Towards Secure and Resilient Networked Embedded Systems

Saurabh Bagchi
School of Electrical and Computer Engineering
Department of Computer Science
Purdue University


Presentation available at: *engineering.purdue.edu/dcsl*

PURDUE UNIVERSITY

Vision and Goals

- Foundations for designing highly secure and resilient networked embedded systems
  - That can achieve mission success
  - Under component failures and sophisticated cyber/physical attacks
- Enable:
  - Systematic and rigorous design principles to build in security and resilience into software code bases of embedded systems
  - Real-time self-diagnostics to detect, identify, and isolate attacks and failures at millisecond level resolution
  - Rational process for deciding on where to spend security budget
  - Self-healing, real-time adaptation, and reconfiguration to achieve mission objectives

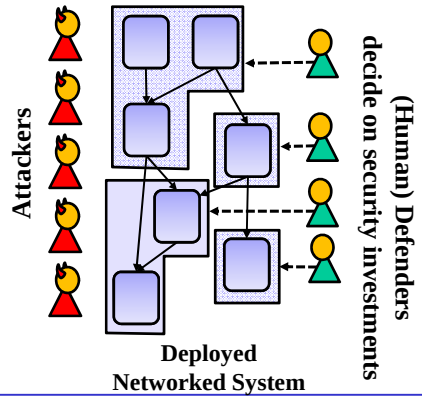
PURDUE UNIVERSITY

Problem Statement

- Many of our critical infrastructures run on large-scale, multi-organizational, interdependent cyberphysical systems (CPS)
- The CPS is subjected to a variety of security threats
  - cyber (*e.g.*, sending malware against a control system)
  - physical (*e.g.*, physically damaging a distribution line)
- Ensuring the security is a complex multi-faceted problem, and requires understanding
  - dynamics of physical systems
  - information exchange and attack propagation in cyber systems
  - human decision making during the design and operation of the coupled system
- Homogeneity in the system eases attack propagation

Solution Directions

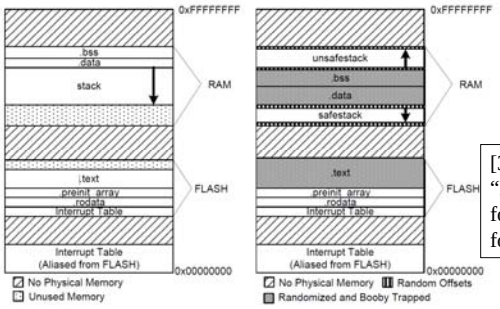
- Game-theoretic analysis provides rational basis for decision making on security investments in shared systems[1, 2]
  - Demonstrated on large-scale CPS and smart grid demand side
  - Tackles systems owned by multiple distinct entities



[1] T. Shawly, J. Liu, N. Burow, S. Bagchi, R. Berthier, and R. Bobba, "A Risk Assessment Tool for Advanced Metering Infrastructures," At the 5th IEEE International Conference on Smart Grid Communications (SmartGridComm), pp. 989-994, November 3-6, 2014.
[2] P. Wood, S. Bagchi, and A. Hussain, "Defending Against Strategic Adversaries in Dynamic Pricing Markets for Smart Grids," At the 8th International Conference on Communication Systems and Networks (COMSNETS), pp. 1-8, January 5-9, 2016, Bangalore, India.

Solution Directions

- Randomization-based security[3]
  - Deals with limited entropy available on embedded devices
  - Randomizes data as well as control to design provably secure systems
  - Bounds degradation in resource usage or performance

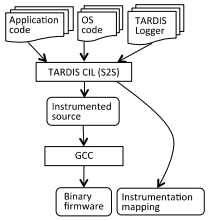


[3] A. Clements, S. Bagchi, M. Payer, "Diversity Enabled Booby-Trapping for Embedded Systems," In preparation for submission.

Solution Directions

- High-fidelity record and replay for debugging[4, 5]
  - Record events in the fielded embedded device
  - Play it back faithfully for diagnosing anomalous events

AVEKSHA



TARDIS

[4] M. Tancreti, V. Sundaram, S. Bagchi, and P. Eugster, "TARDIS: Software-Only System-Level Record and Replay in Wireless Sensor Networks," At the 14th ACM/IEEE Conference on Information Processing in Sensor Networks (IPSN), pp. 286-297, April 13-17, 2015, Seattle, WA.
[5] M. Tancreti, M. S. Hossain, S. Bagchi, and V. Raghunathan, "AVEKSHA: A Hardware-Software Approach for Non-intrusive Tracing and Profiling of Wireless Embedded Systems," At SenSys, pp. 288-301, Seattle, Washington, November 1-4, 2011. (Winner of best paper award)

Presentation available on:
Research group web page
engineering.purdue.edu/dcsl

PURDUE UNIVERSITY