BEHAVIOR-BASED ZERO-DAY INTRUSION DETECTION FOR REAL-TIME CYBER-PHYSICAL SYSTEMS

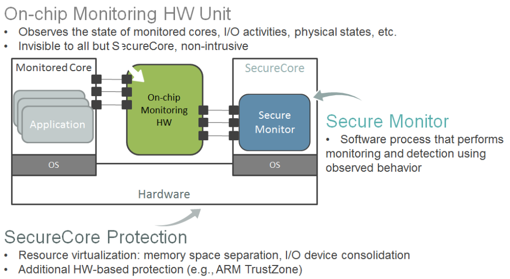
ILLINOIS
UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN

Challenge:

- Detect intrusions in real-time control systems (and further, in more general purpose systems)
- Ensure system remains **safe** in event of attack

Solution:

- Use deterministic behavior of real-time embedded systems to detect deviations (anomalies).
- Developed an architectural framework that can be used to detect anomalies and also take away control (to maintain safety) when an intrusion is detected.
- Developed innovative methods to capture the behavior of systems and for checking at runtime.



On-chip Monitoring HW Unit

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

Monitored Core

Application

On-chip Monitoring HW

SecureCore

Secure Monitor

OS

OS

Hardware

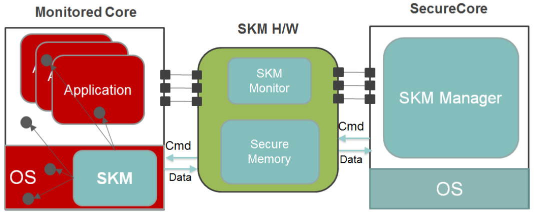
Secure Monitor

- Software process that performs monitoring and detection using observed behavior

SecureCore Protection

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

SecureCore Architecture



Monitored Core

Application

OS

SKM

Cmd

Data

SKM H/W

SKM Monitor

Secure Memory

Cmd

Data

SecureCore

SKM Manager

OS

DragonBeam Architecture

Scientific Impact:

- Innovative methods to capture the behavior of systems for IDS
- Architectural frameworks (SecureCore, DragonBeam) that enable better IDS based on observation of runtime behavior
- Results/methods developed here can be used to understand how to detect anomalies in both, real-time embedded systems as well as general purpose systems.

Broader Impact:

- Real-time control systems are everywhere (automobiles, avionics, power systems, industrial control systems, etc.) and are now being attacked – so these methods can make such systems more secure and safe.
- This work has been included in a graduate course on Cyber-Physical Systems at UIUC.

Project Number NSF CNS 14-23334, University of Illinois at Urbana-Champaign

Contact: **Sibin Mohan** [sibin@Illinois.edu, +1-217-300-3037]