SCC
(Security Control Center)

Presented by *Junyoung Jung*

Mobile & Embedded System Lab.
Dept. of Computer Engineering
Kyung Hee Univ.

Computer Engineering in KyungHee University
Mobile & Embedded System Lab.

Contents

- Motivation
- Related works
- Proposed System
- SCC: Security Control Center
- Demonstration

Motivation

Recent Trends

- Accelerated the launch of a variety of IoT products & services
- Increased interest in IoT device security issues

Problems

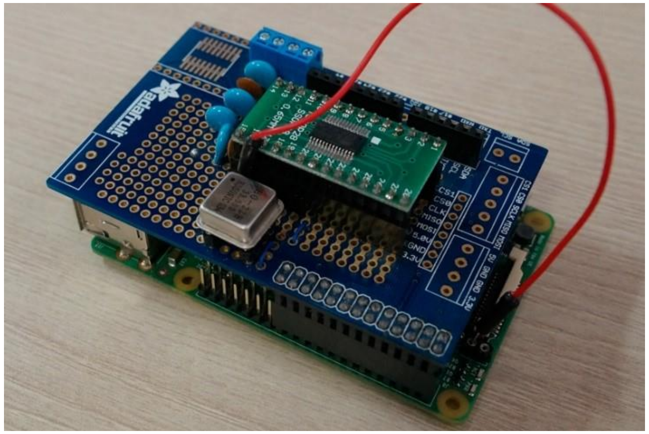
- Manufactured without considering security level
- Absence of a security control system
  - Difficult to respond to security attacks

Need for a Security Control System

(Collecting and Analyzing the information about security attacks.)

Related works

- **SecurePi: Secure Raspberry Pi (Using TPM*)**
  - Linux based high-end secure COTS IoT device platform
    - ① Secure Key Storage & Management
    - ② Secure Boot
    - ③ Secure Firmware Update
    - ④ Remote Attestation
    - ⑤ Secure Communication
    - ⑥ Mandatory Access Control
    - ⑦ Filesystem Integrity
    - ⑧ Filesystem Encryption



*TPM : Trusted Platform Module

Related works

- **SArduino: Secure Arduino (Using SE*)**
  - RTOS/Firmware based Low-end secure COTS IoT device platform
    - ① Secure Key Storage & Management
    - ② Secure Boot
    - ③ Secure Firmware Update
    - ④ Remote Attestation
    - ⑤ Secure Communication

*SE : Secure Elements

Proposed System

❖ Functional requirements (for performing Security Controls)

① Ensure availability of sensitive data

- Storing and managing the encryption key data in TPM/SE
- **Secure Key Storage & Management Monitoring**

② Ensure F/W integrity (Secure Boot)

- Firmware replacement attacks prevention
- **Secure Boot Monitoring**

③ Ensure secure F/W update

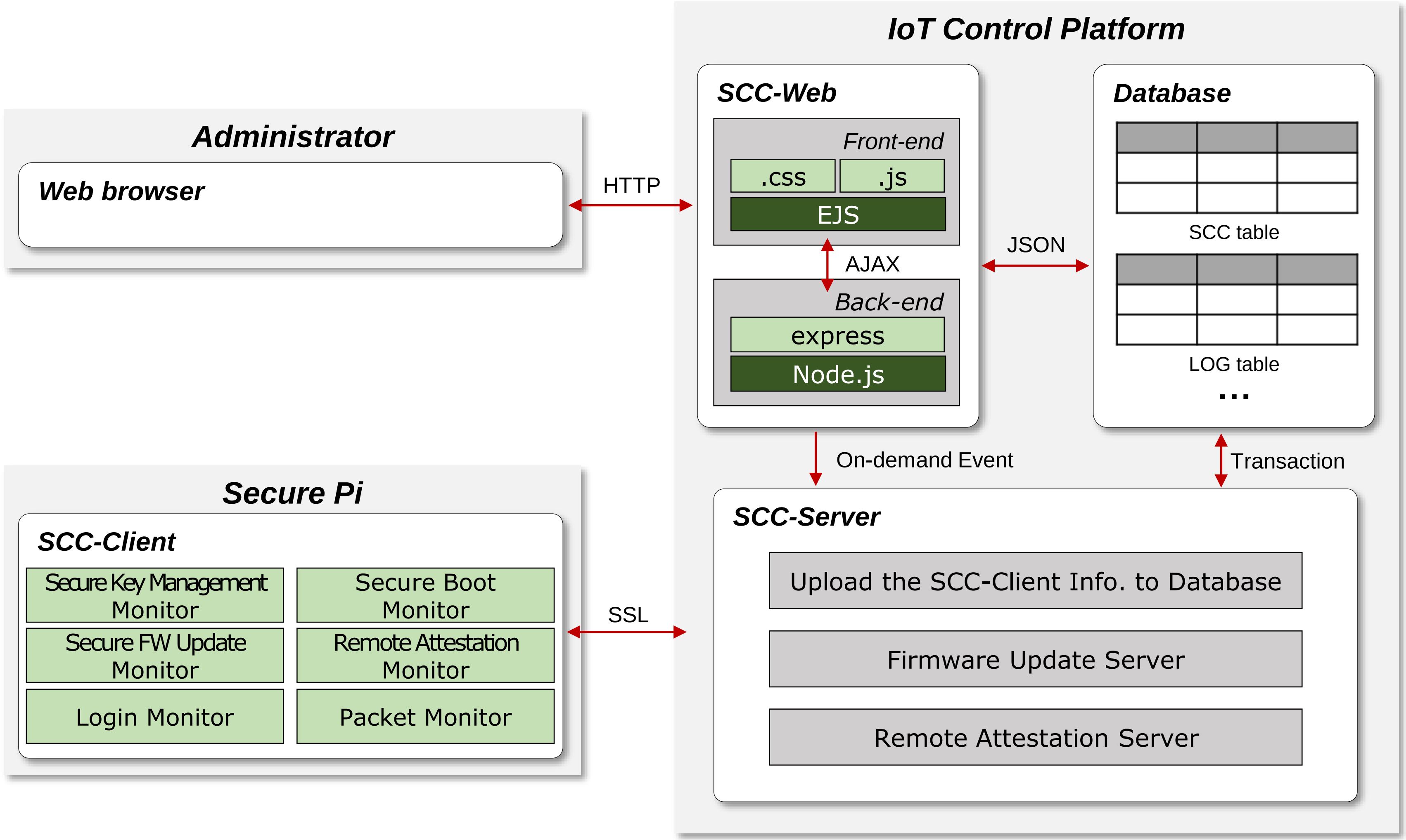
- The previous versions of firmware install prevention
- **Secure Firmware Update Monitoring**

Proposed System

- **Functional requirements (for performing Security Controls)**
  - ④ Ensure F/W integrity (Remote Attestation)
    - Firmware replacement attacks prevention through other device
    - **Remote Attestation Monitoring**
  - ⑤ Detect the device login attempt
    - Checking the login log(*/var/log/auth.log*) periodically
    - **Login Monitoring**
  - ⑥ Detect the device allow/deny packet
    - Checking the *iptables* log periodically
    - **Packet Monitoring**

SCC: Security Control Center

System Architecture



Demonstration

- http://163.180.118.193:3000

① Device registration

② Device detail view

③ Device Firmware Update

- Secure Key Storage & Management
- Secure Boot
- Secure Firmware Update
- Remote Attestation

④ Login & Packet Monitoring

Thank you