TCIPG

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

Behavior-based Intrusion Detection for Smart Grid Components with Real-Time Properties

Man-Ki Yoon, Fardin Abdi, Sibin Mohan, Rakesh Bobba, Lui Sha

RETHINKING REAL-TIME SYSTEM SECURITY

- The power grid has many real-time embedded systems (RTS) deployed in the field.
- Running traditional IDS is not always practical.
- Modern real-time systems are smarter but less secure.

IDS → **aware of real-time environments and can leverage their properties**

FEATURES OF REAL-TIME EMBEDDED SYSTEMS

Limited Resources
- Computational power, energy, cost

Timing Requirement
- Safety, reliability, quality of service

System Upgrade
- Verifiability

Resource Overhead	• Fine-grained monitoring • Instructions, memory access, function/system calls
High Upgrade Cost	• Formal verification for every new update
Increasing Complexity	• Capabilities and access control
Adaptability	• Domain-specific, unforeseen vulnerabilities

RESEARCH PLAN

- **Goal:** **Detection** of anomalous/malicious behavior.
- **Idea:** Based on **predictable behavioral patterns.**
  - Timing, control flow, memory usage, system calls.
  - I/O activity, power consumption, etc.
- **Approach:**
  - Profiling by machine learning or compile-time analysis.
  - Inspection by core-to-core monitoring in multicore.
  - Detection by deviation from legitimate behavior.
- Embedded systems are **predictable by design**.
  - Finite set of operational modes.
  - Period jobs.
- **Deviation** from expected behavior → **Abnormality**

Threat Analysis
- Identification of the aspects of system behavior that are affected by attack type
- Studying attacks that mimic system behavior

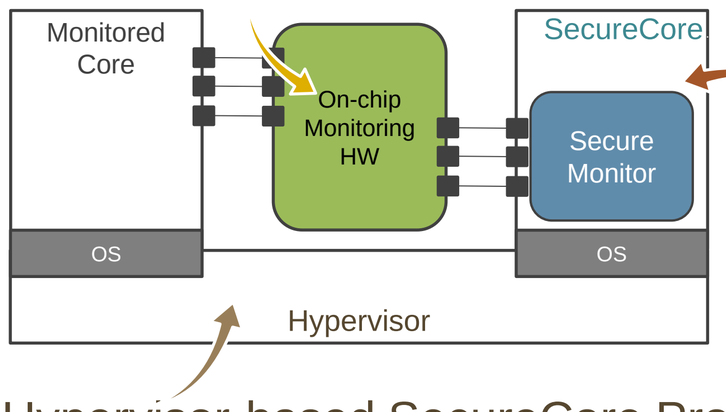
Development of Profiling Method
- How to effectively capture all behavioral variations excluding interference
- Platform-independent profiling
- Multidimensional behavior profiling

Implementation
- Minimal processor architecture modification
- High-resolution monitoring with minimal overhead
- Tamper-resistant secure core

RESEARCH RESULTS

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).

Monitored behavior:
1. Execution time
2. Control flow
3. System call usage
4. Memory requests

→ **Types of attacks that can be detected:**
a. Code injection
b. Code replacement
c. Return address modifications
d. Preventing important tasks from running

Other potential behavioral signals:
i. Network activity
ii. I/O, sensory and actuation signals, etc.
iii. Power consumption

Combine → future work → **Multivariate Analysis**

↓

Increased Difficulty for Attackers

BROADER IMPACT

- **Better security guarantees.**
- **Low overhead.**
- **Greater possibilities for adaptability.**
- **Uses mostly COTS hardware.**
- **Applicability to different types of components.**

FUTURE EFFORTS

- **Multivariate analysis.**
- Application of techniques to **real-world systems.**
- Building testbeds.
- Expand to more general-purpose systems.

UNIVERSITY OF ILLINOIS | DARTMOUTH COLLEGE | UC DAVIS | WASHINGTON STATE UNIVERSITY
FUNDING SUPPORT PROVIDED BY DOE-OE AND DHS S&T