TCIPG Hardware-based IDS for AMI Devices

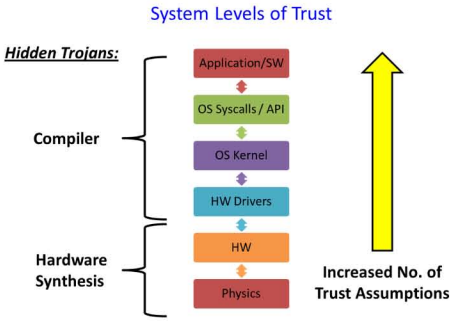
Nathan J. Edwards

Goals

- Identify low-cost circuit components that can create unique hardware signatures that are very difficult to replicate.
- Model hardware-intruder-based attacks.
- Create proof-of-concept for low-level Intrusion Detection System that can identify embedded system device hardware eavesdropping and intruders.
- Create technical solutions that help address cyber security risks in the supply chain.

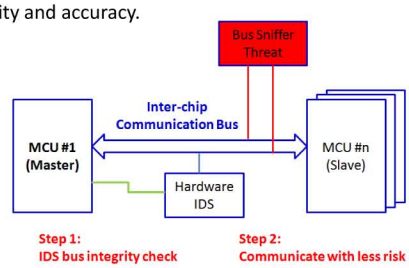
Fundamental Questions/Challenges

- Can we accurately detect passive "eavesdropping" attacks and active "unauthorized use" attacks on inter-chip communication?
- How do we assure the authentication of a device given the complexity of a manufacturing supply chain?
- Challenge: Hardware backdoors can be inserted during manufacturing processes or device lifecycle. A one-time verification is insufficient.
- Challenge: Hardware attacks might be latent/intermittent and not be visible to software or network IDSes.



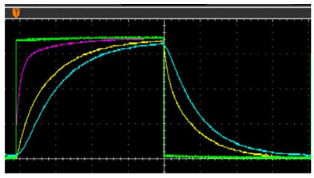
Research Plan

- Identify the electrical characteristics of a hardware-based logic-level cyber-attack (both passive attacks and active attacks).
- Study the analog characteristics of low-cost circuit components to determine if normal manufacturing process variance is enough to create unique hardware signatures (both for IDS and authentication purposes).
- Identify nonlinear circuit configurations that provide a differential comparison between normal inter-chip communication and that of a hardware-based attack, without the use of stored "secret" values.
- Use statistical analysis to derive hardware detection algorithm(s) that can be scaled to different communication bus speeds.
- Determine several design considerations with regard to IDS sensitivity and accuracy.

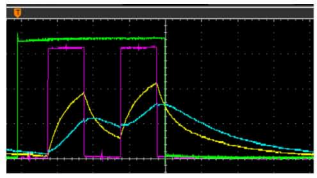


Research Results

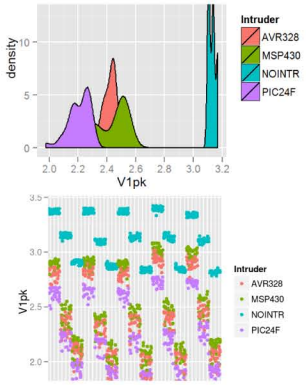
- Created the Smart Meter Research Platform to enable embedded system security research.
- Completed empirical model of hardware-intruder electrical characteristics from 80 million measured data points.
- Signatures of various intruders are distinct.
- Intrusion Detection System can accurately distinguish among several varieties of hardware intruders at 89% accuracy with non-optimized algorithm (i.e., the accuracy can easily be improved).
- 3 provisional patent applications from this activity.



Normal Hardware Response



Hardware Response with Intruder



Broader Impact

- Provides a high-resolution view of the security status of an AMI system.
- Low impact on system performance.
- Low-cost and easily integrated into new Smart Grid devices (also implies possible retrofit into existing designs).
- Technology can be applied to any next-generation critical infrastructure embedded system device.

Interaction with Other Projects

- This hardware-based IDS technology can be combined with a specification-based IDS (TCIPG) and systemwide IDS (TCIPG) to give power utility operators a complete and high-resolution view of the AMI system security status.

Future Efforts

- Extend the proof-of-concept to multiple-master bus communication.
- Use these techniques and hardware to determine if specific intruder ICs within a single class (e.g., PIC24F) can be distinguished.
- Use these techniques and hardware to determine if individual smart meter platforms can be distinguished (authentication).
- Continue hardware security research collaboration with Sandia National Laboratories.
- Work with AMI device manufacturers to test IDS solution on real devices.

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-AC04-94AL850. SAND2012-8082P