Industry Collaboration

- Jason Hamlet, Sandia National Laboratories (DOE)
- Ryan Helinski, Sandia National Laboratories (DOE)
- David Robinson, Sandia National Laboratories (DOE)

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000. SAND2012-8083P