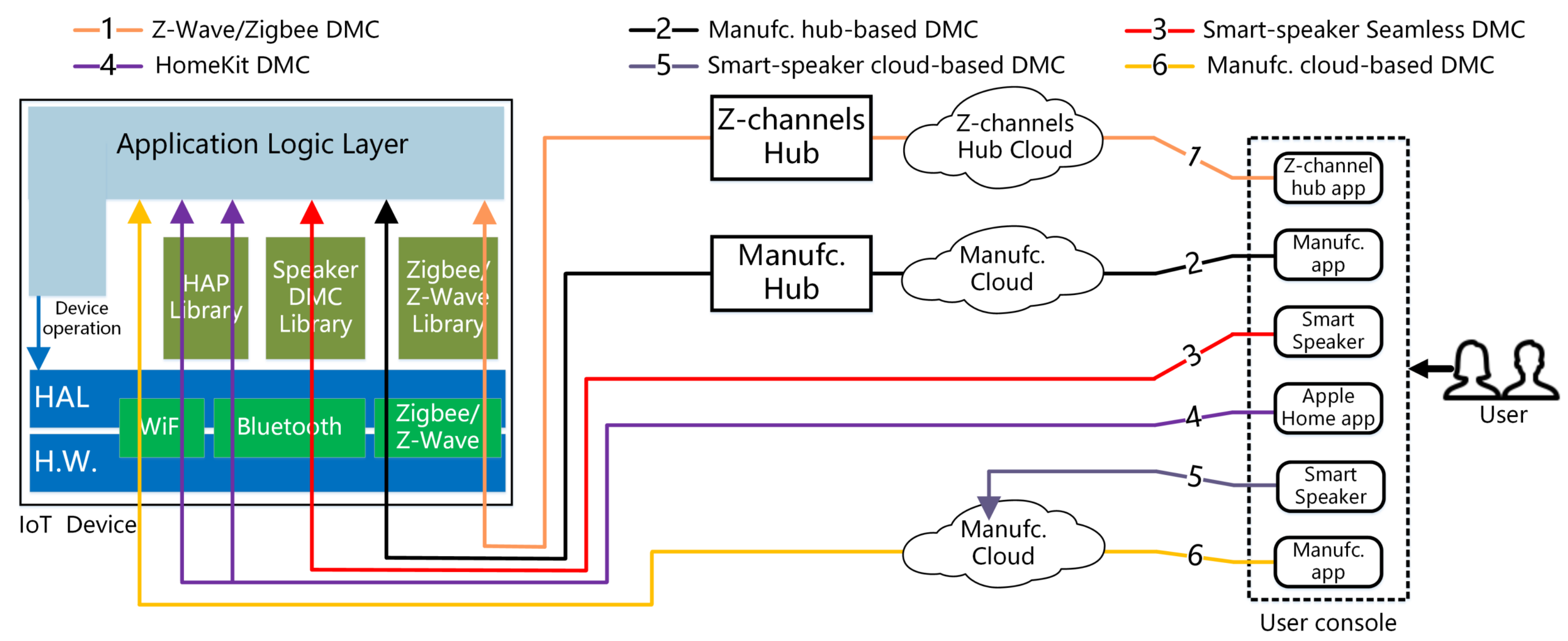
Poster: Who's In Control? On Security Risks of Disjointed IoT Device Management Channels

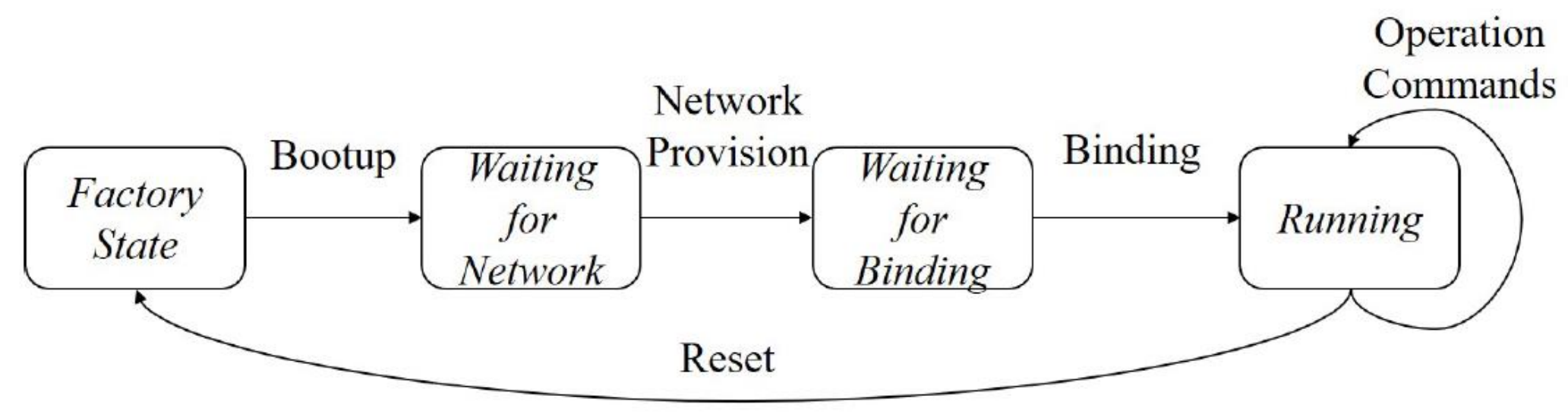
Yan Jia, Bin Yuan, Luyi Xing, Dongfang Zhao, Yifan Zhang, XiaoFeng Wang,
Yijing Liu, Kaimin Zheng, Peyton Crnjak, Yuqing Zhang, Deqing Zou, Hai Jin

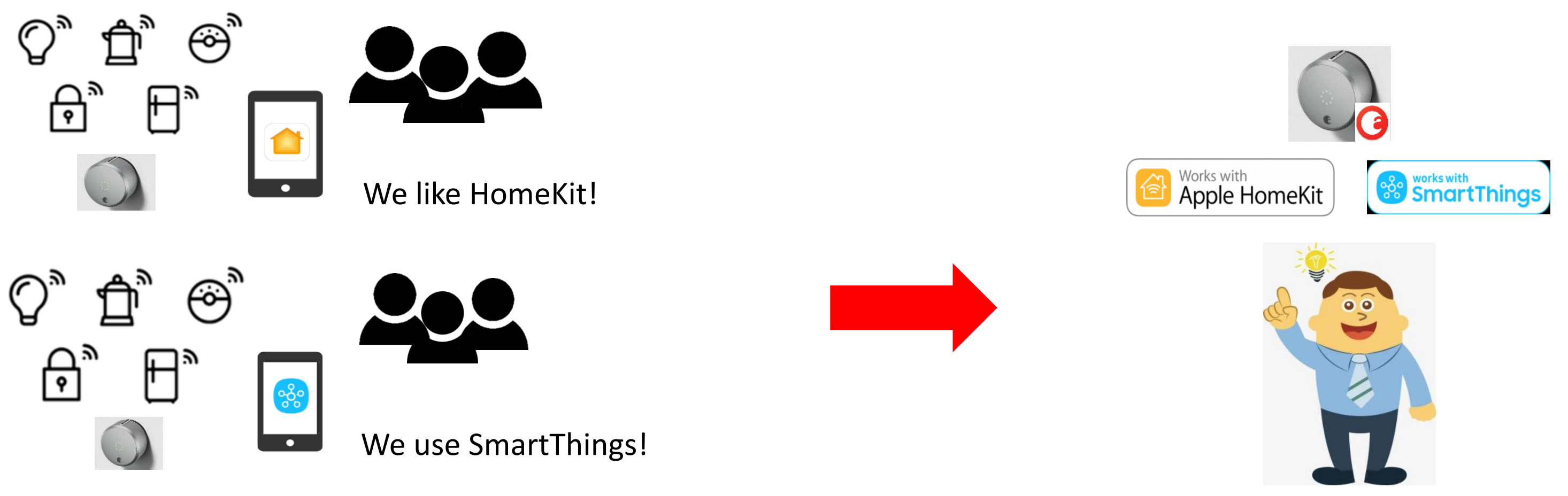
Device Management Channel

- Device Management Channel (DMC)： user console, the IoT cloud, hub, and the on device software stack



- Each DMC is a standalone system and fully controls the device.

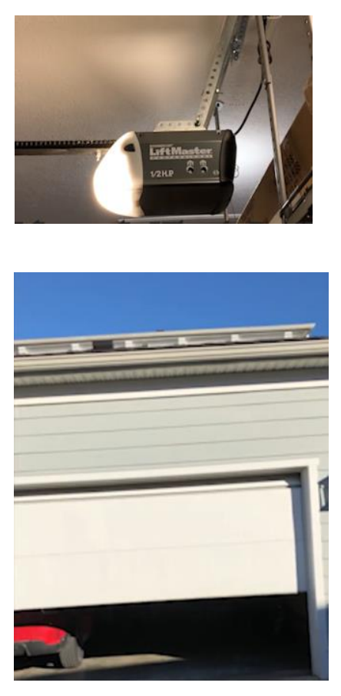


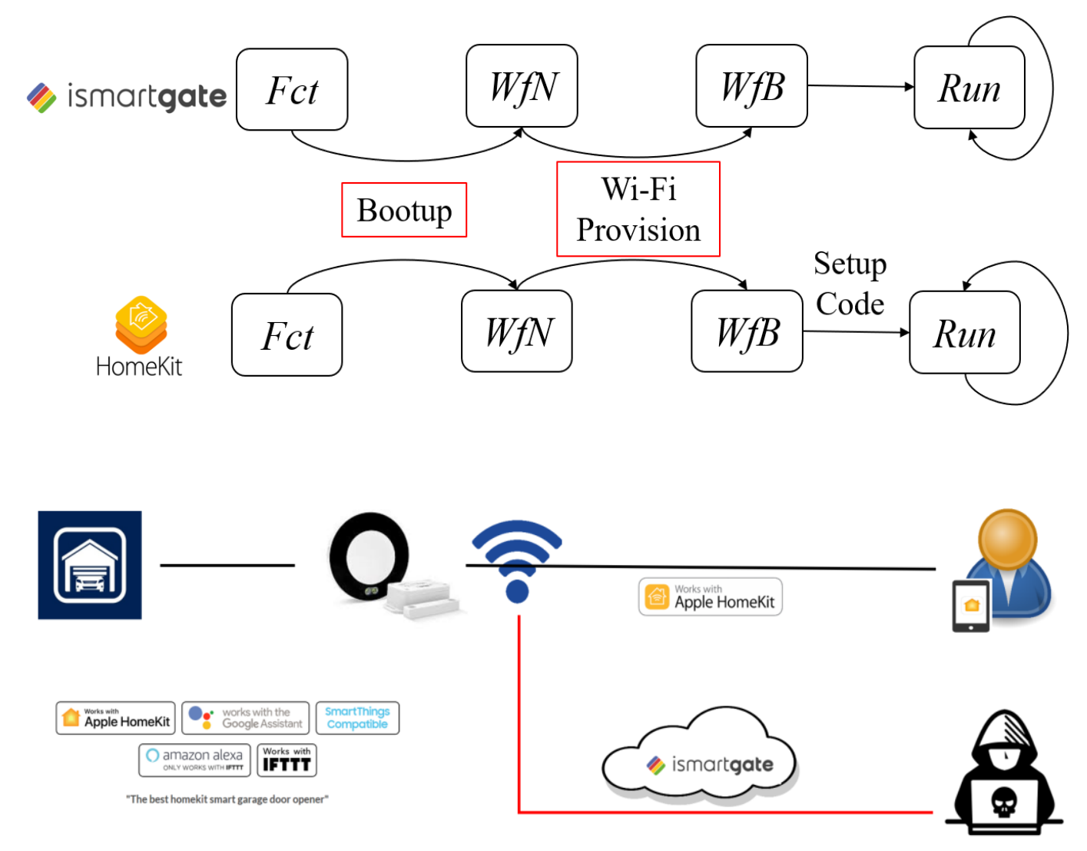


Understanding Codema

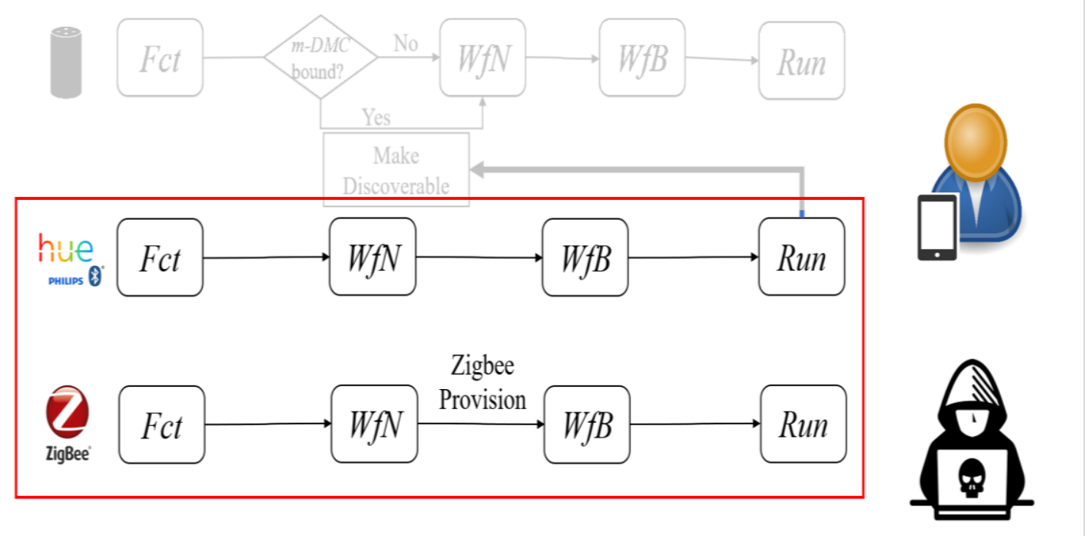
- **Disjointed DMC Management**

➢ Case 1



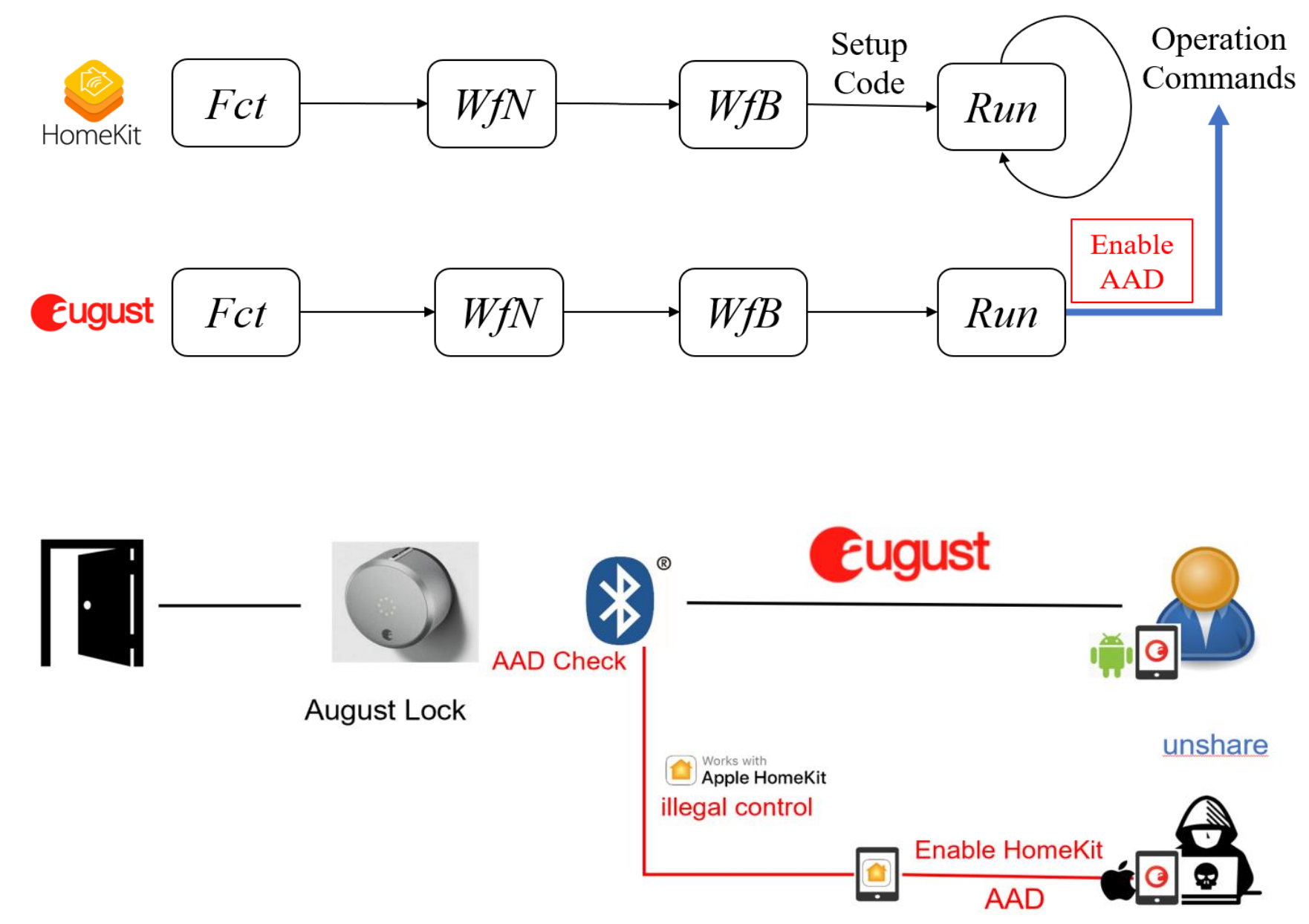


➢ Case 2

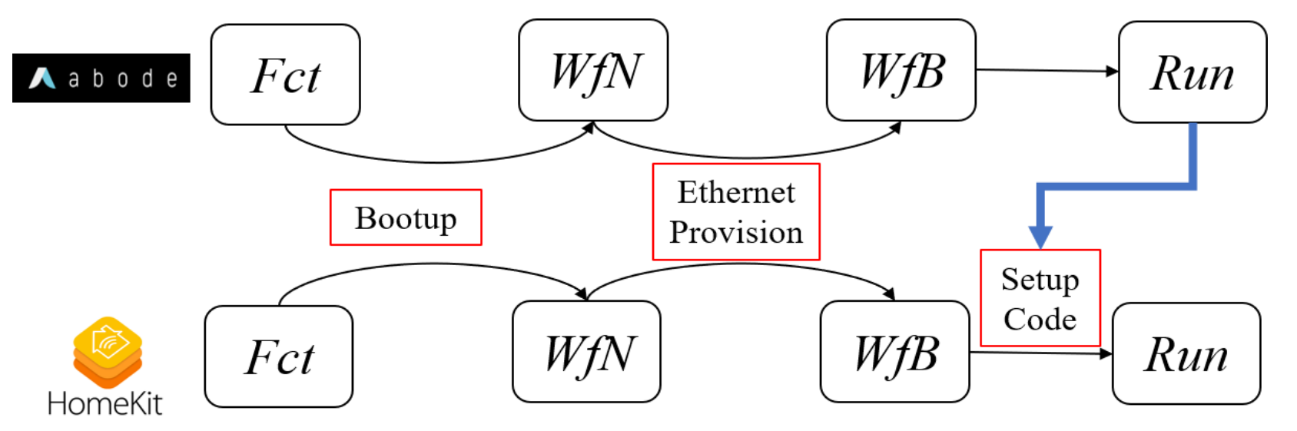


- **Disjointed DMC Management**

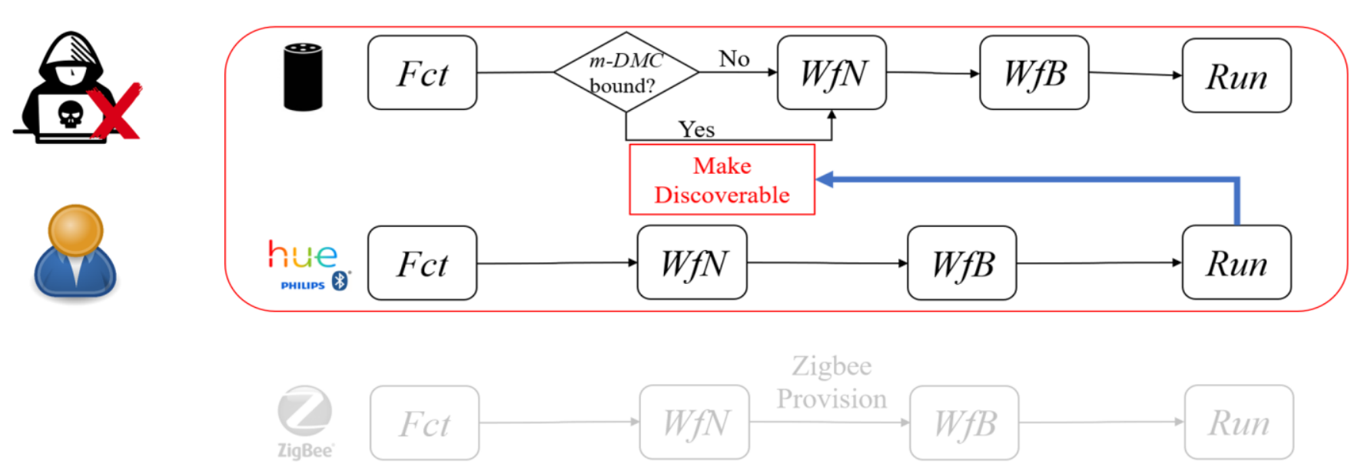
➢ Case 3



➢ Case 4



➢ Case 5



Attack Feasibility Analysis

- **User Perspective**
  - ➢ 83.3% users only sets one DMC.
    - 54.2%: < 5 min, 37.5%: 5-10 min
    - 50% do not know the device supports multiple DMC
  - ➢ Home Wi-Fi is usually shared with different people.
    - Airbnb：58.3%，Tennent：62.5%，Babysitter：62.5%
    - Years：33.3%，Never：45.8%
  - ➢ IoT devices are usually shared by owners.

- **Manufacturer Perspective**
  - ➢ Manual
    - No need to setup all.
    - No instructions for some DMCs
  - ➢ Mobile App

Mitigation

Ideal Solution

✓ Users can choose any DMC they like.

✓ Any a DMC can fully manage the Device.

Standardized cross-DMC management protocol

zigbee
ZWAVE
HomeKit
august
abode

Cannot wait!

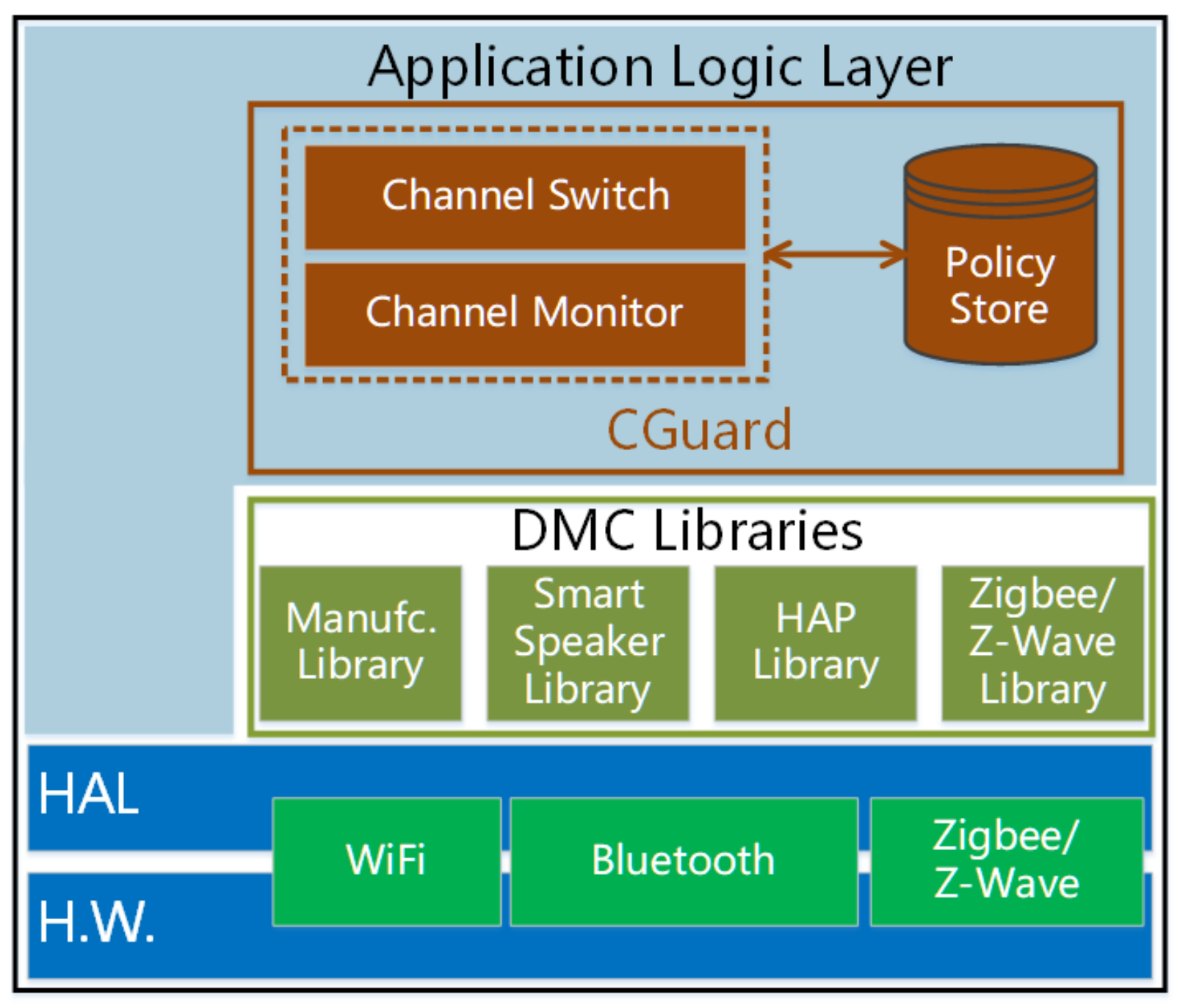
~~Ideal Solution~~ ➡ Fast Mitigation

Practical Fast Mitigation

✓ Owner can first choose any DMC.

✓ Owner can fully control the device's accessibility.

CGuard can be easily deployed by the manufacturer unilaterally.



南开大学 Nankai University
INDIANA UNIVERSITY BLOOMINGTON
西安电子科技大学 XIDIAN UNIVERSITY
华中科技大学
中国科学院大学 University of Chinese Academy of Sciences

Poster: Who’s In Control? On Security Risks of Disjointed IoT Device Management Channels

PUBLISHED PAPER

Title: Who’s In Control? On Security Risks of Disjointed IoT Device Management Channels

Authors: Yan Jia, Bin Yuan, Luyi Xing, Dongfang Zhao, Yifan Zhang, XiaoFeng Wang, Yijing Liu, Kaimin Zheng, Peyton Crnjak, Yuqing Zhang, Deqing Zou, Hai Jin
Email: jiay@nankai.edu.cn, yuanbin@hust.edu.cn, luyixing@indiana.edu, zhaodo@iu.edu, xw7@indiana.edu, yz113@iu.edu, liuyijing@mail.nankai.edu.cn, xbing010@163.com, pcrnjak@iu.edu, zhangyq@nipc.org.cn, deqingzou@hust.edu.cn, hjin@hust.edu.cn

Date: November 15–19, 2021
Venue: In Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security (CCS ’21)
DOI: https://doi.org/10.1145/3460120.3484592

ABSTRACT

An IoT device today can be managed through different channels, e.g., by its device manufacturer's app, or third-party channels such as Apple's Home app, or a smart speaker. Supporting each channel is a management framework integrated in the device and provided by different parties. For example, a device that integrates Apple HomeKit framework can be managed by Apple Home app. We call the management framework of this kind, including all its device- and cloud-side components, a device management channel (DMC). 4 third-party DMCs are widely integrated in today's IoT devices along with the device manufacturer's own DMC: HomeKit, Zigbee/Z-Wave compatible DMC, and smart-speaker Seamless DMC. Each of these DMCs is a standalone system that has full mandate on the device; however, if their security policies and control are not aligned, consequences can be serious, allowing a malicious user to utilize one DMC to bypass the security control imposed by the device owner on another DMC. We call such a problem Chaotic Device Management (Codema).

This paper presents the first systematic study on Codema, based on a new model-guided approach. We purchased and analyzed 14 top-rated IoT devices and their integration and management of multiple DMCs. We found that Codema is both general and fundamental: these DMCs are generally not designed to coordinate with each other for security policies and control. The Codema problems enable the adversary to practically gain unauthorized access to sensitive devices (e.g., locks, garage doors, etc.). We reported our findings to affected parties (e.g., Apple, August, Philips Hue, ismartgate, Abode), which all acknowledged their importance. To mitigate this new threat, we designed and implemented CGuard, a new access control framework that device manufacturers can easily integrate into their IoT devices to protect end users. Our evaluation shows that CGuard is highly usable and acceptable to users, easy to adopt by manufacturers, and efficient and effective in security control.