An Architectural Mechanism for Resilient IoT Services

Hokeun Kim¹, Eunsuk Kang¹, David Broman², Edward A. Lee¹

¹University of California, Berkeley
²KTH Royal Institute of Technology

SafeThings 2017
November 5, 2017

Sponsored by the TerraSwarm Research Center, one of six centers administered by the STARnet phase of the Focus Center Research Program (FCRP) a Semiconductor Research Corporation program sponsored by MARCO and DARPA.
Safety and Security of the IoT

- Safety & Security: No longer separate issues!


https://www.lightbluetouchpaper.org/2017/06/01/when-safety-and-security-become-one/
Availability and Safety

• Shutting down critical IoT services can cause disastrous problems!
  – Power grids
  – Hospitals
  – Transportation
  – many more…


How do we design an IoT network to be resilient against availability & other types of attacks?
Cloud & Edge Computing

- Many existing IoT solutions are based on clouds
- Alternative emerging architecture: **Edge Computing**

### Cloud servers
- More available resources
- Higher latency
- Less stable connections
- More challenging to guarantee data privacy
- Limited context awareness (of local system)

### Edge computers (Internet gateways)
- Restricted resources
- Better connectivity
- Lower latency
- Greater control over data
- Better context awareness (of local system)

### IoT devices (Things)
Secure Swarm Toolkit (SST)

- Locally centralized, globally distributed architecture
SST Overview

- **Auth**
  - Software solution deployed on edge devices
  - Local authentication/authorization entity
  - Responsible for authorization of local Things through key distribution
  - Manages trust relationship with other Auths
Challenges in Securing the IoT

- Authentication/Authorization
- Heterogeneity
- Open environment
- Scalability
- Availability

Addressed in this paper

[*] “A Toolkit for Construction of Authorization Service Infrastructure for the Internet of Things”, ACM/IEEE IoTDI ’17, CPSWeek
Threat Model

• Attacker Capabilities
  – Disrupt IoT services by targeting edge devices
  – DoS attacks (packet flooding, etc.)

• Assumption
  – Some subset of edge devices exposed to attacker

Our Goal
Provide services to Things even in the presence of attacks on some Auths
Proposed Approach

- A trusted Auth takes over authorization tasks of a failed Auth

Original topology

Current SST

Auth (on edge computer)
Entity (on IoT device)

$t_j$ is authorized by $A_i$

Trust between Auths
Communication between entities

Idea: Secure Migration
Migration Policies

- Which Auth should each Thing be migrated to?
- Non-trivial! Hard constraints & alternative costs

When $A_1$ fails, migrate $t_4$ from $A_1$ to $A_2$

$t_4$ can't communicate with $t_5$ after migration

$A_1$'s signal range  $A_2$'s signal range

$A_1$'s signal range  $A_2$'s signal range

• Which Auth is directly reachable through wireless communication?
• Is Auth equipped with HW security support (e.g., TPM or Intel SGX)?
• Is Auth located in a restricted-access area?
Migration Policy Construction as ILP

- Computing a migration policy as an optimization problem!
  \[
  \begin{align*}
  &\text{minimize} & & c^T x \\
  &\text{subject to} & & Ax \leq b
  \end{align*}
  \]

- Formulation in Integer Linear Programming (ILP)
  - Variables: Boolean, set true if Thing X assigned to Auth Y
  - Coefficients: Communication costs
  - Constraints:
    - Thing-Thing communication requirements
    - Auth/Auth trust relationships
    - Auth capacity: Max # Things for each Auth

More details in paper!
Preliminary Experiment

- Application: Smart Door Control through Mobile App

Simulation environment:
- 4 Auths, 19 door controllers, 26 apps
- Implemented & running on Linux Containers
- ns-3 for simulating wired & wireless communication
- Gurobi as the ILP solver

Floor map of 5th floor Cory Hall, UC Berkeley
Experimental Results

- Measuring availability (i.e., “open door” request accepted) when different numbers of Auths fail
  - Three different migration cases
Summary

• Edge-based architecture has certain advantages over cloud-based security solutions

• Proposed migration approach is promising for higher availability under failures of some edge computers
  – Suitable for safety-critical environments

• Computing migration policy can be formulated as an ILP problem
Future Work

• Scalability: For large networks, ILP may become too complex (on-going work)
• Hybrid solution for better availability (Auths on both clouds & edges)
• Theoretical bounds & resiliency analysis depending on network topology
• Advanced threat model
  – Selectively attack Auths to maximize damage (instead of random DoS)