Codema Attack: Controlling Your Smart Home Through Dangling Management Channels

Yan Jia , Bin Yuan

black hat ASIA 2022

The 28th ACM Conference on Computer and Communications Security
ACM CCS 2021

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

南開大學
Nankai University

INDIANA UNIVERSITY
BLOOMINGTON

西安電子科技大學
XIDIAN UNIVERSITY

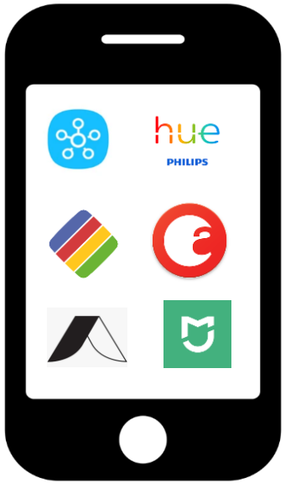
華中科技大學
HUAZHONG UNIVERSITY OF SCIENCE AND TECHNOLOGY

中国科学院大学
University of Chinese Academy of Sciences

Control

Control

Control



Too many apps!

HomeKit

zigbee

Z-WAVE

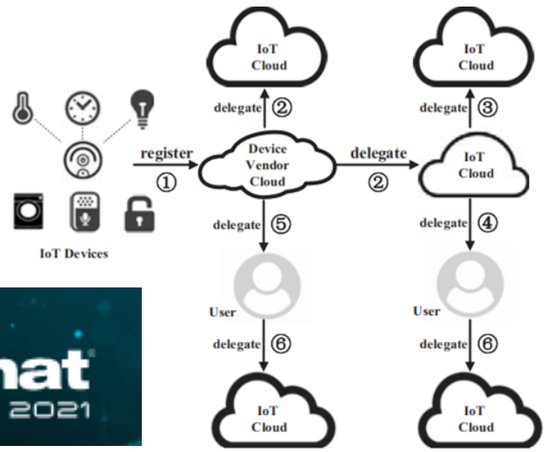
amazon alexa

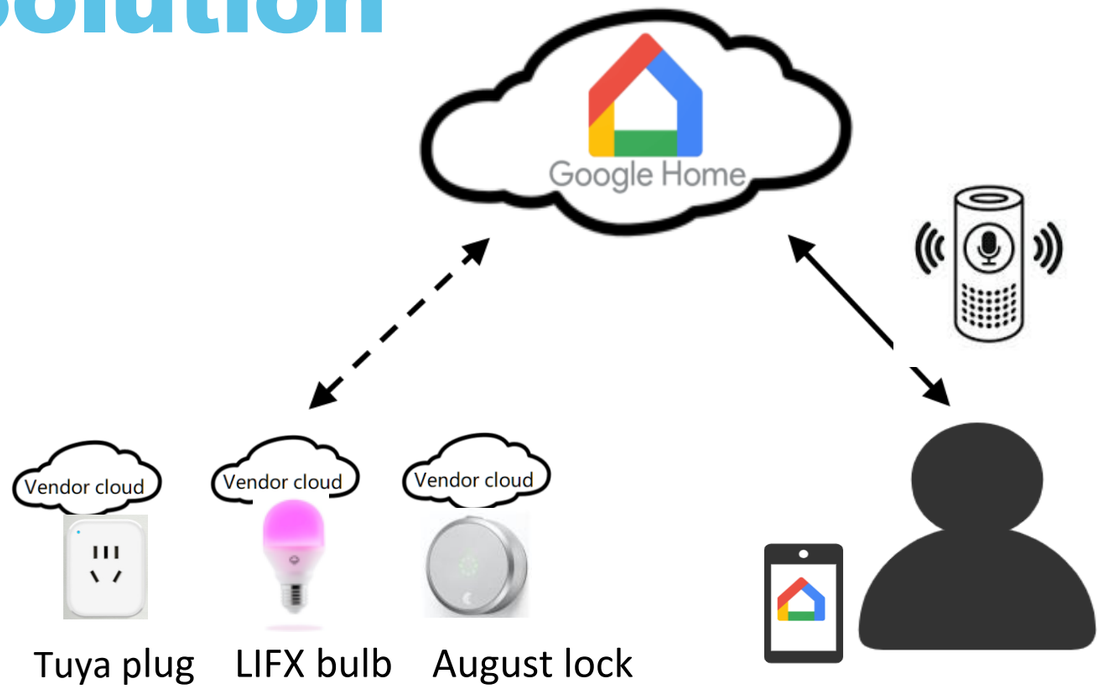
Google Home

Third-party Cloud Solution

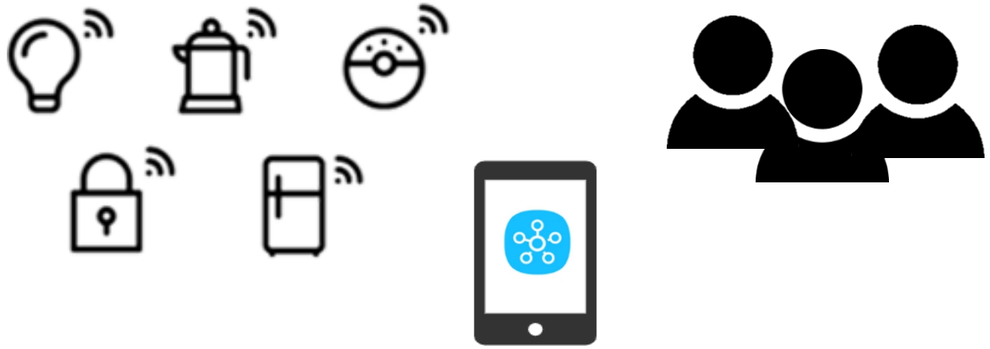
The risks hidden in the complex delegation chain were discussed in

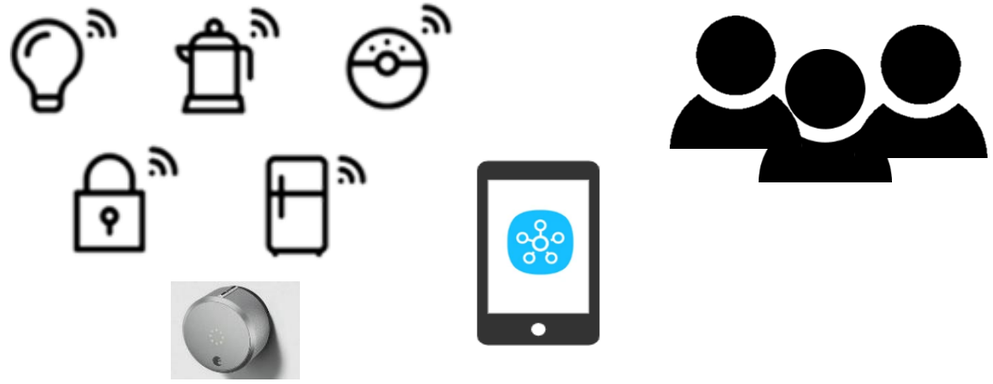
[Blackhat Aisa 2021-" How I Can Unlock Your Smart Door: Security Pitfalls in Cross-Vendor IoT Access Control"]





A user uses Google Home to control all her devices from different vendors





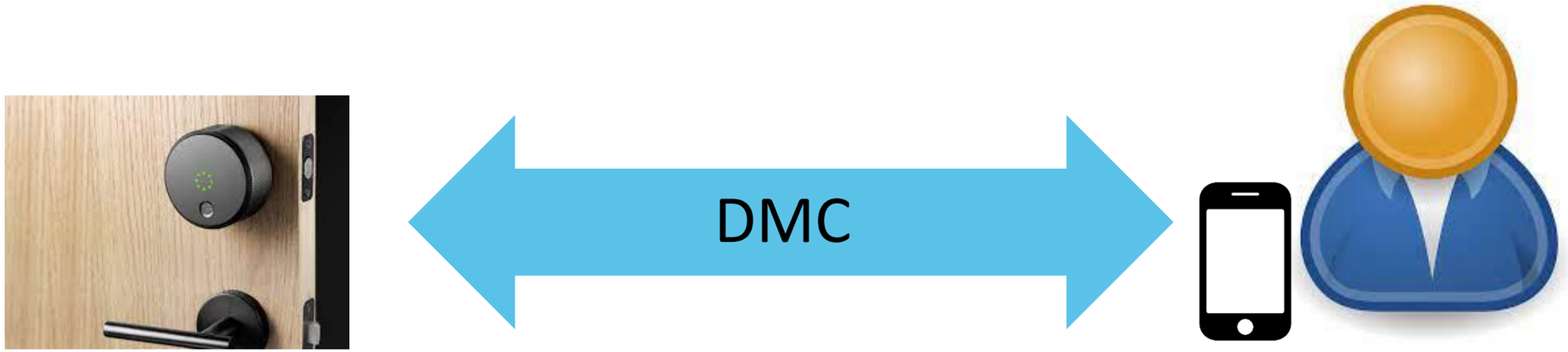
Works with Apple HomeKit

works with SmartThings

Integrating multiple
Device Management Channel!

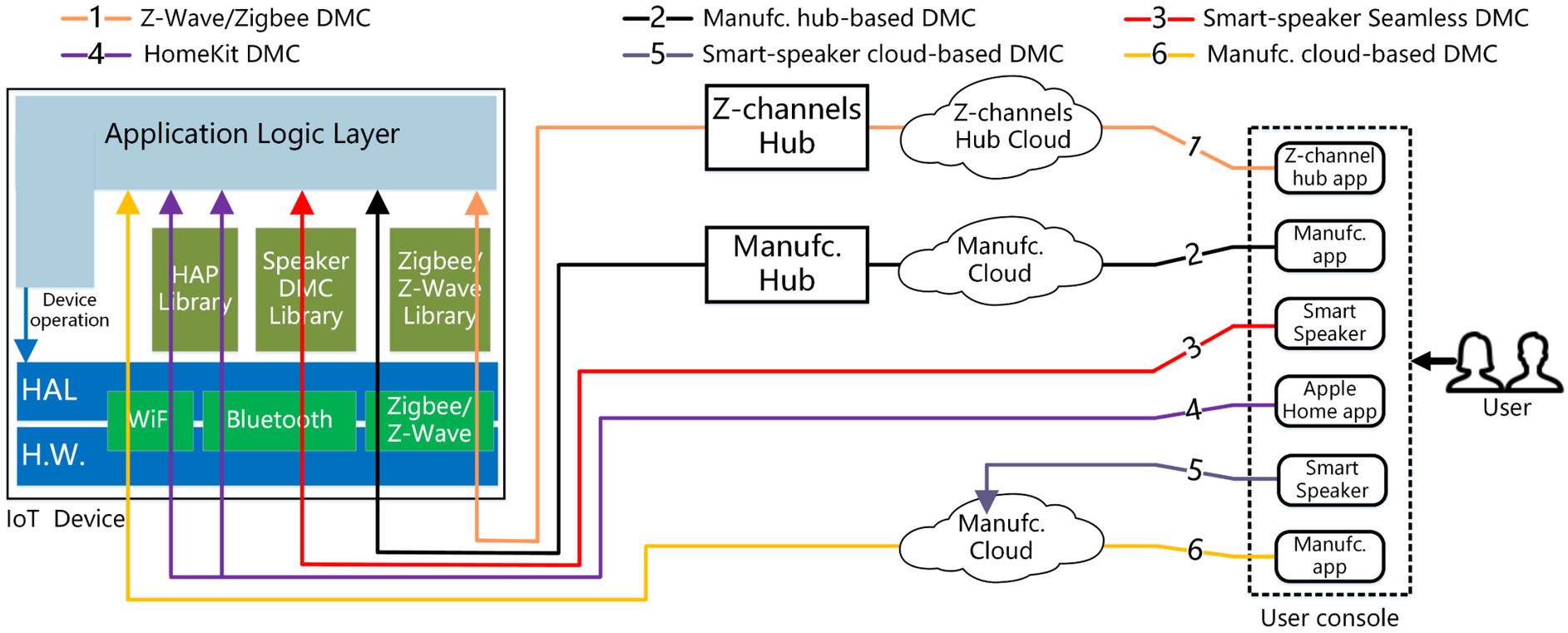
Device Management Channel (DMC)

On an IoT device, the user console, the IoT cloud, hub, and the on-device software stack together form the DMC to allow the user to manage the device.



Device Management Channels (DMC)

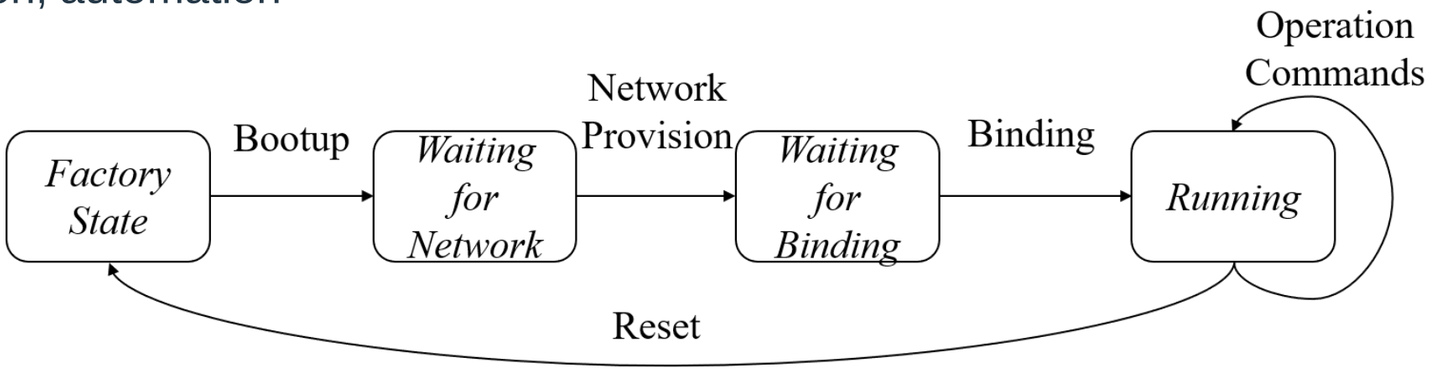
On an IoT device, the user console, the IoT cloud, hub, and the on-device software stack together form the DMC to allow the user to manage the device.



Device Management Channel (DMC)

Each DMC is a standalone system.

- Network Provision
  - Wi-Fi, Zigbee/Z-Wave hub, Bluetooth
- Binding
  - HomeKit setup code, physical button, automation
  - The first user is the owner.
- Running
  - Device control
  - User management



Device Management Channel (DMC)

Each DMC is a standalone system.

- Network Provision
  - Wi-Fi, Zigbee/Z-Wave hub, Bluetooth
- Binding
  - HomeKit setup code, physical button, automation
  - The first user is the owner.
- Running
  - Device control
  - User management

Integrating multiple
Device Management Channel!

Chao**t**ic **De**vice **Ma**nagement
(Codema)

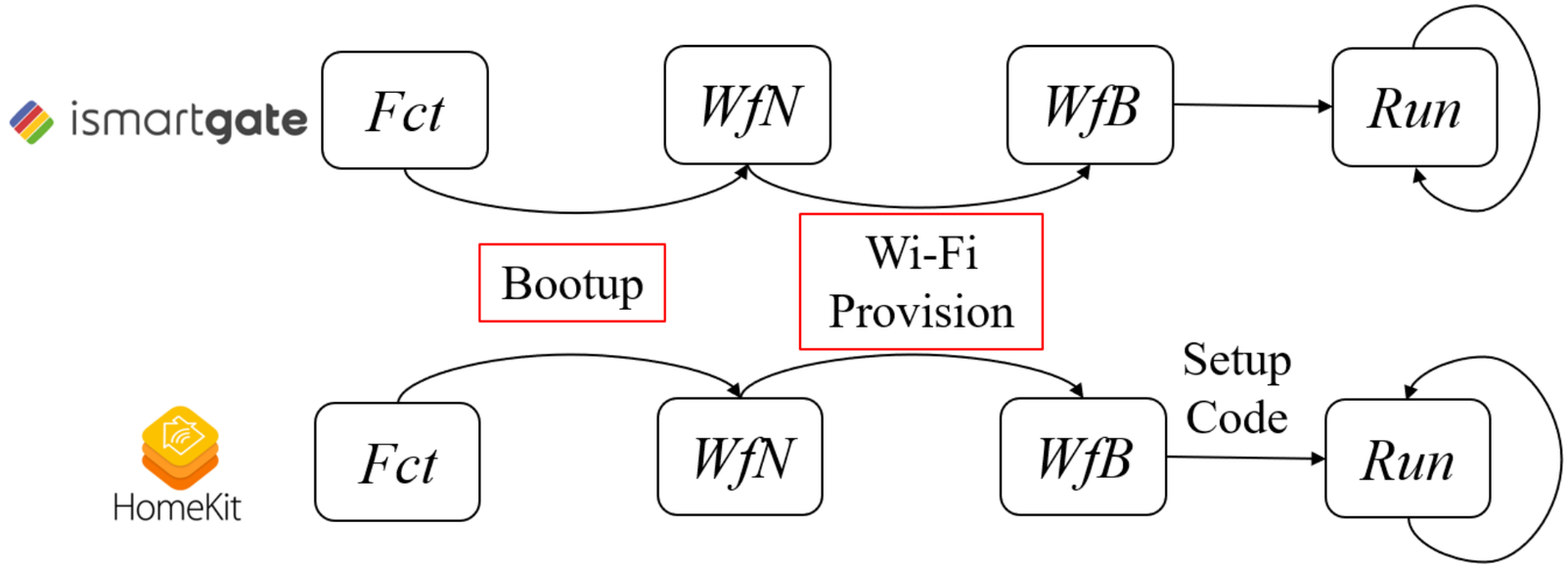
Codema Attack: Controlling Smart Home Through Dangling Management Channels

Demo Video

Understanding Codema

Disjointed DMC Management

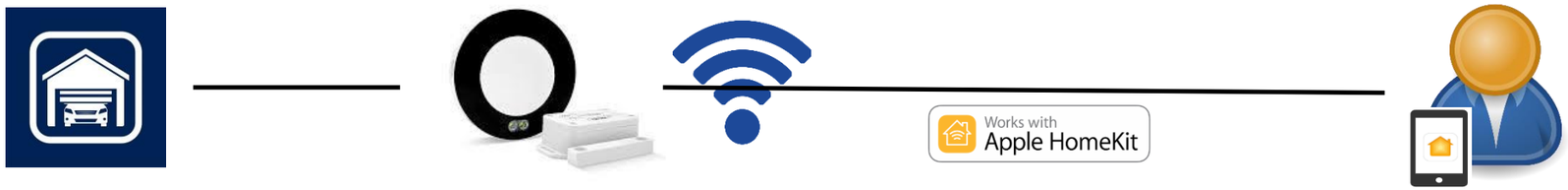
- Codema Flaw 1: Disjointed HomeKit and m-DMC

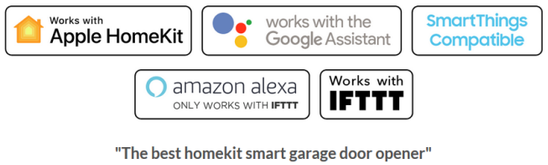


Understanding Codema

Disjointed DMC Management

- Codema Flaw 1: Disjointed HomeKit and m-DMC

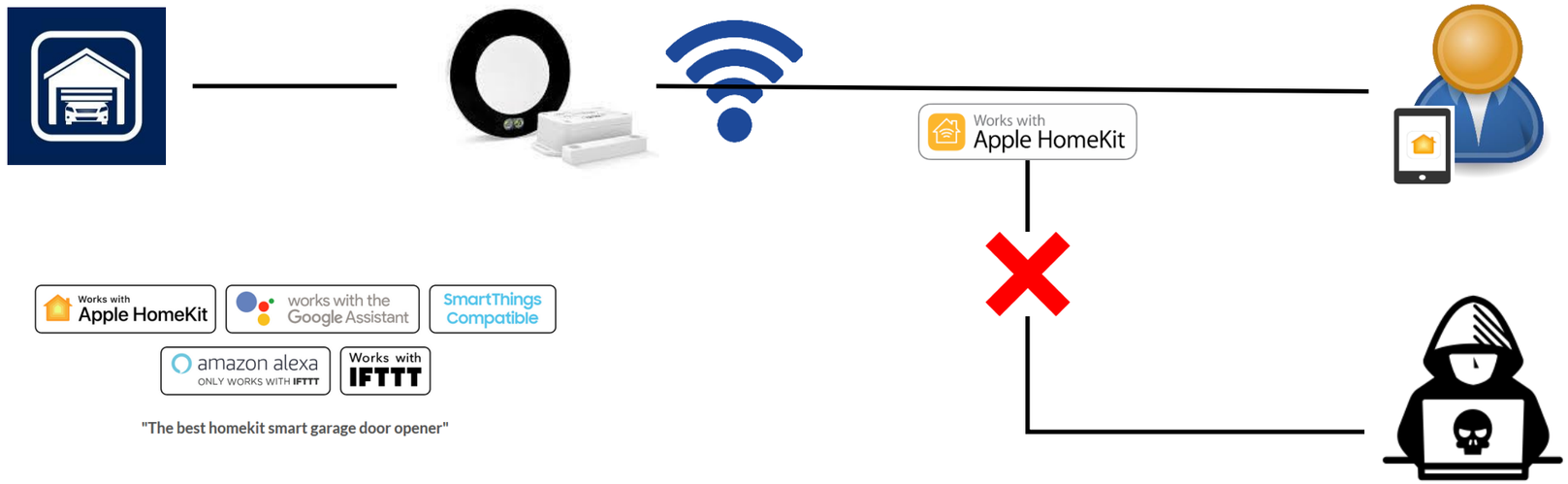




Understanding Codema

Disjointed DMC Management

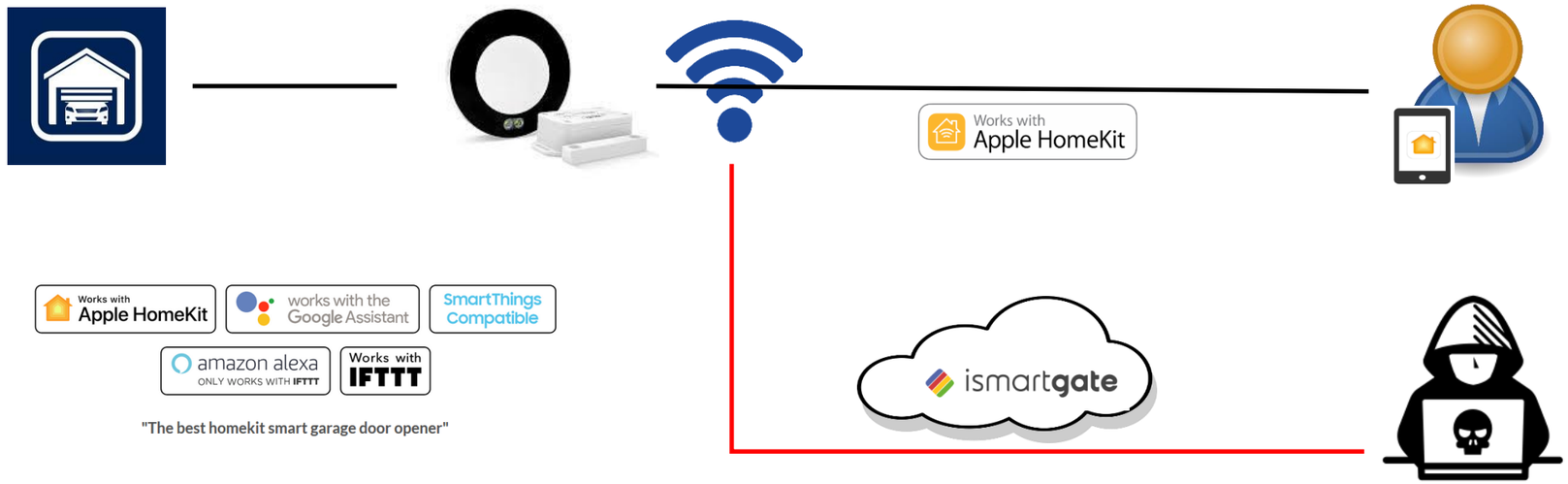
- Codema Flaw 1: Disjointed HomeKit and m-DMC



Understanding Codema

Disjointed DMC Management

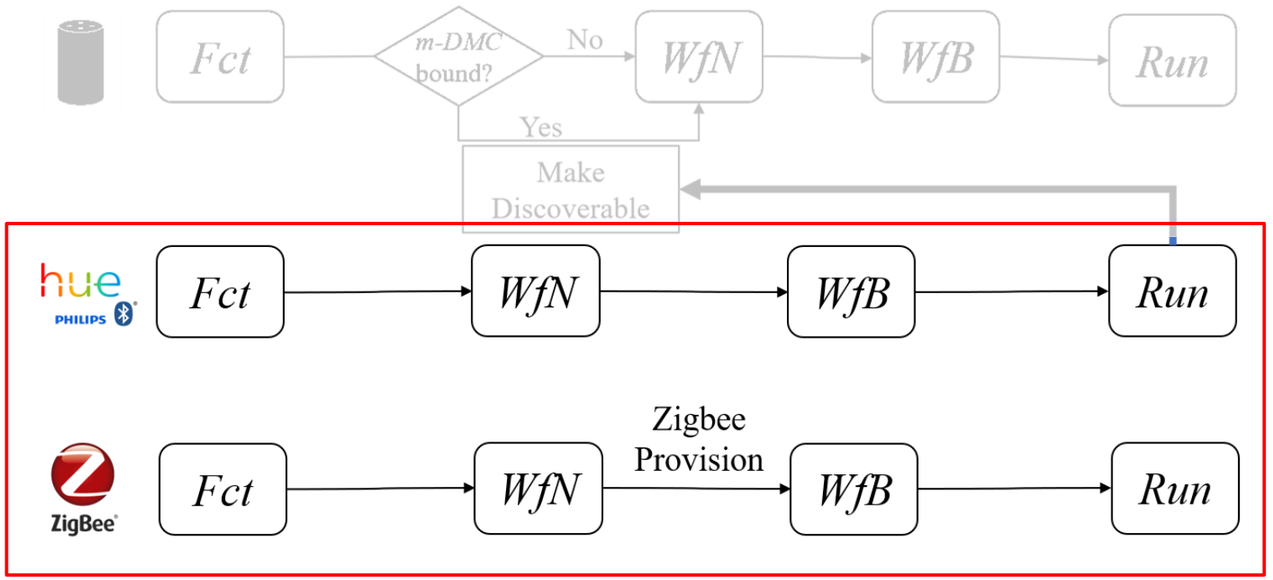
- Codema Flaw 1: Disjointed HomeKit and m-DMC



Understanding Codema

Disjointed DMC Management

- Codema Flaw 2: Disjointed Zigbee-based DMC and m-DMC



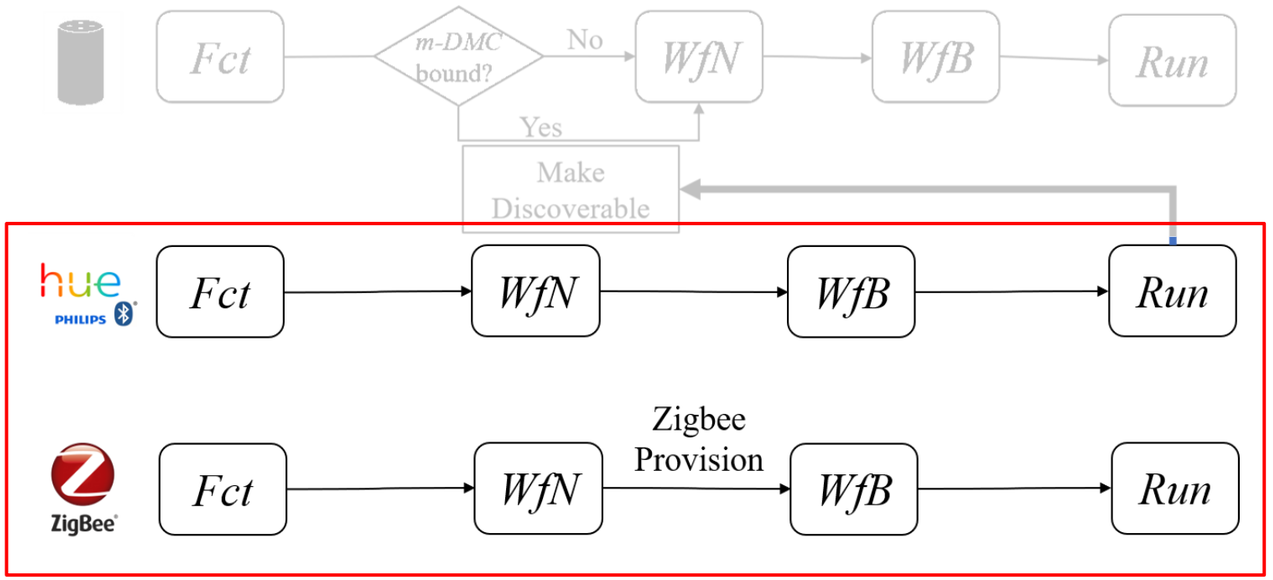
Understanding Codema

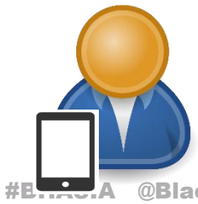
Disjointed DMC Management

- Codema Flaw 2: Disjointed Zigbee-based DMC and m-DMC

Bluetooth App Control*

Works with the Hue Bridge





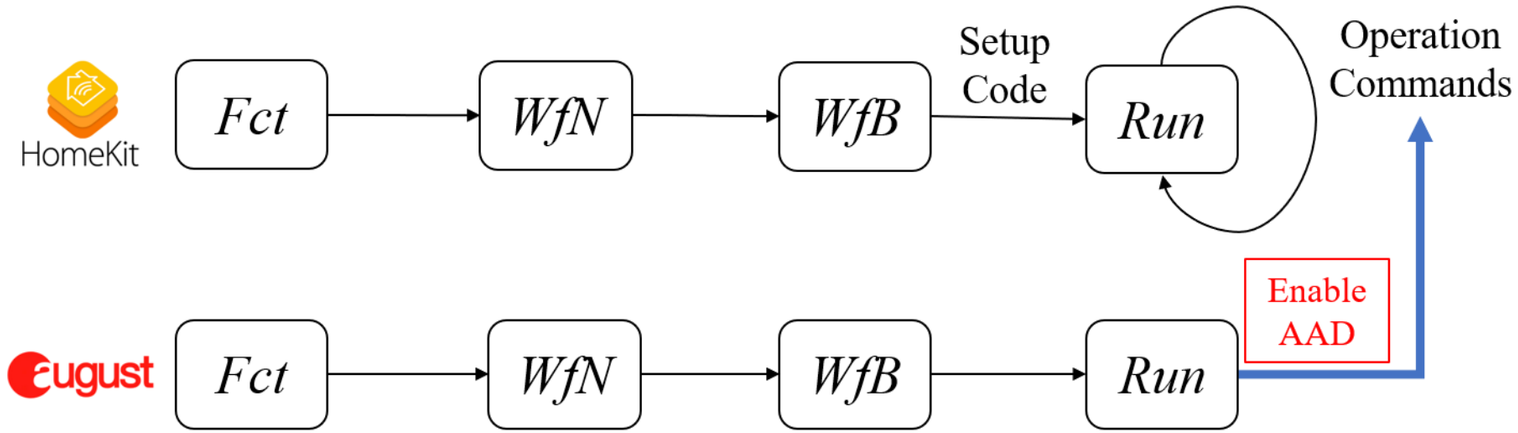
Codema Attack: Controlling Smart Home Through Dangling Management Channels

Video

Understanding Codema

Weak Cross-DMC Management

- Codema Flaw 3: Insufficient cross-DMC control on Run state

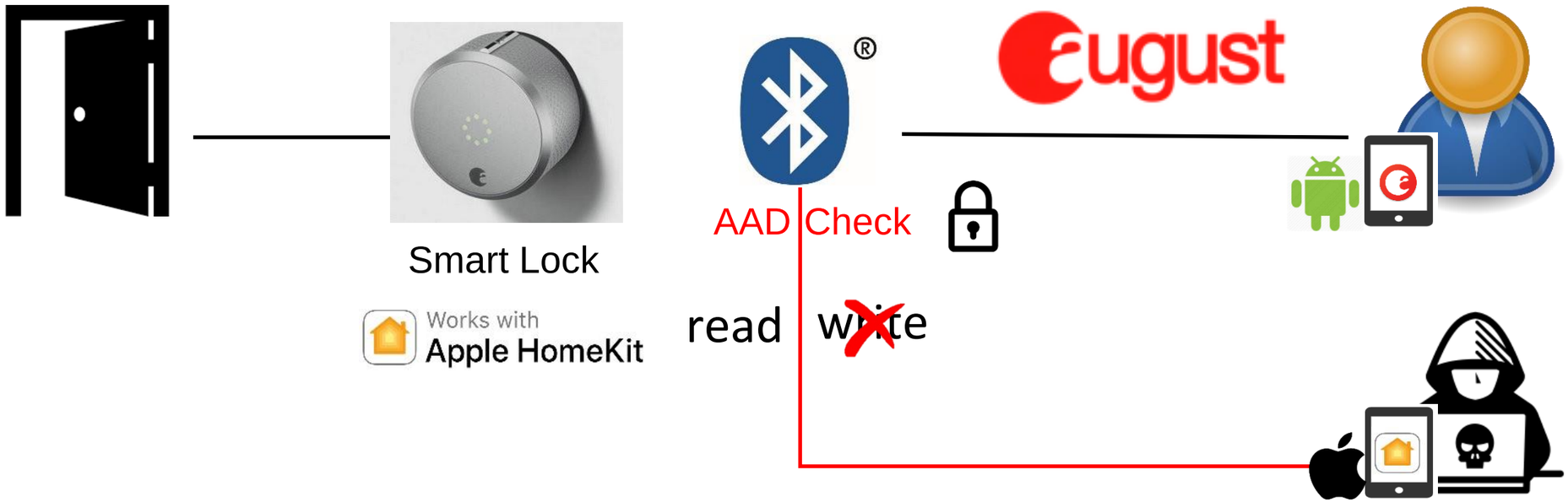


Works with Apple HomeKit

Understanding Codema

Weak Cross-DMC Management

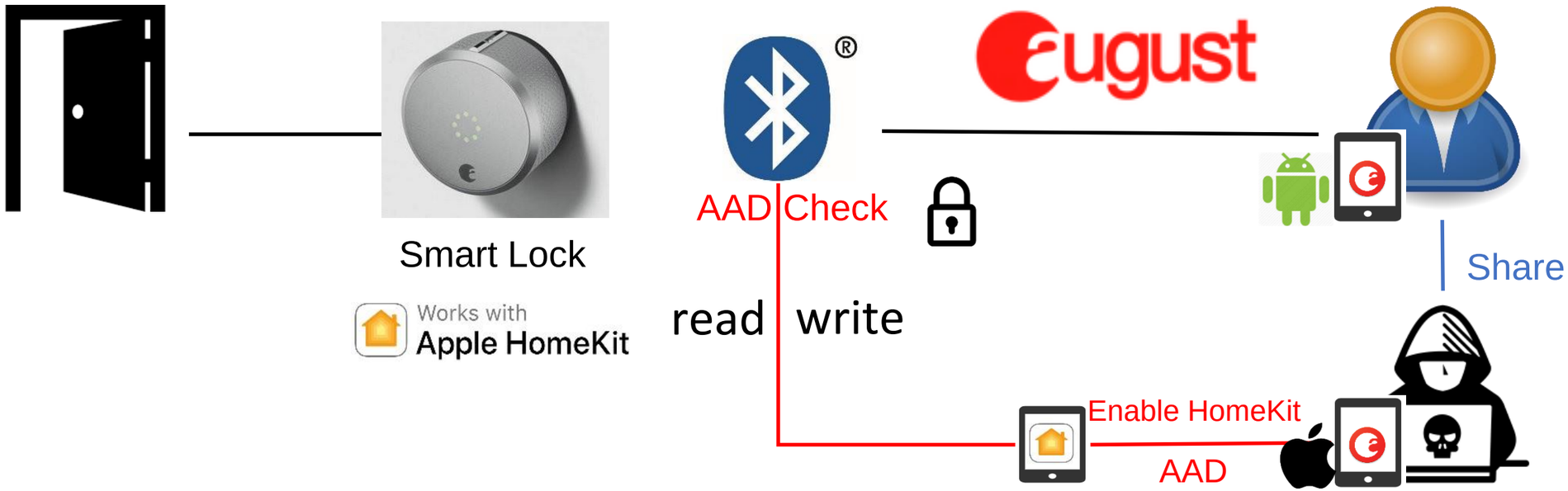
- Codema Flaw 3: Insufficient cross-DMC control on Run state



Understanding Codema

Weak Cross-DMC Management

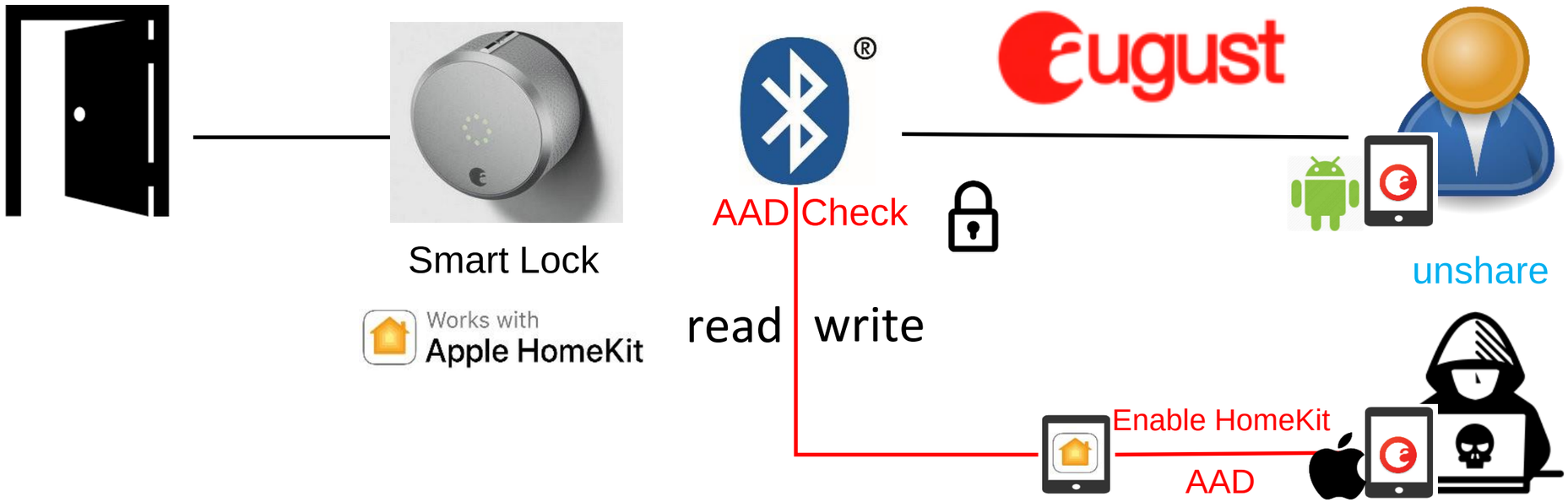
- Codema Flaw 3: Insufficient cross-DMC control on Run state



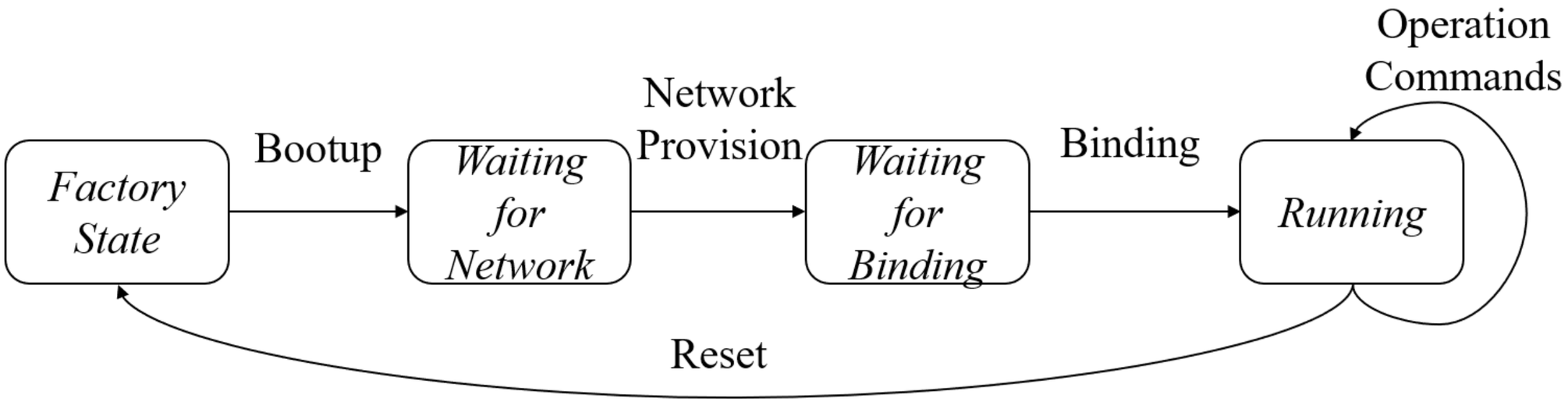
Understanding Codema

Weak Cross-DMC Management

- Codema Flaw 3: Insufficient cross-DMC control on Run state



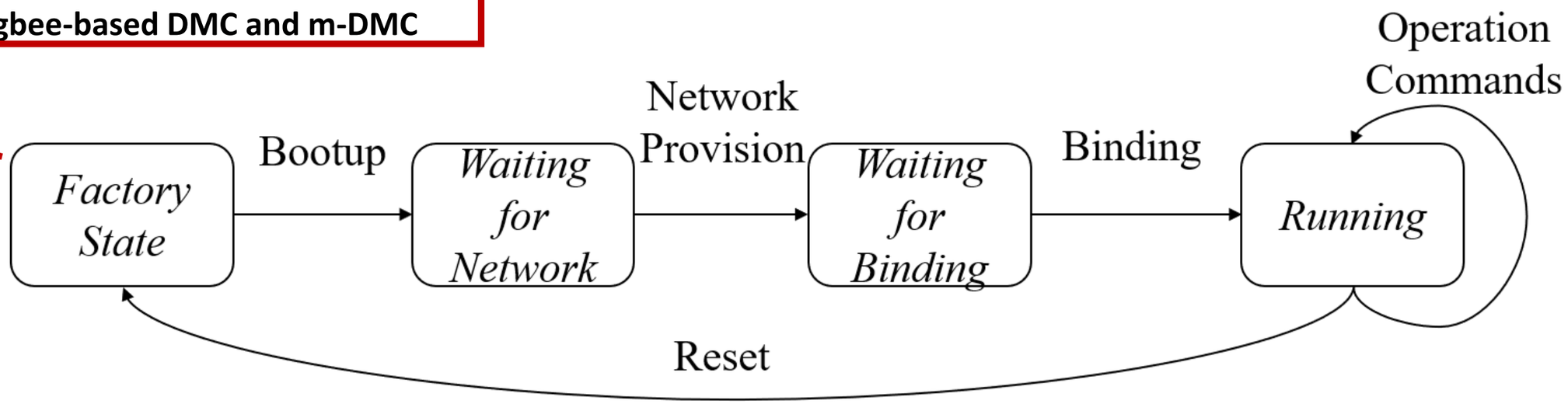
Understanding Codema



Understanding Codema

Codema Flaw 1:
Disjointed HomeKit and m-DMC

Codema Flaw 2:
Disjointed Zigbee-based DMC and m-DMC

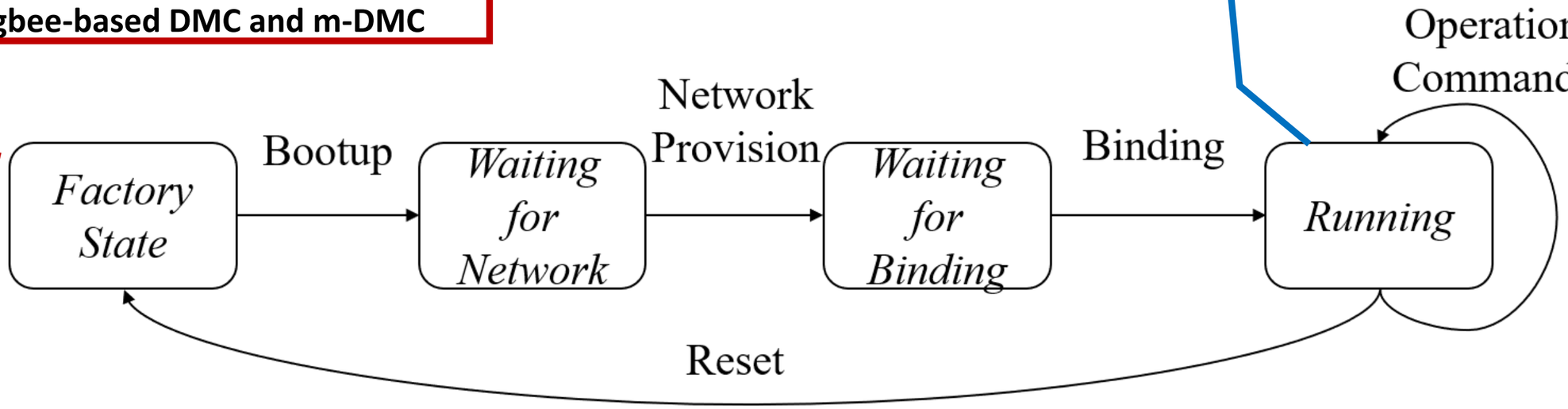


Understanding Codema

Codema Flaw 1:
Disjointed HomeKit and m-DMC

Codema Flaw 2:
Disjointed Zigbee-based DMC and m-DMC

Codema Flaw 3: Insufficient cross-DMC control on Run state

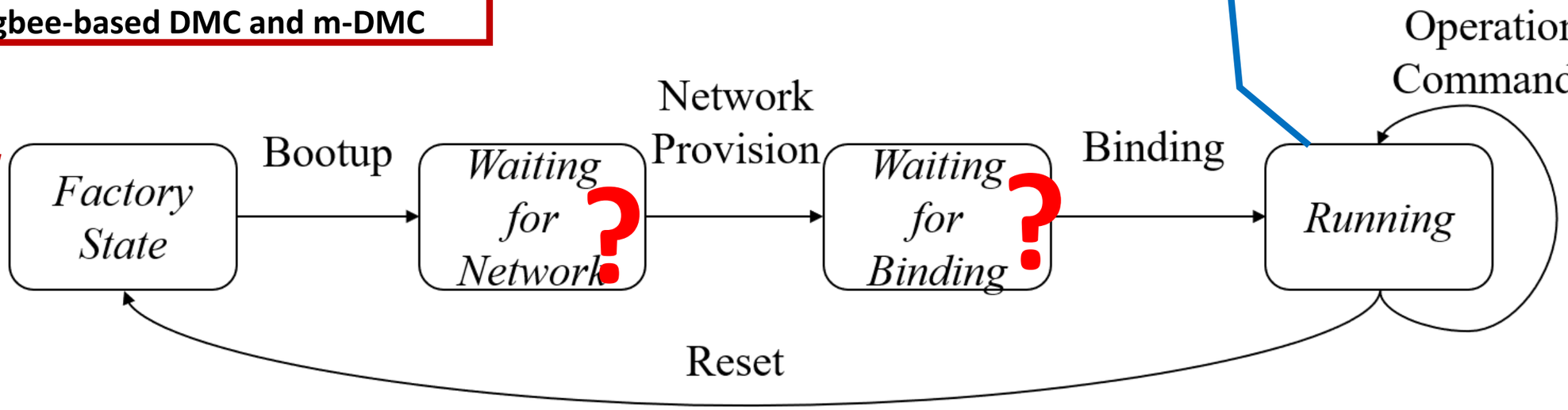


Understanding Codema

Codema Flaw 1:
Disjointed HomeKit and m-DMC

Codema Flaw 2:
Disjointed Zigbee-based DMC and m-DMC

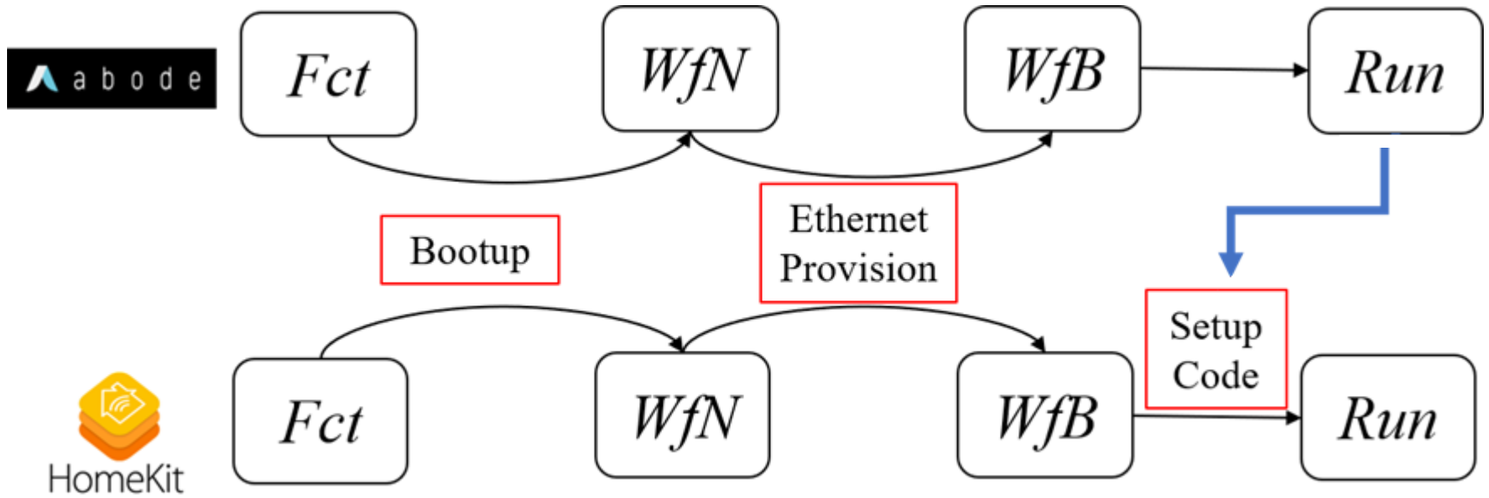
Codema Flaw 3: Insufficient cross-DMC control on Run state



Understanding Codema

Weak Cross-DMC Management

- Codema Flaw 4: Insufficient cross-DMC control on user binding (Wait for Binding state)



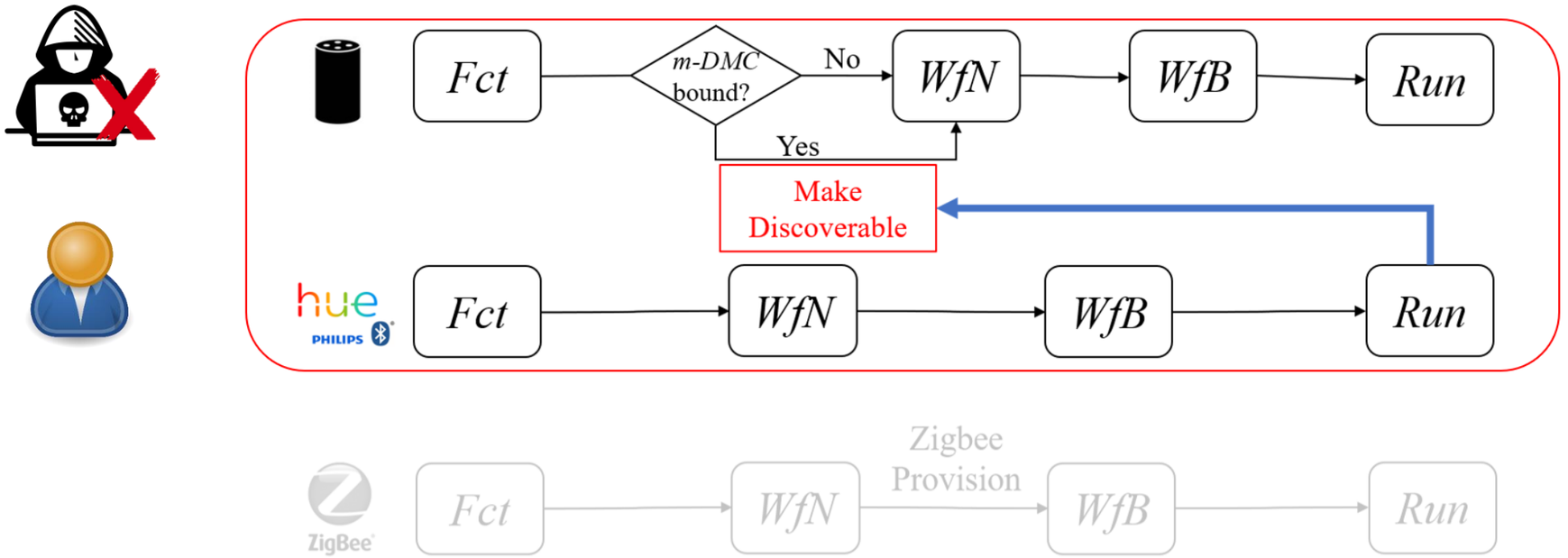
A malicious user can obtain the HomeKit setup code from the m-DMC when he is temporarily authorized.

Later, he uses the setup code to enable the HomeKit DMC and remains the access to the device via HomeKit DMC even if his right is revoked from the m-DMC.

Understanding Codema

Weak Cross-DMC Management

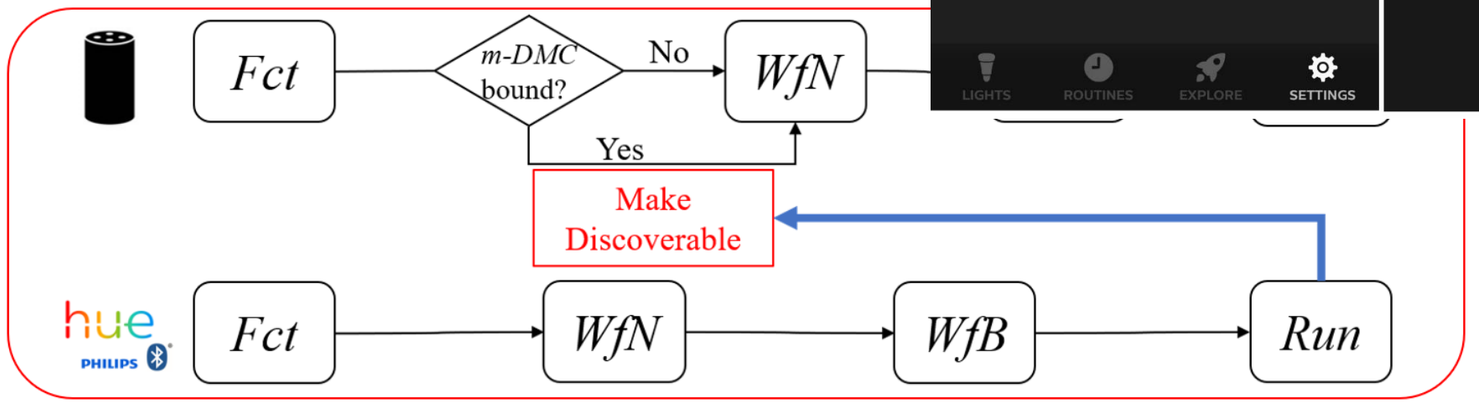
- Codema Flaw 5: Insufficient cross-DMC control on network provision (Wait for Network state)

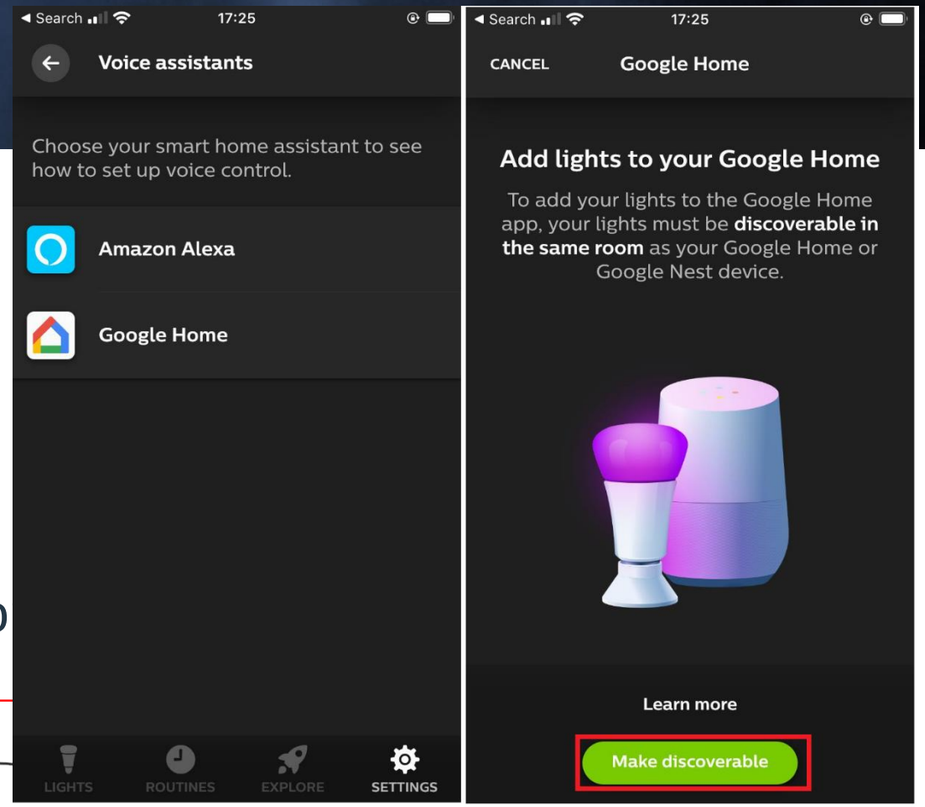


Understanding Codema

Weak Cross-DMC Management

- Codema Flaw 5: Insufficient cross-DMC control on netwo

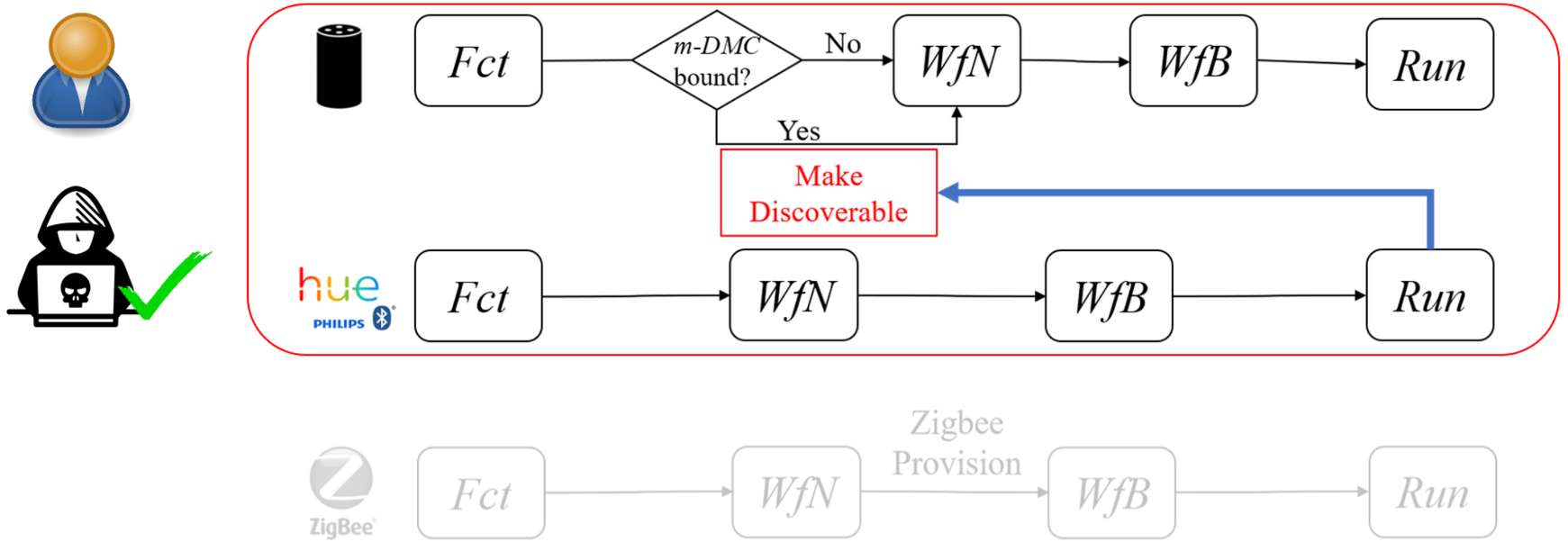




Understanding Codema

Weak Cross-DMC Management

- Codema Flaw 5: Insufficient cross-DMC control on network provision (Wait for Network state)



Attack Conditions

Conditions for a successful Codema attack

C1: The device owner opts for some but not all DMCs to manage a device.

C2: The adversary can access the target device's Wi-Fi network.

C3: The owner grants the adversary a temporary access to the target device.

Flaw	1	2	3	4	5
Condition	C1,C2	C1	C1, C2, C3	C1,C2,C3	C1

The codema vulnerabilities are highly related to **Human Behaviors**

Conditions for a successful Codema attack

C1: The device owner opts for some but not all DMCs to manage a device.

C2: The adversary can access the target device's Wi-Fi network.

C3: The owner grants the adversary a temporary access to the target device.

Is Codema vulnerability a real-world threat

Analyzing the Feasibility of Codema Attack

The User Perspective

C1: The device owner opts for some but not all DMCs to manage a device.

C2: The adversary can access the target device's Wi-Fi network.

C3: The owner grants the adversary a temporary access to the target device.

User study

24 participants, most (18/24) have IoT experience, 18<ages<40.

All of them have a technical or related education background.

configure an IoT device + a follow-up questionnaire

Analyzing the Feasibility of Codema Attack

The User Perspective

C1: The device owner opts for some but not all DMCs to manage a device.

C2: The adversary can access the target device's Wi-Fi network.

C3: The owner grants the adversary a temporary access to the target device.

User study (24 participants, device setup + follow-up questionnaire)

C1: 83.3% participants only setup one DMC.

C2: Home Wi-Fi is usually shared but the password is rarely changed.

C3: : IoT users are willing to share smart home devices.

Analyzing the Feasibility of Codema Attack

The Vendor Perspective

The specification

- no requirement for configuring all DMCs
- may not show all DMCs (IoT supply chain, update)
- “Please do not lose the code that is at the bottom of the device. Adding the device back will need the setup code after factory reset.”

The apps

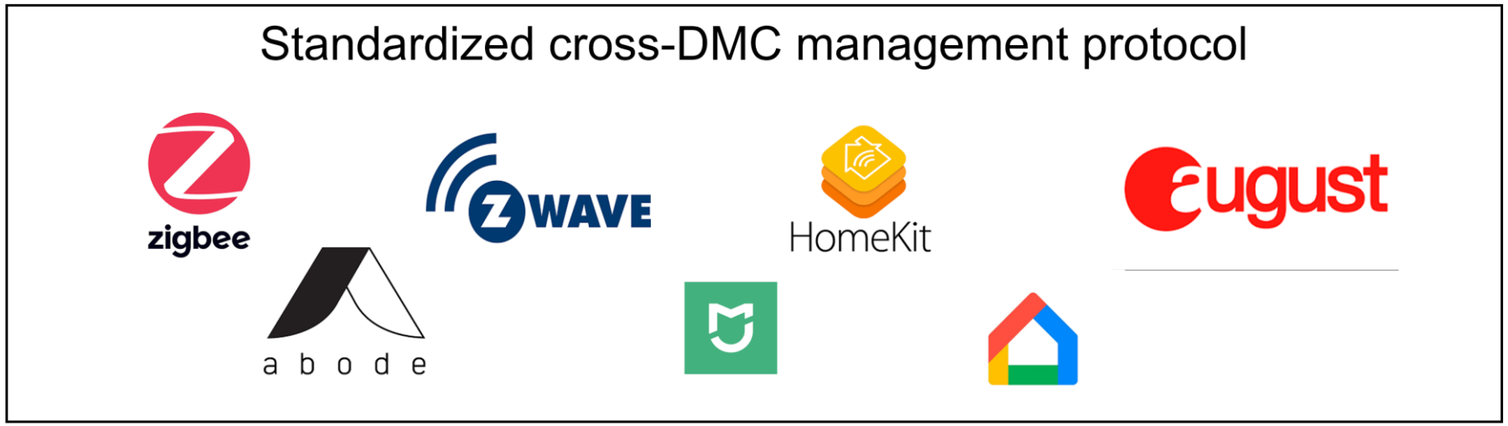

different platforms

different versions

Defending against the Codema Attack

Ideal solution: DMCs coordinate with each other

- Given a device (under its factory setting), the user can choose any of its supported DMCs.
- Any DMC the owner opts for helps her fully control the device by coordinating security policies across all DMCs.

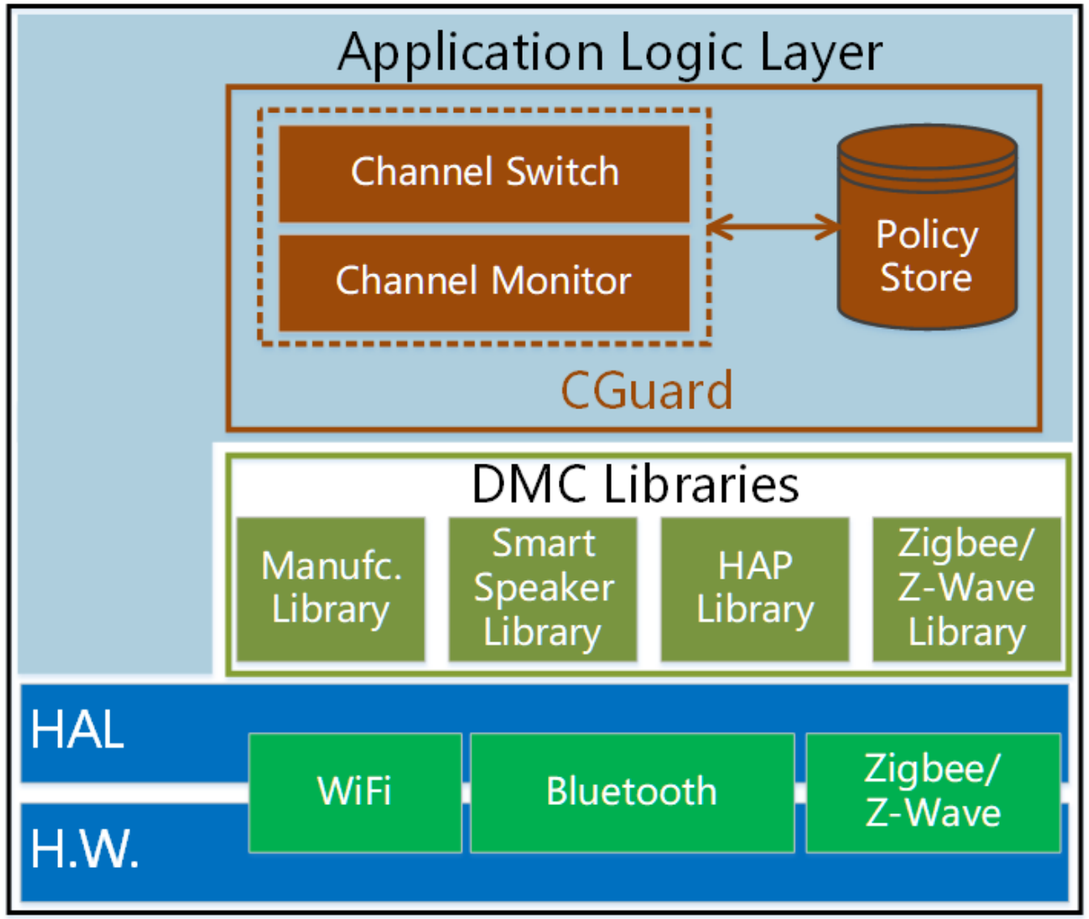


Cannot wait!

Defending against the Codema Attack

Our practical solution: CGuard

- Easy to deploy
  - adopted by the manufacturers
  - no change to the third-party DMCs



Defending against the Codema Attack

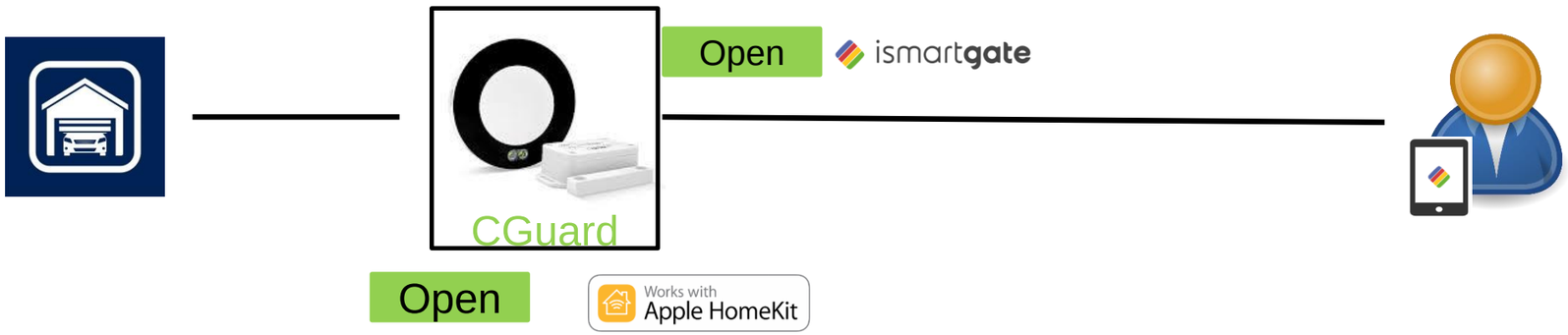
Mitigation goals

- Control goal: The users can fully control her device (including all DMCs)
- Usability goal: The users can choose any DMC to use at the factory set

Defending against the Codema Attack

Mitigation goals

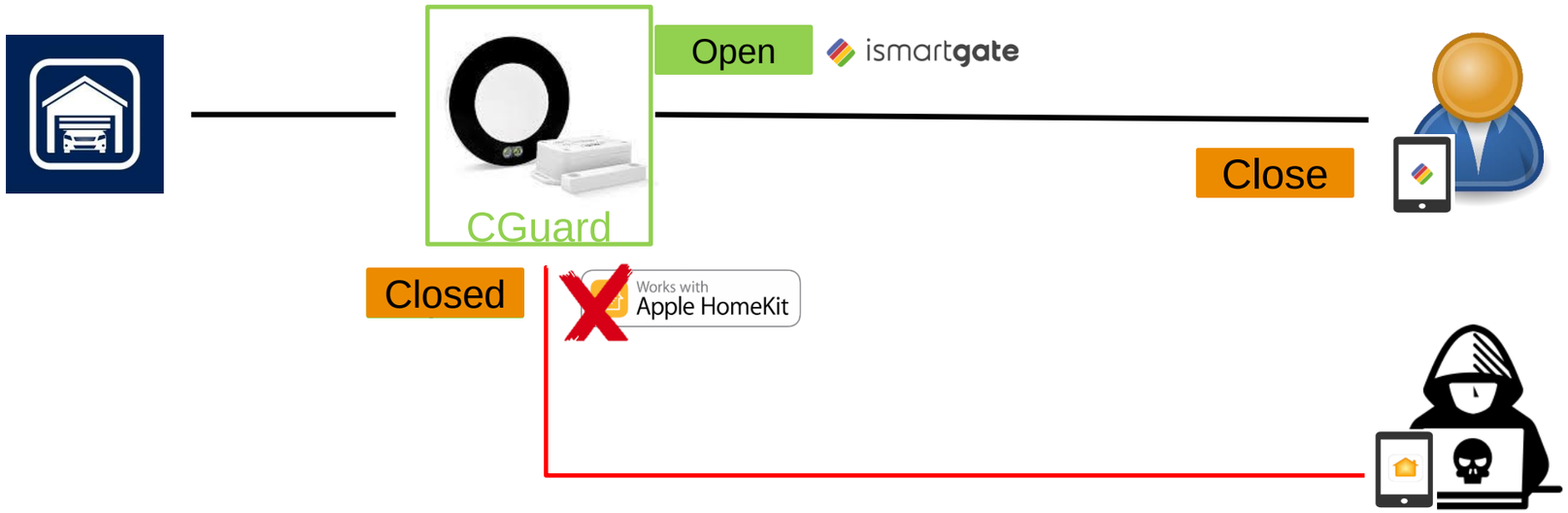
- Control goal: The users can fully control her device (including all DMCs)
- Usability goal: The users can choose any DMC to use at the factory set



Defending against the Codema Attack

Mitigation goals

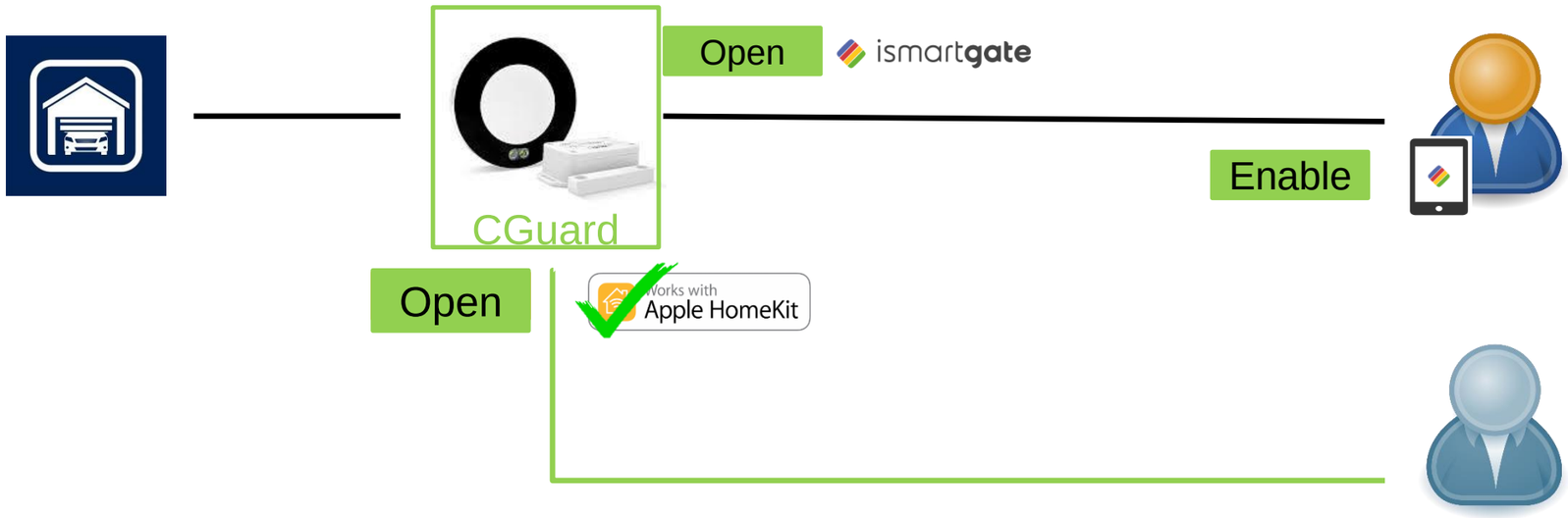
- Control goal: The users can fully control her device (including all DMCs)
- Usability goal: The users can choose any DMC to use at the factory set



Defending against the Codema Attack

Mitigation goals

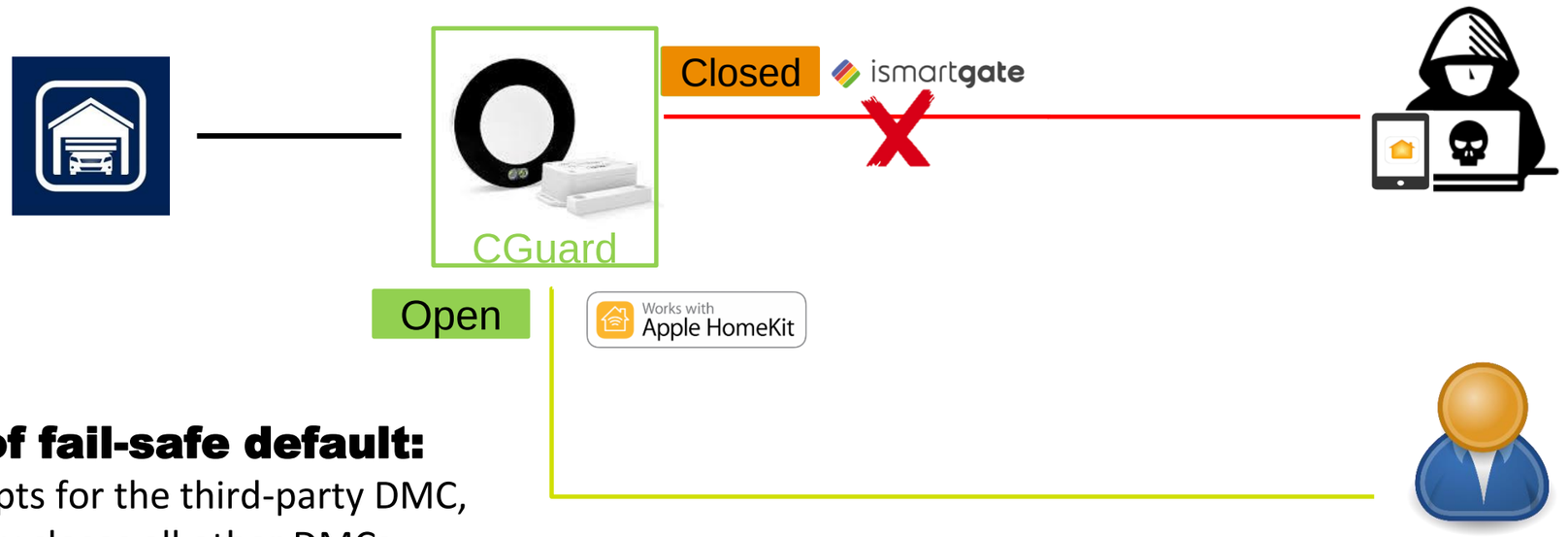
- Control goal: The users can fully control her device (including all DMCs)
- Usability goal: The users can choose any DMC to use at the factory set



Defending against the Codema Attack

Mitigation goals

- Control goal: The users can fully control her device (including all DMCs)
- Usability goal: The users can choose any DMC to use at the factory set



The principle of fail-safe default:
For an owner who opts for the third-party DMC, CGuard automatically closes all other DMCs.

Conclusion

New understanding on the IoT security

- a new category of weaknesses in IoT designs -- Codema
- realistic security risks and serious consequences

Practical solution

- a new access-control framework for multiple DMC enabled devices
- timely solution
- easy to adopt

Thank You

Yan Jia , Bin Yuan

jiay@nankai.edu.cn, yuanbin@hust.eud.cn