Integrated Data Space Randomization and Control Reconfiguration for Securing Cyber-Physical Systems

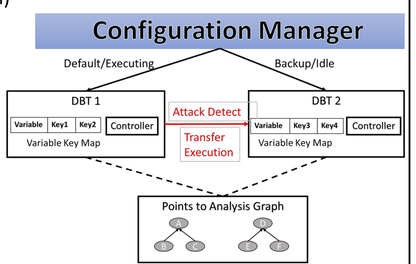
Bradley Potteiger, Feiyang Cai, Zhenkai Zhang, and Xenofon Koutsoukos
Institute for Software Integrated Systems, Vanderbilt University

Motivation

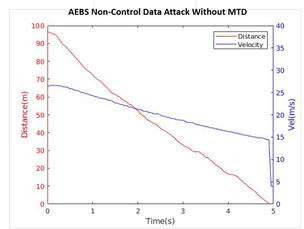
- CPS-IoT are increasingly subjected to sophisticated cyber-attacks
- Several high profile autonomous vehicle accidents demonstrate the tightly coupled nature between the CPS software and physical dynamics
- Non-control data attacks have become a primary memory corruption exploit utilized to compromise CPS safety and behavior
- CPS not only have to maintain integrity while under cyber attacks, but also need to ensure safe operation

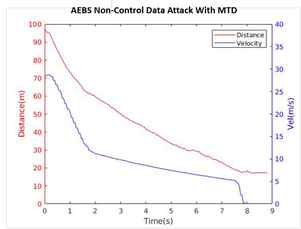
Testbed

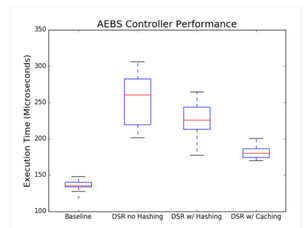
- Autonomous Vehicles
  - Sensors, actuators, cyber infrastructure
  - Rich interaction with the physical world
- Hardware Testbed
  - Controller Board – NVIDIA Jetson TX2
  - Network interfaces
    - 100 Mbps Ethernet
    - ZeroMQ Communication Library
- Simulation Environment
  - CARLA– Open source autonomous vehicle simulator (Physical Domain)
  - MTD Framework – Encapsulates controllers on NVIDIA Jetson TX2
    - Configuration Manager – Oversees attack detection and reconfiguration process
    - Dynamic Binary Translator (DBT) – Creates MTD virtualized environment for DSR implementation. Sandboxes vulnerable application
    - Points to Analysis Graph – Contains instruction and memory relationships

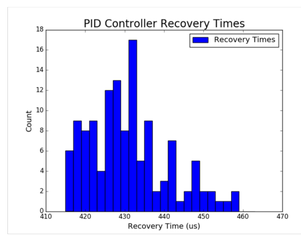


Results

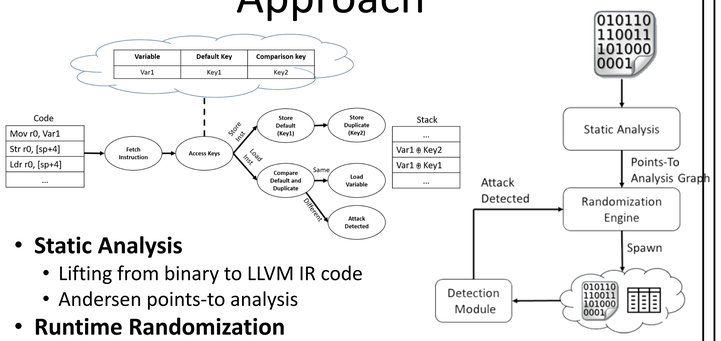








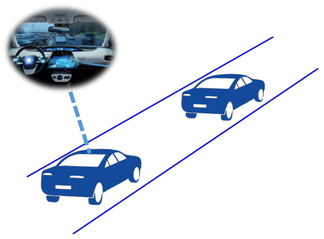
Approach

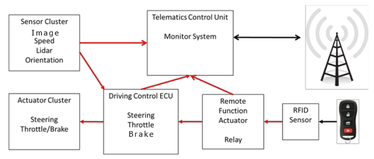


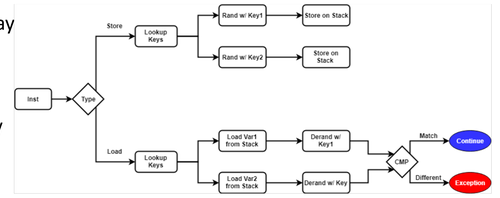
- **Static Analysis**
  - Lifting from binary to LLVM IR code
  - Andersen points-to analysis
- **Runtime Randomization**
  - Variable randomization table stores two unique keys for every utilized memory location
  - When stored to memory, variable will be replicated, leaving two uniquely randomized variable instances stored in memory
  - When loaded from memory, the variables are derandomized with their respective keys, and compared for equality
- **Control Reconfiguration**
  - When a variable equality check fails, a variable integrity violation has occurred, and the recovery process starts
  - Execution will be transferred to a backup controller with a different randomization environment

Case Study

- Scenario: 2 vehicle scenario
  - **Leader:** Vehicle stopped at traffic light
  - **Follower:** Autonomous vehicle with Advanced Emergency Braking System
- Controllers:
  - **Neural Network Controller –** 3 layer neural network.
  - **Emergency Controller –** Applies full break
- Vulnerability: Buffer overflow vulnerability in controller input processing function from remote function actuator
- Attacker Process:
  - Gain access to vehicle network by compromising telematics control unit through remote cellular interface
  - Spoof a false Remote Function Actuator packet and transmit to the neural network controller
  - Utilize buffer overflow vulnerability to alter critical variables
- Attacker Goal:
  - Non-control data attack to alter the stored distance local variable in the neural network controller
  - Tricks controller into believing the stopped car is farther away than it actually is
  - Results in autonomous vehicle crashing into the back of the stopped vehicle
- Defender Goal: Detect the attack. Recover to the backup Emergency Controller
- Metric: Vehicle speed and distance from the stopped vehicle, reconfiguration time







Broader Impact

- An automotive hardware in the loop testbed allows for analyzing ECU and internal network behavior in environments similar to deployment.
- MTD techniques limit adversary reconnaissance knowledge by dynamically changing various system properties.
- DSR implementations protect against non-control data attacks, but reconfiguration mechanisms are critical to ensure safe vehicle operation.
- Different controller architectures limit the probability of a subsequent cyber-attack through the same attack vector.

2019 NSF Cyber-Physical Systems Principal Investigators' Meeting
November 21-22, 2019 | Crystal City, Virginia

Website: https://cps-vo.org/group/mtd

Award ID#: CNS-1739328