Composing Capability-Based Rules for Securing IoT Devices

Yunhan Jack Jia and Z. Morley Mao, University of Michigan

New Trends in IoT Industry

- Third-party IoT app markets are emerging
- Samsung’s SmartThings
- Apple’s HomeKit
- Google’s Weave/Brillo
- Vera Control’s Vera3
- AllSeen Alliance’s AllJoyn
- Security threats come from both vulnerable device and vulnerable apps, e.g.,
  - Honeywell home controller vulnerability
  - Backdoor Pin Code Injection attack [Fernandes et al., S&P’16]
- The signature of such attacks is:
  - The malicious usage of the IoT devices/apps are beyond their declared functionality.
- Solution:
  - Using SDN to enforce the security policy among IoT devices.

Challenges:

- The varying nature of third-party app support making policy enforcement difficult:
  - New security policy abstraction is required
  - Hard for device administrator to specify proper security policies. [HotNets’15]
- Call for a more flexible and automatic approach to enforce security policy

Composing Capability-Based Rules from IoT Apps and Update Automatically

```
Auto-DoorLock App

section ("Lock the door when no motion")
{
    input (motionSensor, capability.motionSensor)
    input (doorLock, capability.lock)
}
subscribe (motionSensor, "motion.inactive", handler)
def handler(event)
{
    doorLock.lock()
}
```

*SmartThing app in Groovy language as an example

Example: Generating security policy when installing an IoT app that enables automatic locking the door when everyone has left the room.

Case Study

**Attack:** backdoor pin code injection
- Vulnerable app opens web interface to take remote command
- Attacker exploits the dynamic feature of the language to execute command beyond the app's functionality.
  - Declared functionality: capability.battery
  - Dynamic feature being exploited: device.'$command'
**Defense:**
- Generate SDN rule that only allows the app to obtain battery info from the lock.

Next step

- Investigate if the design is applicable to the major IoT platforms that supports 3rd party app.
- Is the threat model valid?
- Does the static analysis approach applicable?
- Does the platform support the capability-based access control?
- System implementation
- SDN rule generalization
- Rule update overhead optimization