Intrusion Detection for Smart Grid Components by Leveraging of Real-Time Properties

Overview and Problem Statement

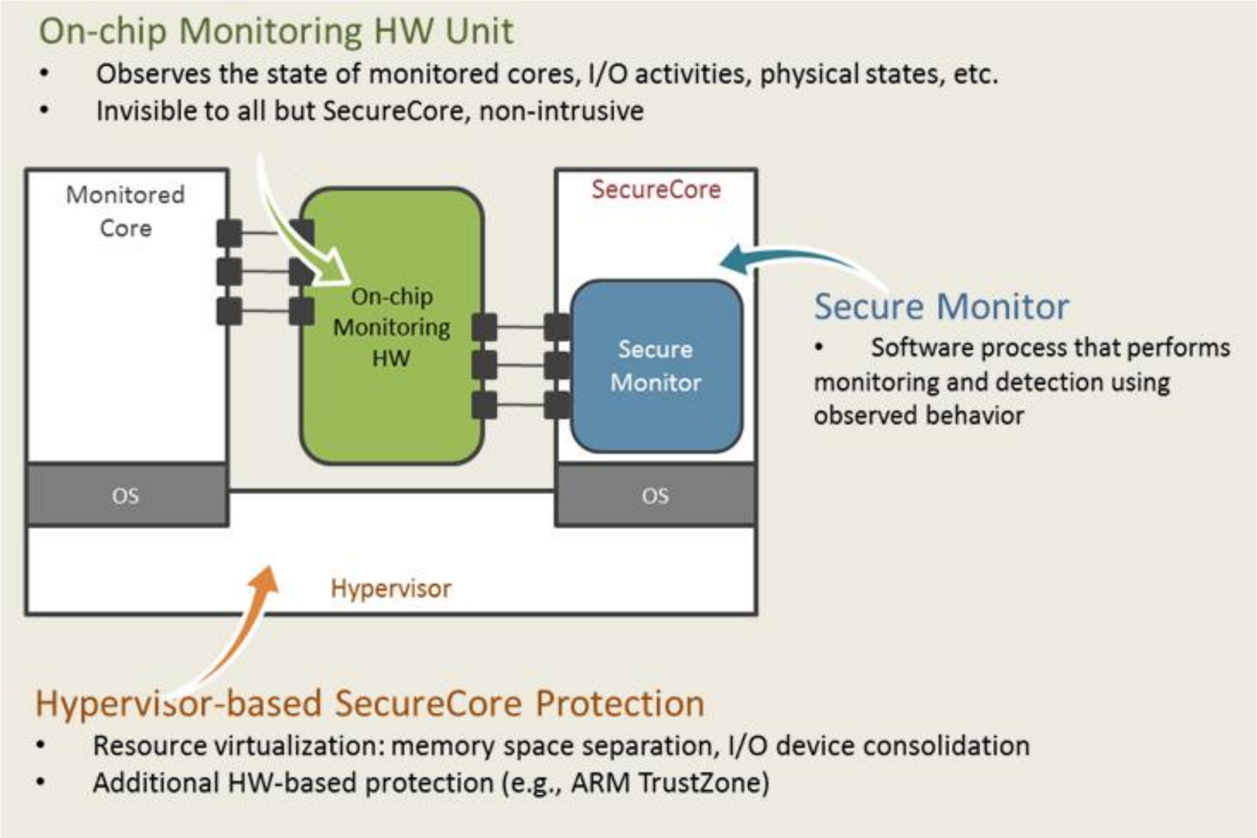
We aim to tackle the problem of detecting intrusions in power grid components with real-time properties. Most components that require a safety-critical model of operation fall under this category. The main technique is to perform behavioral analysis of such systems in order to find anomalies with respect to attributes such as execution time, memory, and I/O. Complementary to traditional cyber security technologies that aim to prevent intrusions, our work focuses on survivability: the ability to continue operating safely even if intruders succeed in penetrating a system. Furthermore, an intruder's act of performing unsafe operations or modifying the existing data acquisition and/or control software will lead to detection and removal using our techniques. The detection approach will be coupled with the development of architectures that will maintain the safety of the overall safety-critical system, even if an attacker is able to intrude successfully into the system.

Research Objectives

- Develop behavioral models of real-time control systems used in the smart grid.
- Use above models along with trusted hardware modules to monitor the components for deviations from expected behavior.
- When intrusions are detected, transfer control away from the main controller to the trusted hardware module; the main controller will be either shut down gracefully or analyzed by engineers. Either way, the physical control system will not be harmed.
- **Smart Grid Application Area:** Security for components with real-time properties in the smart grid and mobile devices used for monitoring components in the grid.

Technical Description and Solution Approach

- The overall solution will be applicable at the *individual node* level, where we monitor cyber properties such as execution time and memory, as well as I/O traffic, using a trusted platform. The technique is likely to be successful because most computational components in cyber-physical systems have deterministic behavior (by design) that can be monitored for anomalies. For this activity, we started with *execution time* and *control* behavior and are now experimenting with other system properties, such as memory and OS behavior and I/O.
- We developed timing-based analysis models for real-time control systems, both for exact timing and for statistical methods. We also implemented methods to follow the control flow of the code in such systems. We are currently analyzing the memory traffic/usage and the distribution of system calls.
- We intend to implement the analysis and detection methods to detect anomalies in smart grid components such as IEDs.
- We are also developing secure hardware-based monitoring platforms; the following image shows the high-level design using a multicore platform (which we call "SecureCore").


On-chip Monitoring HW Unit

- Observes the state of monitored cores, I/O activities, physical states, etc.
- Invisible to all but SecureCore, non-intrusive

Secure Monitor

- Software process that performs monitoring and detection using observed behavior

Hypervisor-based SecureCore Protection

- Resource virtualization: memory space separation, I/O device consolidation
- Additional HW-based protection (e.g., ARM TrustZone)

Results and Benefits

- Increased security for individual computational nodes in the power grid (e.g., IEDs and smart meters).
- Ability of such components to detect and recover from failures due to malicious activity.
- **Technology Readiness Level:** Developed initial analysis based on learning the behavior of execution time profiles; developed initial multicore-based detection architecture; developed initial compile-time analysis to capture control flow of programs; developed initial FPGA-softcore-based prototype to monitor control flow of real-time programs; developed SecureCore architecture and implemented it in the Simics full system simulator; developing memory and system-call-based analyses now.

Researchers

- Sibin Mohan, sibin@illinois.edu
- Rakesh Bobba, rbobba@illinois.edu

Industry Collaborators

- Qualcomm Research.
- In discussions with power system vendors.