SAND2019-8322D

DARPA ConSec

Victoria Zheng
Mentor: Jason Gao

Mission Statement

Develop a system to automatically generate, deploy, and enforce secure configurations of components and subsystems for use in military platforms.

- DARPA ConSec (Configuration Security)

Background

Internet of Things (IoT) devices have exploded in popularity and use in recent times. Development of devices outpaces IoT security research (which is often not the priority) and as a result, most off-the-shelf devices on the market are extremely vulnerable to common attacks.

Examples of IoT devices: Smart lock, internet-connected camera, smart fridge, FitBit

Common IoT Vulnerabilities and Exploits:

- Weak default passwords – easy to brute force
- Hard-coded admin passwords in source code
- Denial of Service (DoS)
- Unencrypted and open network of IoT devices: network traffic could easily be intercepted to steal information
- Replaying of control signals

Results

- Instrumented inputs and outputs for virtual heaters, cooling units, water supply, and other sensors needed for a complete scenario simulation
- Engineered a realistic and compact simulation environment in hardware and software
- Constructed, delivered, and deployed to various performer sites nationwide

Goal

Design and create testbeds consisting of commercial IoT devices to simulate a real, functioning enterprise, on which performers will develop an automated configuration system to optimally secure it.

Simulation Scenario

A fictional company is running a lucrative algae bioreactor enterprise which utilizes a system of interconnected Internet of Things (IoT) devices to control and maximize production.

Devices

- Internet Protocol (IP) Camera
- BrewPi & RaspberryPi
- OpenSprinkler Pi
- ICS (Industrial Control System) Network
- Central Controller Arduino

U.S. DEPARTMENT OF ENERGY
NNSA National Nuclear Security Administration

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.
SAND No. _____

Sandia National Laboratories