An Instruction Set Randomization Framework for Developing Secure and Resilient CPS

Bradley Potteiger, Zhenkai Zhang, Xenofon Koutsoukos

Vanderbilt University

Institute for Software Integrated Systems

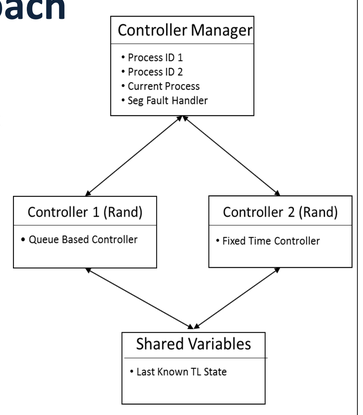
1025 16th Avenue South, Nashville TN, 37212

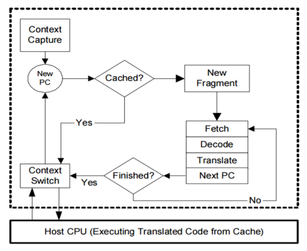
Motivation

- CPS are vulnerable to code injection attacks through buffer overflow vulnerabilities
- Instruction Set Randomization (ISR) mitigates this attack by altering machine code architecture
- System crashing can have devastating effects on safety critical CPS
- Performance overhead can lead to real time constraint violations

Approach

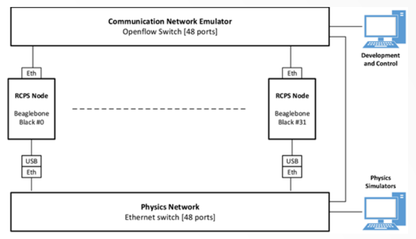
- Control Software ISR
  - Machine code encoded with 32 bit key (patched binutils objcopy function)
- Runtime Derandomization
  - Code is executed through virtual binary translation layer (MAMBO)
  - Context Switch between MAMBO and host cpu
  - Derandomization during decode stage of MAMBO pipeline
- Detection
  - Segmentation fault signal catcher in control manager
- Recovery
  - –Switch to known safe controller

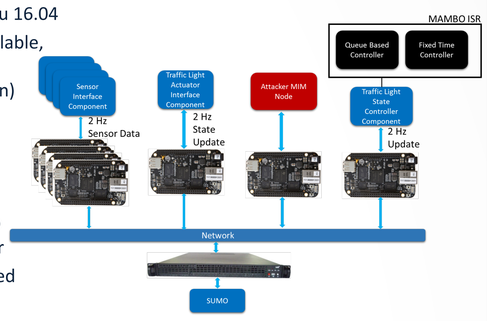




Experiment Setup

- **Hardware Testbed**
  - Cluster of 32 Beaglebone Black Nodes
    - Run component based application code
  - Two network interfaces:
    - Ethernet Network
    - Emulated Protocol Network (OpenFlow Switch)
- **Software Environment**
  - Platform – 32 bit Arm V71 architecture running Xenomai Real Time Linux on Ubuntu 16.04
  - SUMO – Open source, scalable, microscopic road traffic simulator (Physical domain)
  - Traffic Light Controllers – Beaglebone Black
  - Randomization – Binutils ObjCopy
  - ISR Framework – MAMBO Dynamic Binary Translator
  - Communication – Emulated Network





Code Injection Attack Scenario

Model elements: 4 inductive loop sensors (number of cars in queue), traffic light actuator interface (changes traffic light state), traffic light state controller (when to change state and what state to change to), Attacker node

Controllers:

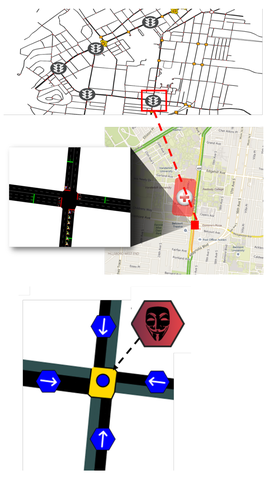
- **Queue Based State Controller -** Manages traffic light state based on number of detected waiting vehicles at specific directions (Min Green Time: 30 s) (Max Green Time: 120 s)
- **Fixed Time Controller** – Manages traffic light state based on a fixed schedule

Vulnerability: Buffer Overflow vulnerability in queue based state controller when receiving data from sensors.

Attack model: Inject malicious payload into state controller through sensor spoofing. Payload opens a remote root shell to the attacker, allowing them to run a malicious fixed time state controller with a significant green time for the non critical route (East-West).

Attacker Goal: Create backup on critical route (North-South)

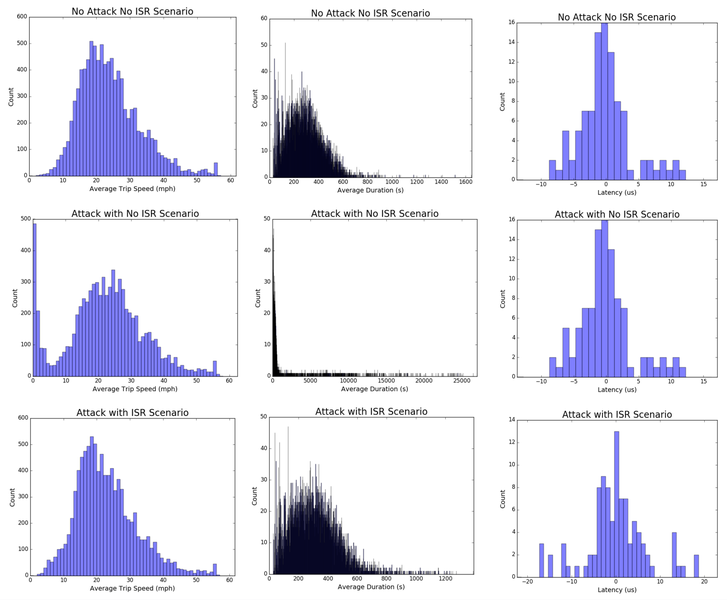
Metric: Average Trip Speed, average trip duration



<u>No Attack and No ISR</u>
Average Speed: 23.9 mph
Average Duration: 285.60 s
Mean Period Latency: -.0010 us
Std Period Latency: 3.82 us

<u>Attack and No ISR</u>
Average Speed: 22.1 mph
Average Duration: 1168.42 s
Mean Period Latency: -.0011 us
Std Period Latency: 3.97 us

<u>Attack and ISR</u>
Average Speed: 22.94 mph
Average Duration: 306.76 s
Mean Period Latency: -.08 us
Std Period Latency: 6.85 us



Performance Overhead

No ISR Average: 80.118 ns

ISR Average: 83.010ns

Overhead: 3.7%

No ISR STD: 33.710ns

ISR STD: 35.252 ns





Summary

- An ISR based framework was developed to mitigate the effects of code injection attacks
- By switching between controller designs at attack time, system crashing is prevented.
- There exists performance overhead at load time for ISR but execution time overhead is minimal, making the effect on real time constraints minimal

Ongoing Work

- Exploration of address space and data space randomization techniques
- Assessment of MTD strategies on automobile safety and security.

This work was supported by the AFRL SURE Program. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not reflect the views of AFRL.

HoTSoS *Symposium and Bootcamp*

HOT TOPICS *in the* **SCIENCE OF SECURITY**

APRIL 4-5, 2017 | HANOVER, MARYLAND