CPS: synergy: collaborative research: Support for security and safety of programmable IoT systems PIs: Atul Prakash, University of Michigan Darko Marinov, University of Illinois





Objectives

Detect and prevent bugs in ioT applications. Risks:

- IoT device failures and compromises
- Attacks on other devices in an IoT network

Approach

- Provide an application testing framework
- Provide a security layer to monitor application-level events



System Architecture Controllers ontrole Module 1: No Create a virtual device ive requests from Module 2 Module 2 ¥ handle request or reject Module N IoT apps Log requests OAuth 2.0 over CoAP Device: OAuth 2.0 over CoAP Get/Put/Post IoTivity Cloud Server Database MySQL Cloud Interfac requests requests request_id request_type status device_attr1 device_attr2 device_attr3 primary ke Message Queue fieldname Resource Directory time timestamp success boolear

Safety Enforcement

- Developed an application server (controlee) that
 enforces security policies
- Initial prototype implemented that detects attempts to cause device failures by sending requests at high rates
- Validated using virtual devices with and without protection

Future Plan

- Create automated tests
- · Extend the set of policies
- Provide as a library that can be integrated into apps on devices or deployed in the cloud or a hub
- Develop device-specific fuzzing techniques to test IoT application code on the devices
- Simulate attacks to test the robustness of the rejection policies