TCIPG Hardware-based IDS for AMI Devices

Nathan J. Edwards

Goals

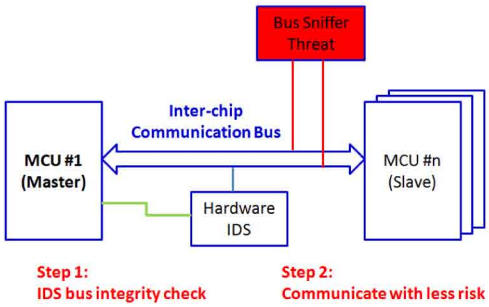
- Identify low-cost circuit components that can create unique hardware signatures that are very difficult to replicate.
- Model hardware-intruder-based attacks.
- Create proof-of-concept for low-level Intrusion Detection System that can identify embedded system device hardware eavesdropping and intruders.

Fundamental Questions/Challenges

- What kind of surface-mount components have enough variance to create unique signatures that are not stored in memory?
- Can we accurately detect passive “data sniffing” attacks and active “unauthorized use” attacks on inter-chip communication?
- Challenge: hardware-based IDS solution must be low-cost in order for industry to use technology on AMI devices.
- Challenge: hardware-based IDS solution must not have significant impact on the AMI device performance.
- Challenge: analog circuit components degrade independently over time and shift their characteristics with changes in the operating environment.

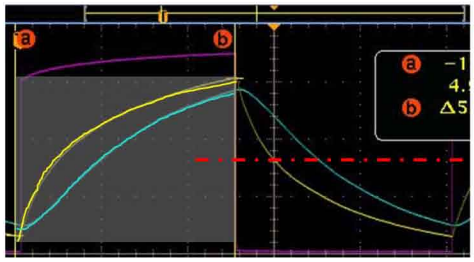
Research Plan

- Study the analog characteristics of low-cost circuit components to determine if normal manufacturing process variance is enough to create unique hardware signatures.
- Find a pragmatic method to use the unique characteristics for device authentication without the use of “secret” values stored in memory.
- 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.
- Identify the electrical characteristics of a hardware-based logic-level cyber-attack (both passive attacks and active attacks).
- Derive a hardware detection algorithm that can be scaled to different communication bus speeds.
- Determine several design considerations with regard to IDS sensitivity and accuracy.
- Conduct Red Team analysis of IDS technology and strengthen solutions.

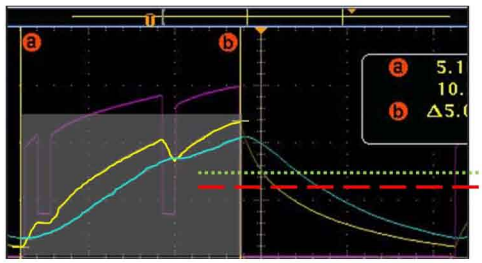


Research Results

- Variations in resistor and capacitor manufacturing are not enough to create significantly unique hardware signatures in time domain.
- Hardware charge/discharge phases statistically equiv. (< 5% error) during normal operation (without intruder) and offer per-cycle detection.
- An intruder attached to communication bus changes shape of waveforms and shifts line of symmetry, peak voltages, and several 1st-order/2nd-order values.



Normal Hardware Response



Hardware Response with Intruder

Broader Impact

- Provides a high-resolution view of the security status of 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 System-wide 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.
- Continue to explore low-cost solutions for unique hardware signatures.
- Create low-cost functional prototype for emulated environment.
- Work with AMI product manufacturers to test IDS solution on real devices.