Hidden and Lost Control:

on Security Design Risks in IoT User-Facing Matter Controller

Haoqiang Wang[1,2,3], Yiwei Fang[1,2,3], **Yichen Liu[2]**, Ze Jin[1,2,3],
Emma Delph[2], Xiaojiang Du[4], Qixu Liu[1,3], Luyi Xing[2]

1. Institute of Information Engineering, Chinese Academy of Sciences
2. Indiana University Bloomington
3. School of Cyber Security, University of Chinese Academy of Sciences
4. Stevens Institute of Technology

Introduction

- Diverse IoT vendors.
- Diverse IoT apps.
- Diverse IoT development frameworks.

...

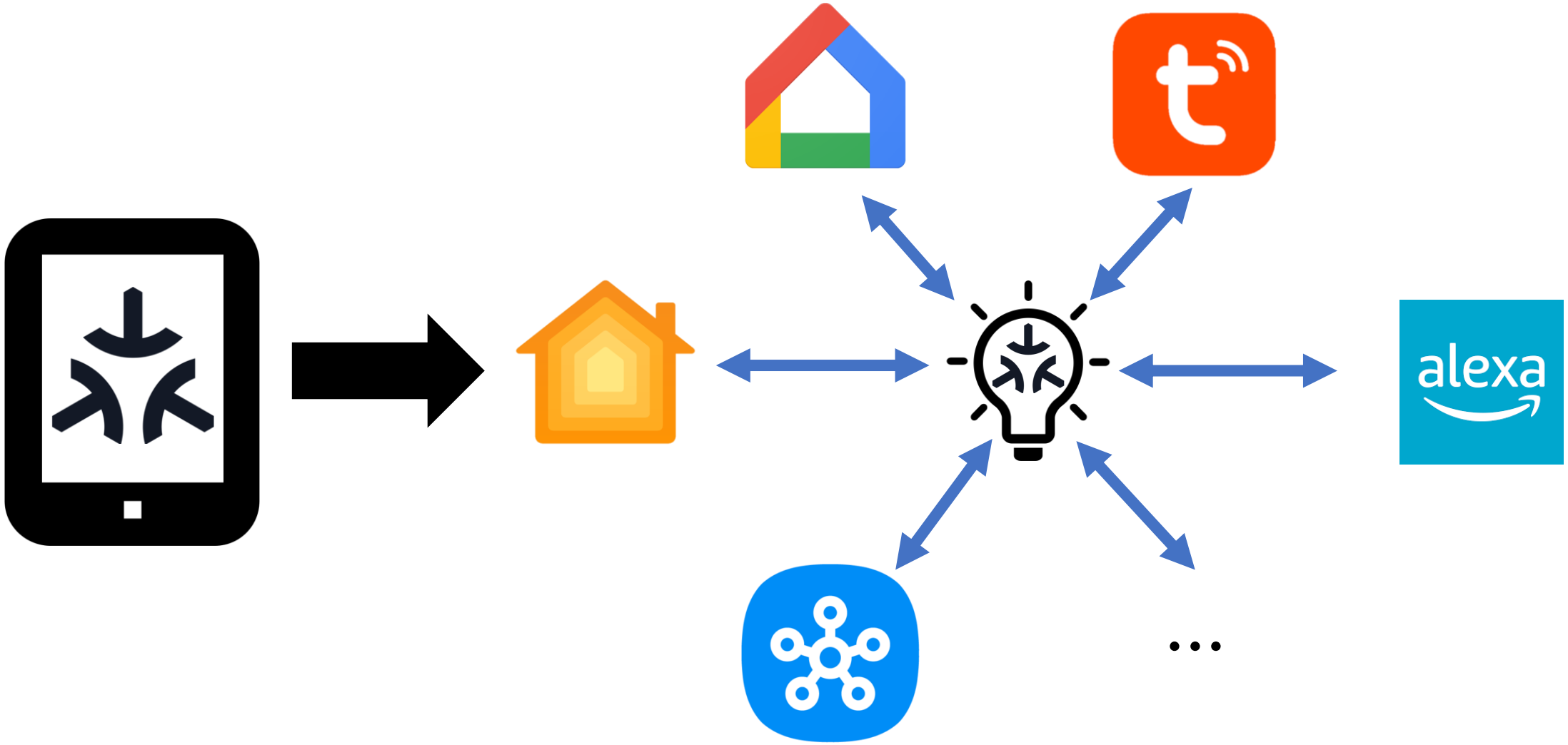
Introduction

- Diverse IoT vendors.
- Diverse IoT apps.
- Diverse IoT development frameworks.

Matter Protocol

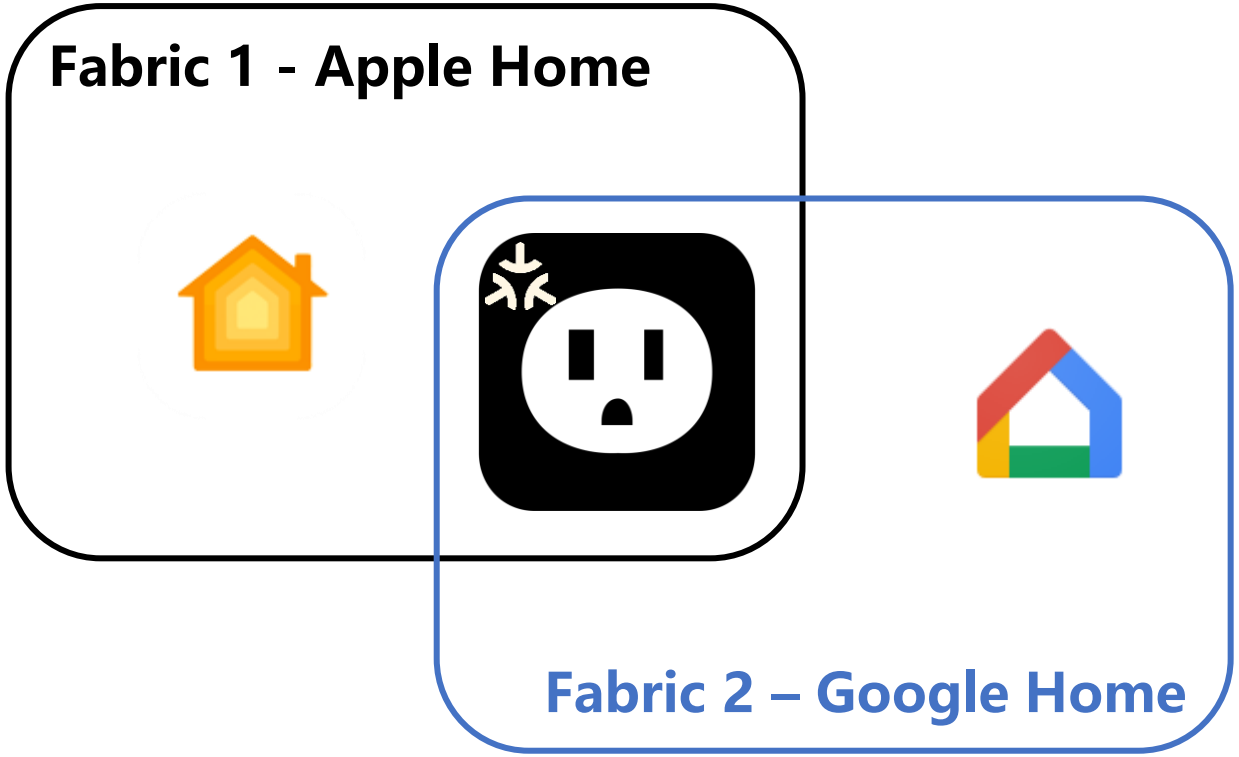
...

Matter Protocol

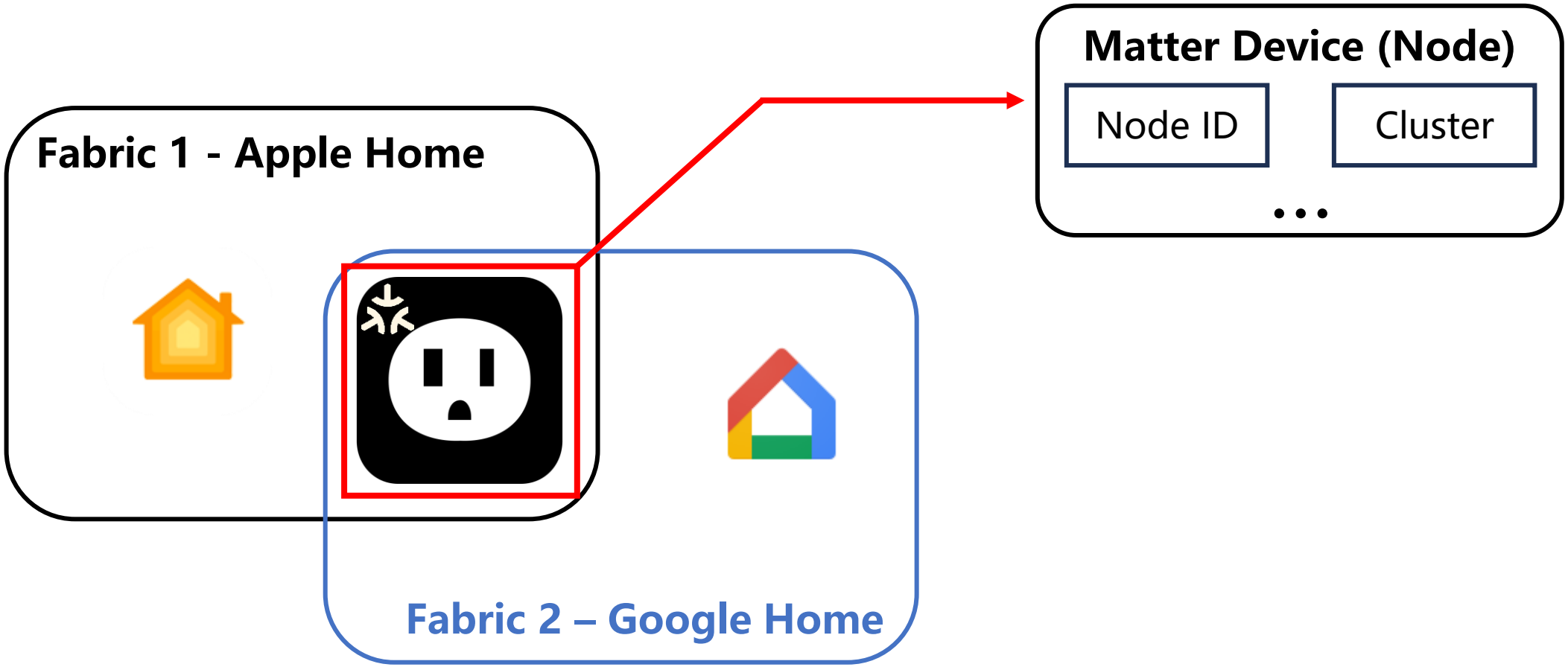


Matter can overcome the prevalent fragmentation and heterogeneity in the smart home industry.

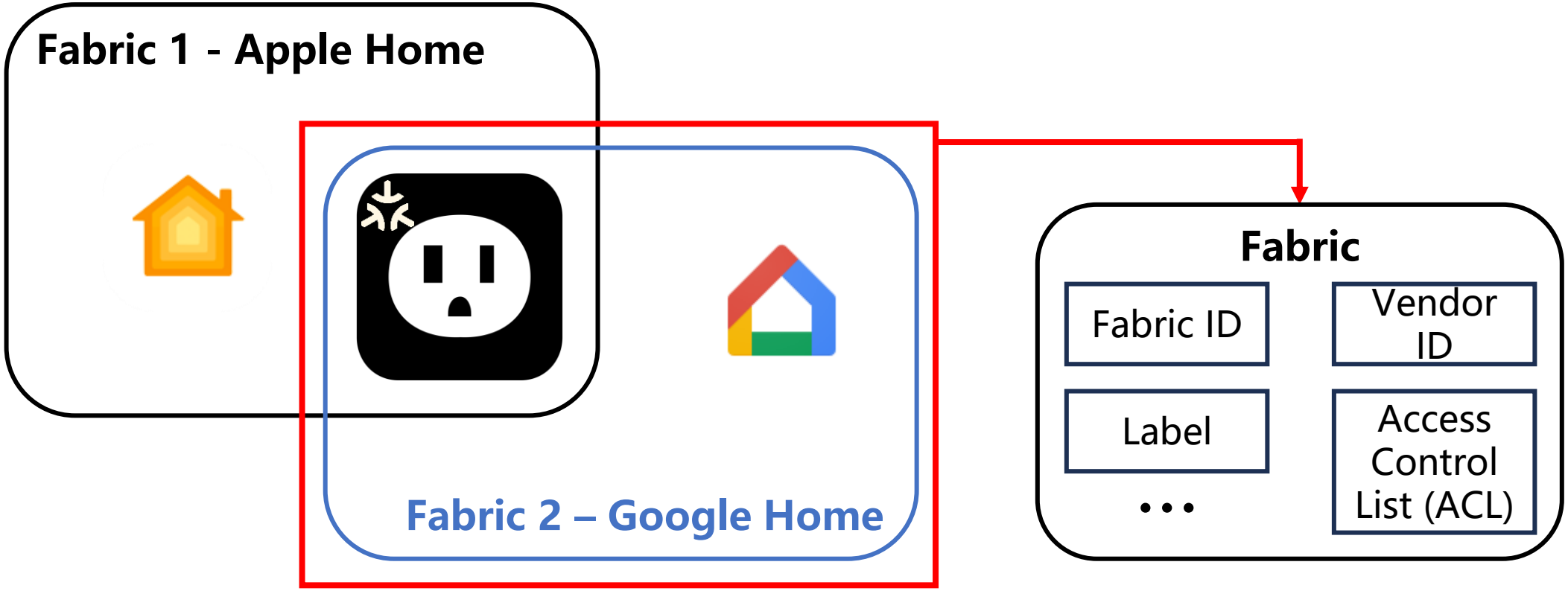
Matter Protocol



Matter Protocol

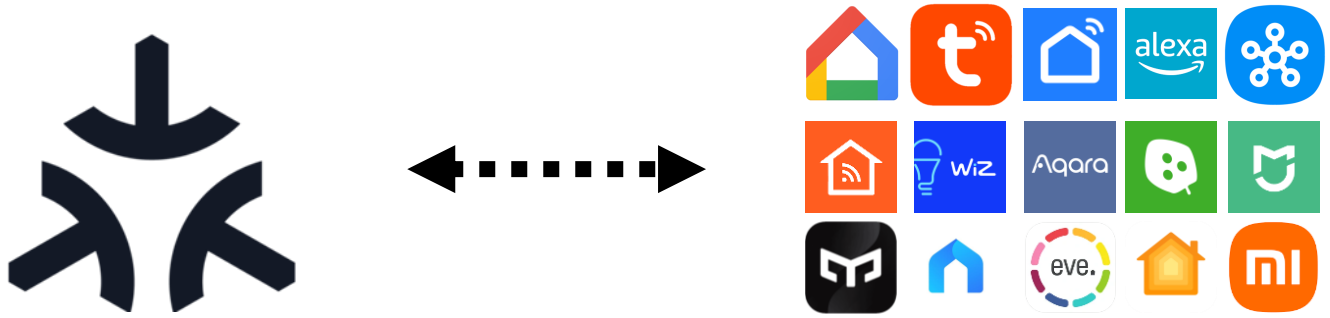


Matter Protocol



Key Research Questions

- **RQ1:** How do real-world IoT vendors integrate Matter to existing IoT devices and applications?
- **RQ2:** Can vendors securely integrate Matter to IoT devices and applications, and what is the error space that we should be aware of?
- **RQ3:** How well does Matter as a standard define and support IoT vendors' secure integration?



UMCCI (User-facing Matter Control Capabilities and Interfaces)

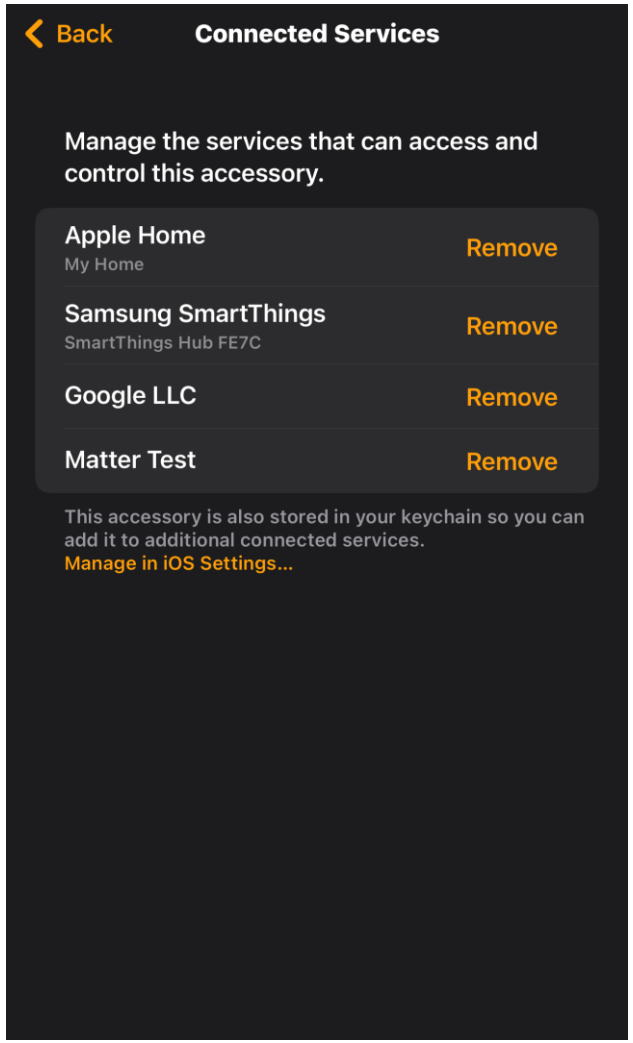
IoT Vendors

Develop

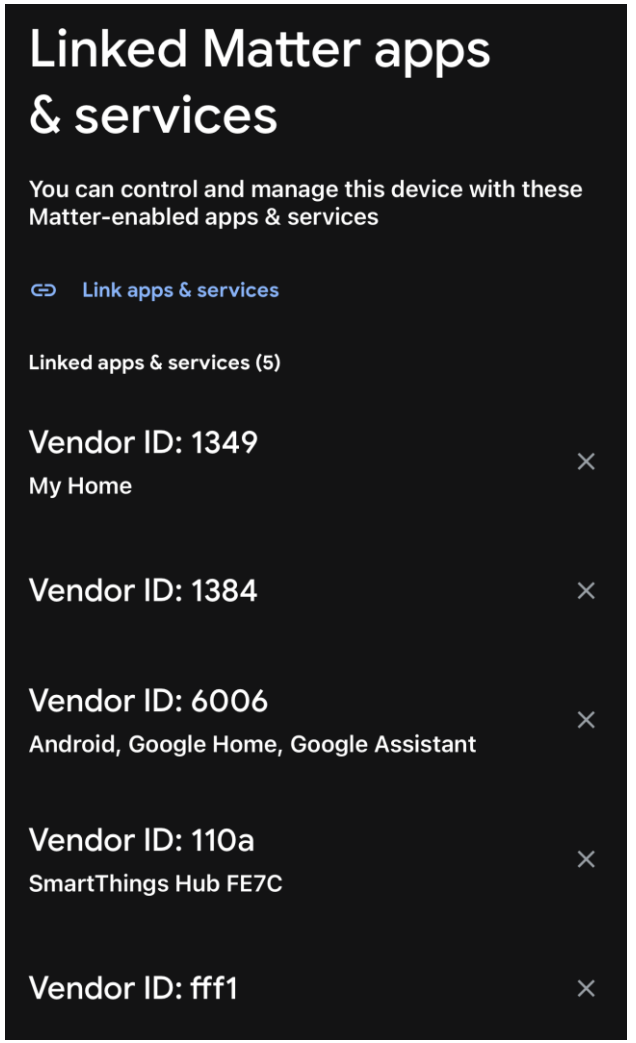
User-facing Matter Control Capabilities and Interfaces

In the IoT mobile app or hub, vendors additionally develop **user-facing Matter control capabilities and interfaces**, which we refer to as ***UMCCI***, such as a GUI or voice interface, for users to view, use, and control Matter devices through Matter controllers.

UMCCI (User-facing Matter Control Capabilities and Interfaces)



UMCCI in Apple Home



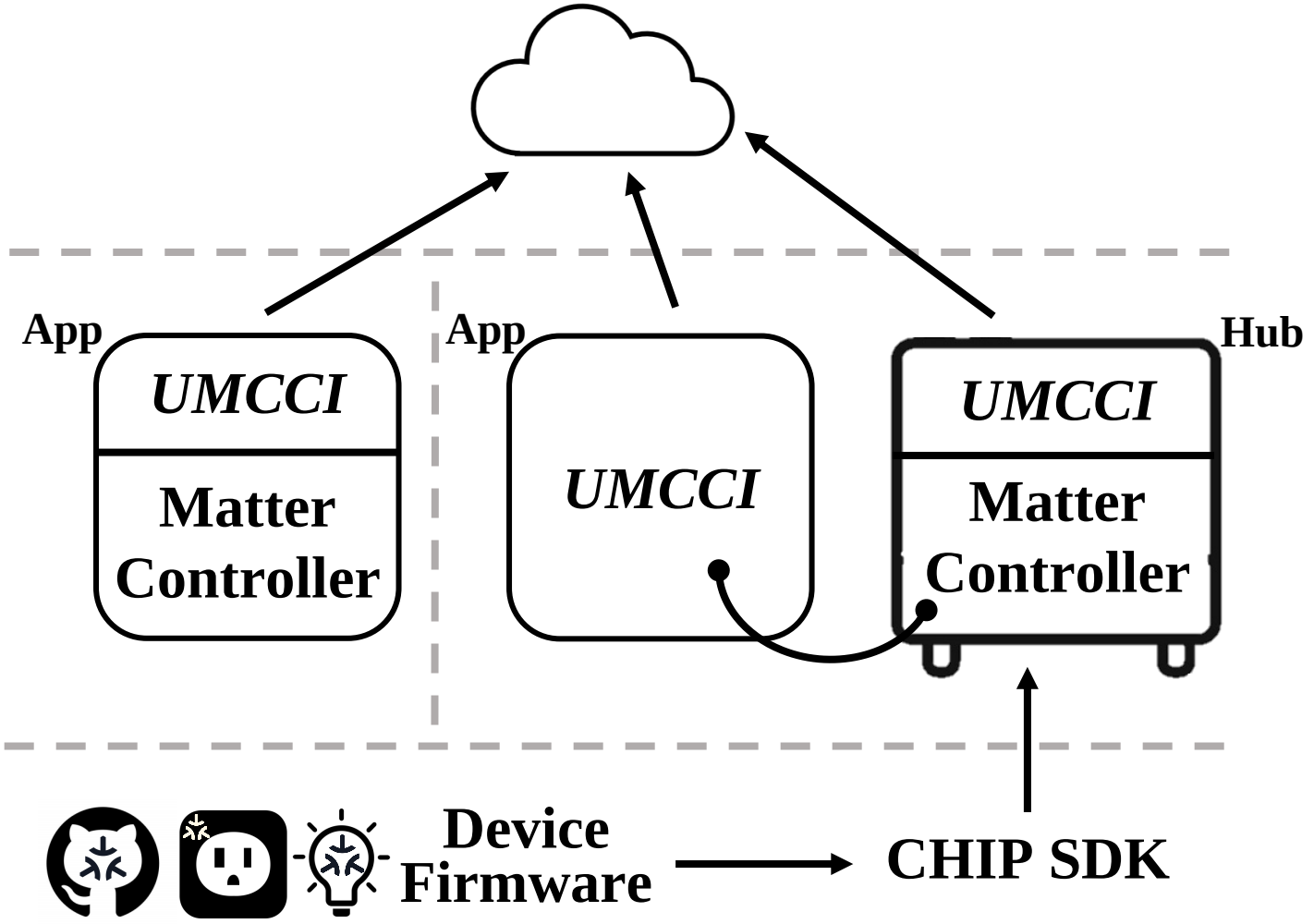
UMCCI in Google Home

Matter Development Model

Vendors' Cloud Layer (Remote)

Vendors' Matter Application Layer (Local)

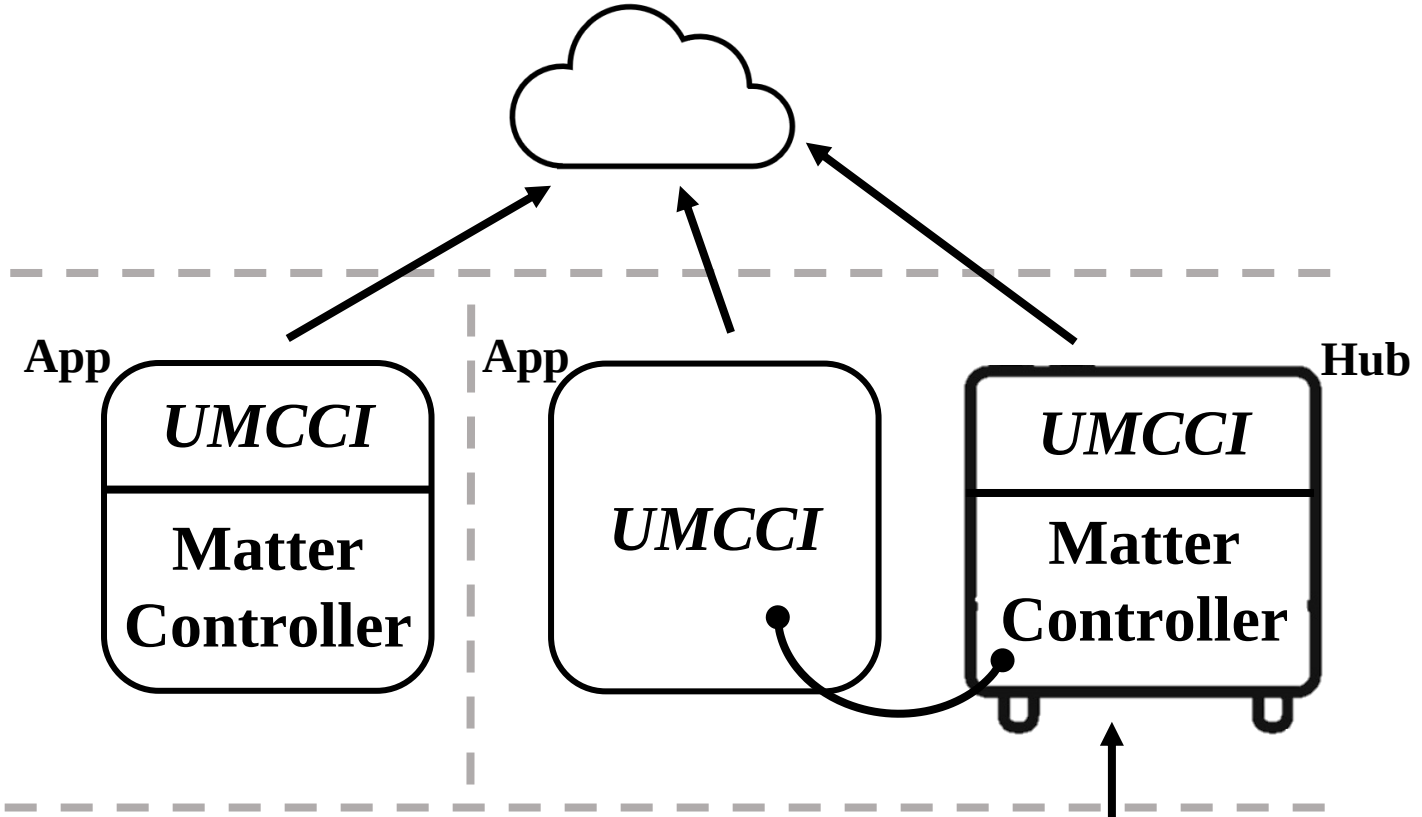
Matter Open-Source Layer



Matter Development Model

Vendors' Cloud Layer
(Remote)

Vendors' Matter
Application Layer (Local)

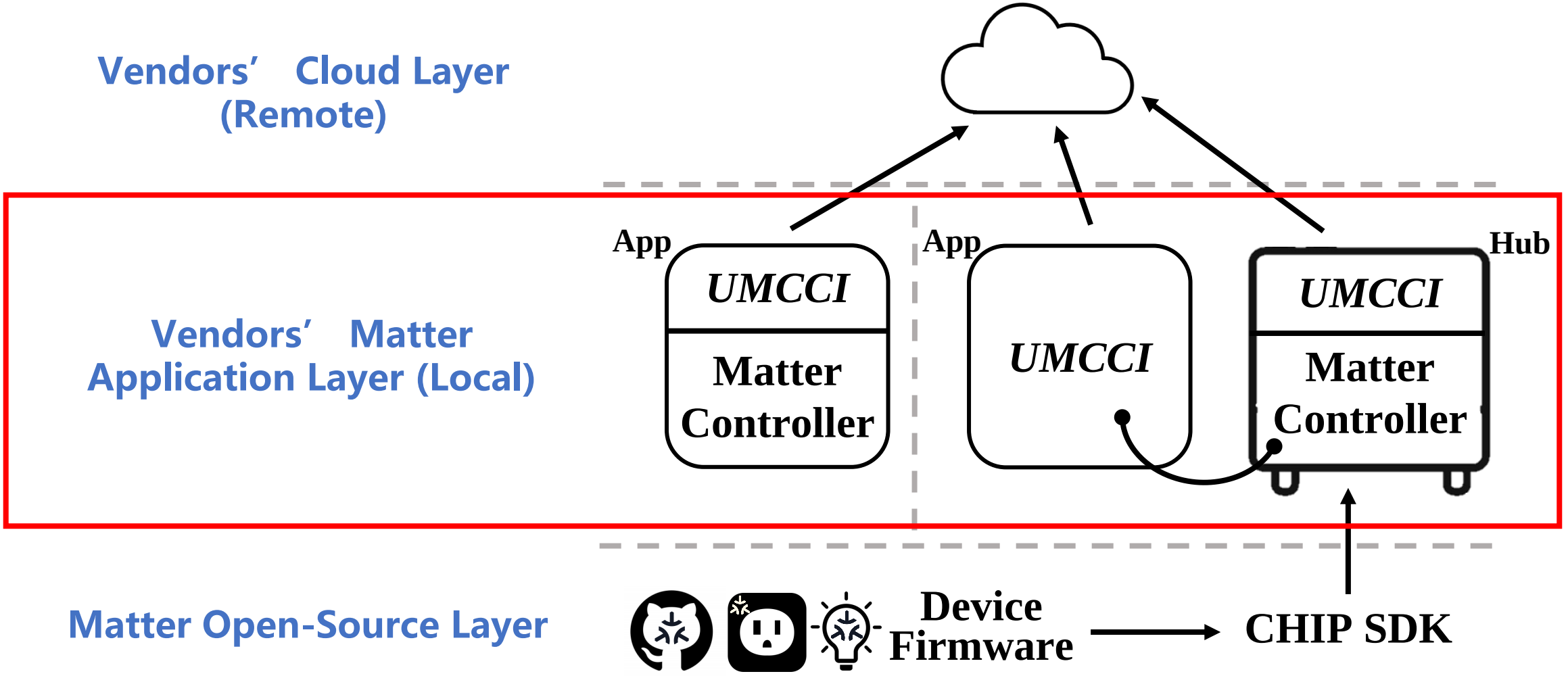


Matter Open-Source Layer

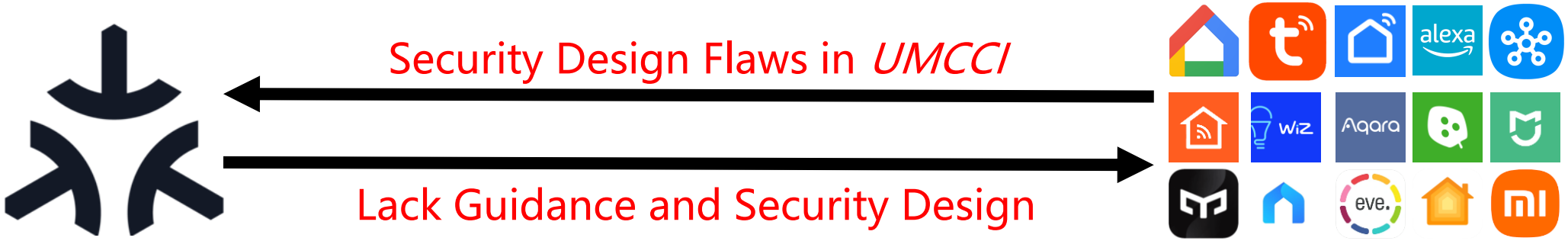
Device
Firmware

CHIP SDK

Matter Development Model

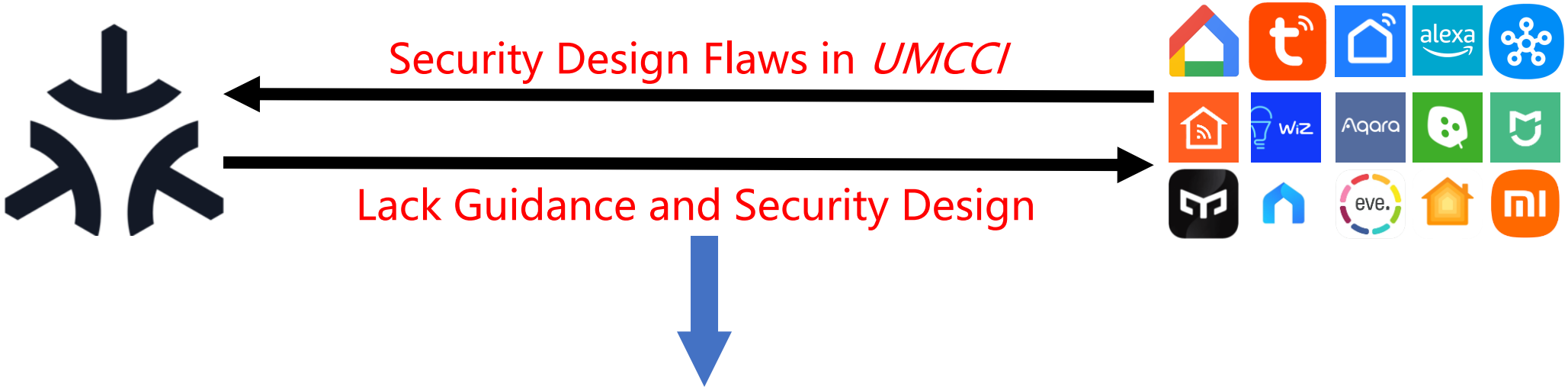


Security Risks in Matter Integration



- **View access-control information (P1).** Provide legitimate users with capabilities to view or query Matter access-control information, including all Matter controllers of the IoT devices, all Matter nodes (e.g., Matter devices, controllers) under a Matter fabric, and Matter ACL information maintained in Matter devices.
- **Access-control information trustworthiness (P2).** The access control information shown to users should be true and trustworthy.
- **Update access-control information (P3).** Provide capabilities for legitimate users to establish or revoke access-control for Matter devices.

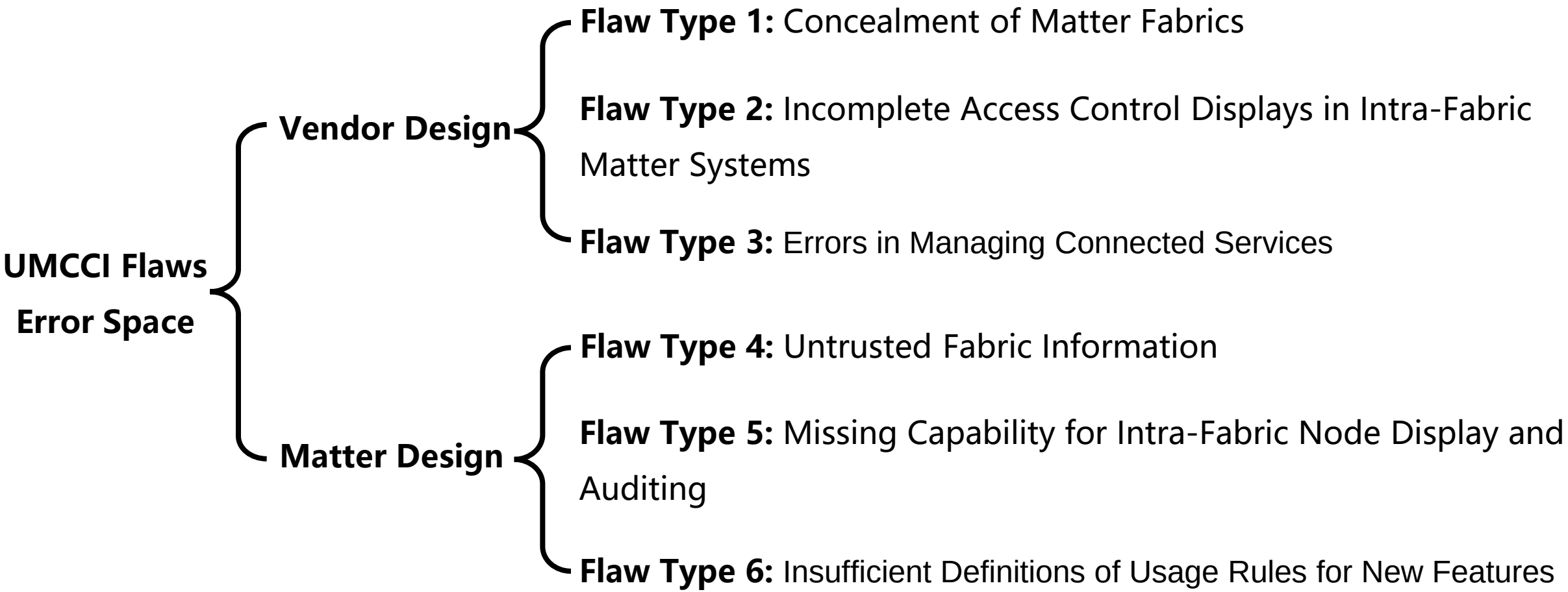
Security Risks in Matter Integration



We find that the apps of Apple Home, SmartThings, Google Home, Tuya, and others either **show a partial list of controllers based on the vendors' problematic interpretation of Matter UMCCI**, or **show unverified controller information** (e.g., controller vendors or controller names) that can be faked by malicious IoT users (such as prior employees, guests, and delegatee users) to **hide from device owners their unauthorized control** over Matter devices.

***UMCCI* Flaws**

UMCCI Flaws

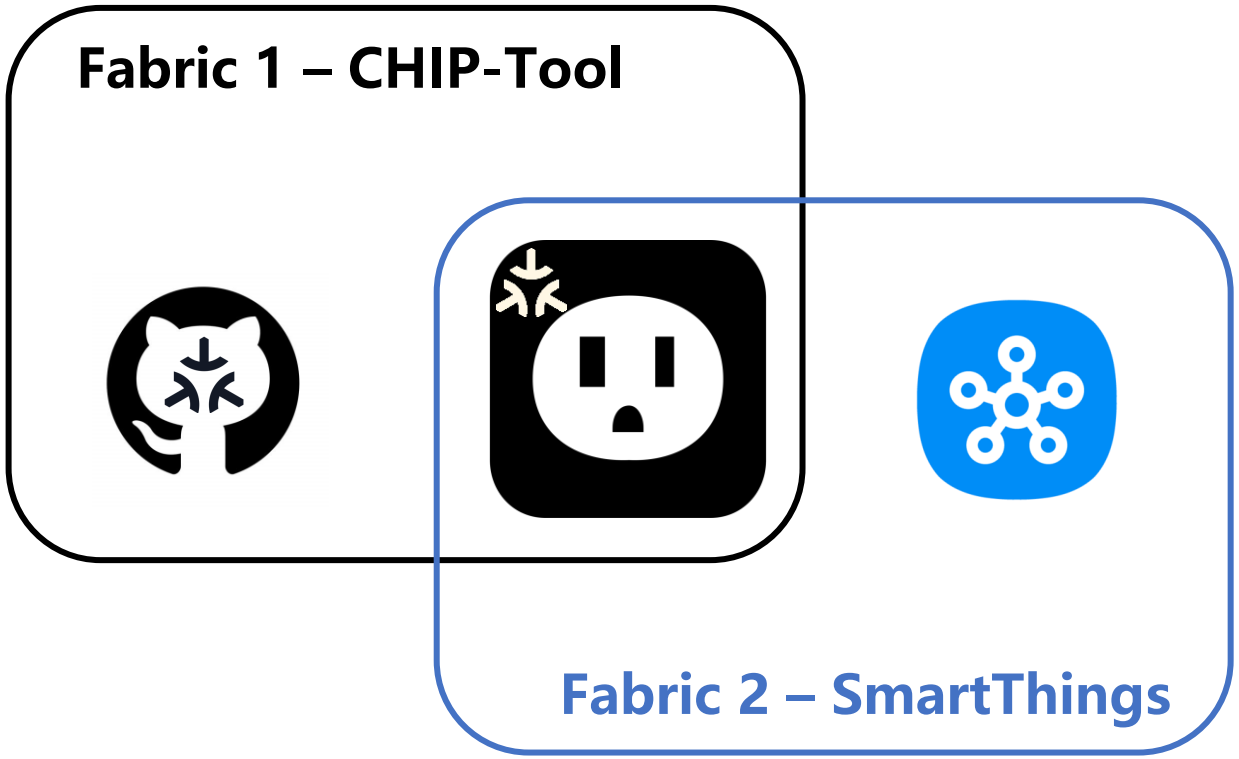

UMCCI Flaws Error Space
Vendor Design
Flaw Type 1: Concealment of Matter Fabrics
Flaw Type 2: Incomplete Access Control Displays in Intra-Fabric Matter Systems
Flaw Type 3: Errors in Managing Connected Services
Matter Design
Flaw Type 4: Untrusted Fabric Information
Flaw Type 5: Missing Capability for Intra-Fabric Node Display and Auditing
Flaw Type 6: Insufficient Definitions of Usage Rules for New Features

UMCCI Flaws

UMCCI Flaws		Apple	Google	Amazon Alexa	Samsung SmartThings	Tuya	Aqara	Uascent	Signify WiZ
Vendor Design	Flaw Type 1	✗	✓	N/A	✗	✓	✓	✓	N/A
	Flaw Type 2	✗	✗	N/A	✗	✗	✗	✗	N/A
	Flaw Type 3	✓	✓	✗	✓	✓	✓	✓	✗
Matter Design	Flaw Type 4	✗	✓	✓	✓	✗	✓	✓	N/A
	Flaw Type 5	✓	✓	✓	✓	✗	✓	✗	N/A
	Flaw Type 6	✓	✓	✓	✓	✓	✓	✓	✗

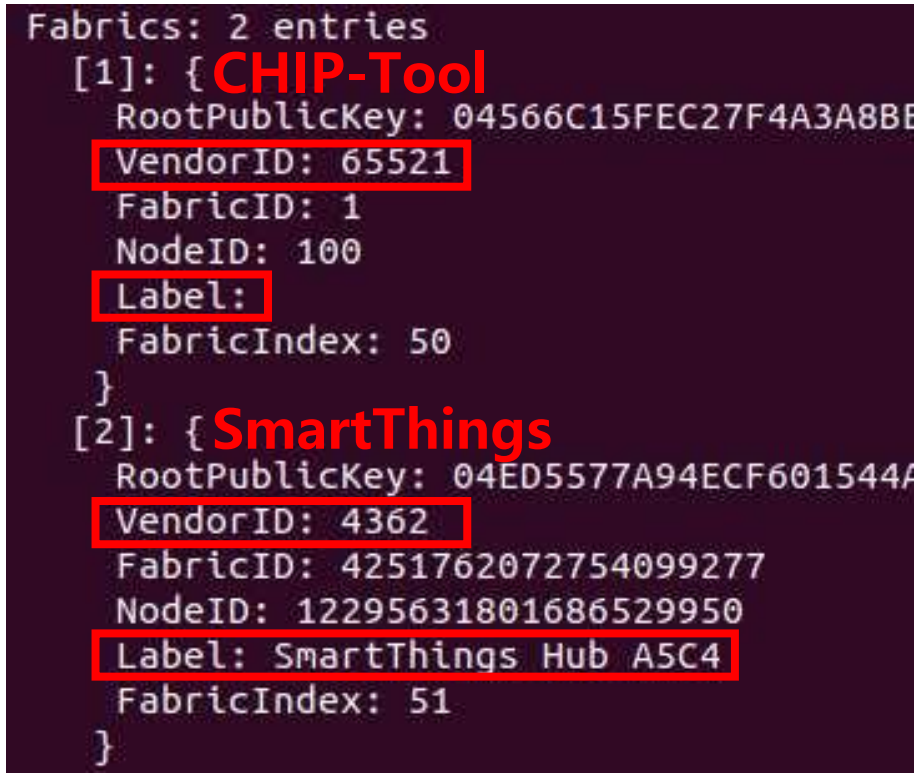
Vendor	Device Model	IoT App Name	Flaw Type of Matter Controller
Apple	HomePod mini	Home	1, 4
Google	Nest mini	Google Home	None
Samsung SmartThings	Station EP-P9501	SmartThings	1
Amazon Alexa	Echo Dot 3	Amazon Alexa	3
Tuya	Smart Wired Gateway Pro THP10-Z-X	Tuya Smart/Smart Life	2, 4, 5
Uascent	LED Light	uHome+	5
Aqara	M2 Hub 2002	Aqara Home	2
Signify WiZ	A19 Light	WiZ V2	3, 6
Zemismart	LED E27	N/A	None
Nanoleaf	A60 Smart Bulb	Nanoleaf	None
Xenon	SM-PW703 Smart Plug	N/A	None

Example: Flaw Type 1 - Concealment of Matter Fabrics



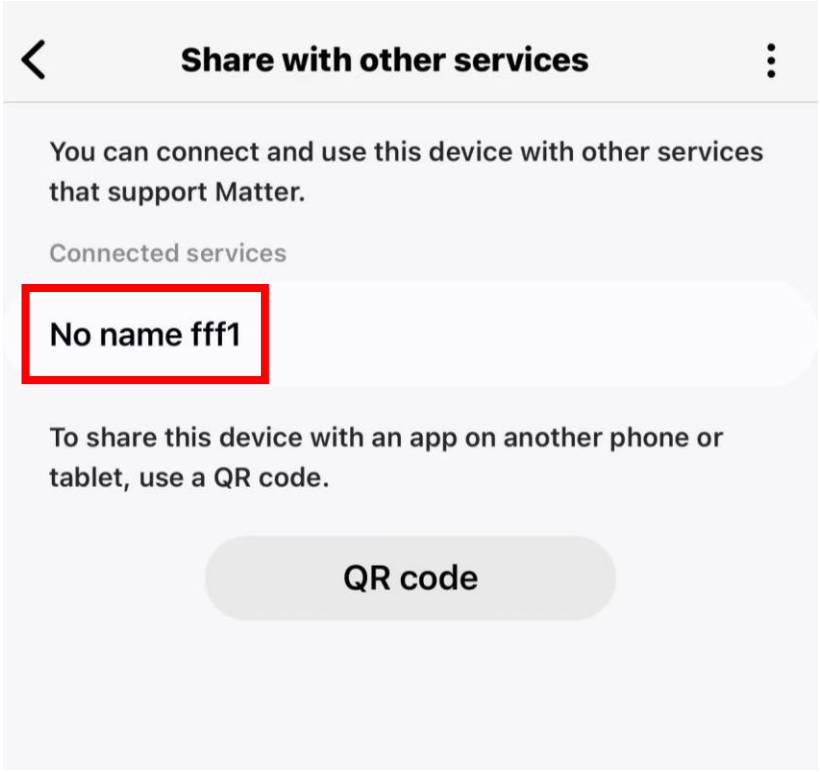
Example: Flaw Type 1 - Concealment of Matter Fabrics

chip-tool operationalcredentials read fabric



2 Fabrics

UMCCI of SmartThings App



Only 1 Fabrics

Example: Flaw Type 1 - Concealment of Matter Fabrics

chip-tool operationalcredentials read fabric

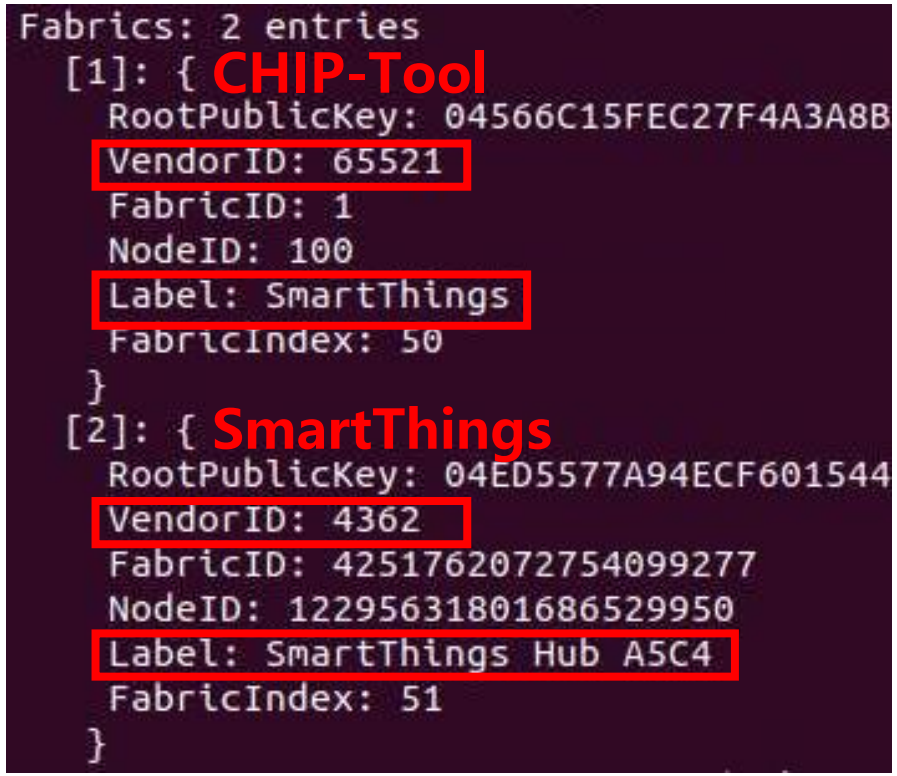
```
Fabrics: 2 entries
  [1]: {CHIP-Tool
    RootPublicKey: 04566C15FEC27F4A3A8BE
    VendorID: 65521
    FabricID: 1
    NodeID: 100
    Label:
    FabricIndex: 50
   }
  [2]: {SmartThings
    RootPublicKey: 04ED5577A94ECF601544A
    VendorID: 4362
    FabricID: 4251762072754099277
    NodeID: 12295631801686529950
    Label: SmartThings Hub A5C4
    FabricIndex: 51
   }
```

chip-tool operationalcredentials update-fabric-label

```
Fabrics: 2 entries
  [1]: { CHIP-Tool
    RootPublicKey: 04566C15FEC27F4A3A8B
    VendorID: 65521
    FabricID: 1
    NodeID: 100
    Label: SmartThings
    FabricIndex: 50
   }
  [2]: { SmartThings
    RootPublicKey: 04ED5577A94ECF601544
    VendorID: 4362
    FabricID: 4251762072754099277
    NodeID: 12295631801686529950
    Label: SmartThings Hub A5C4
    FabricIndex: 51
   }
```

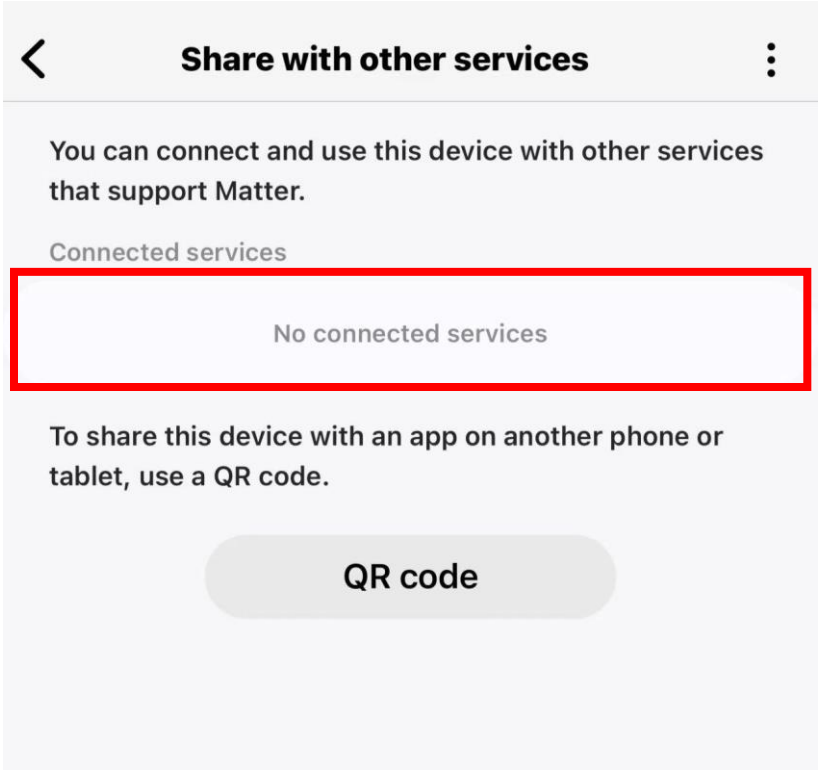
Example: Flaw Type 1 - Concealment of Matter Fabrics

chip-tool operationalcredentials read fabric



2 Fabrics

UMCCI of SmartThings App



No Fabrics

Example: Flaw Type 1 - Concealment of Matter Fabrics

Stealthiness Discussion

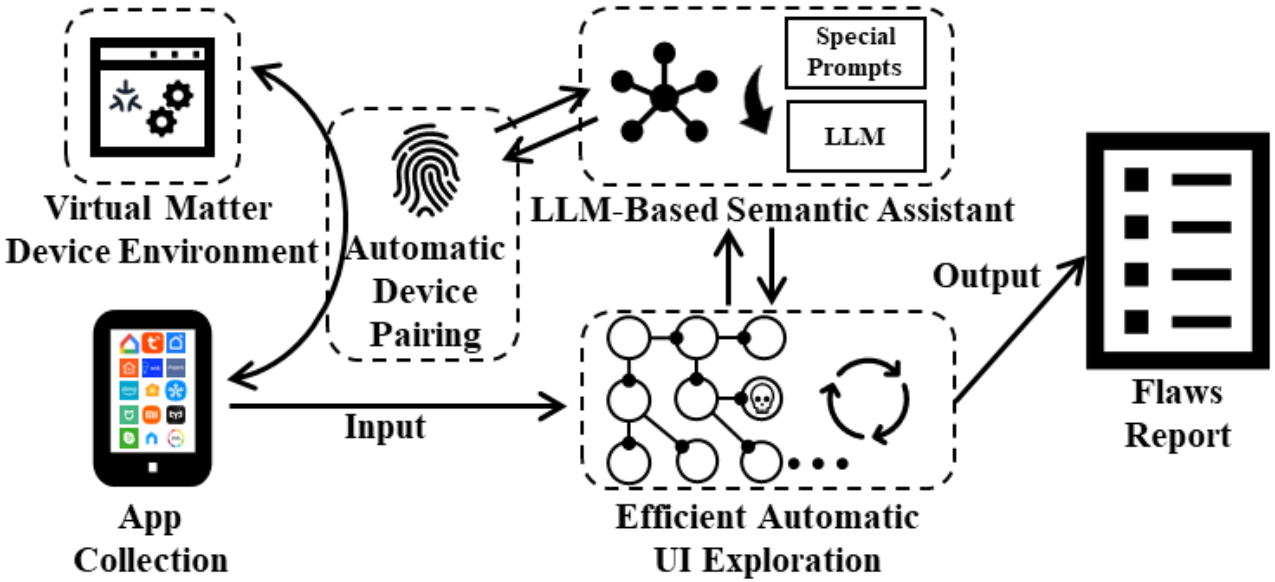
In real scenarios like Airbnb, this flaw allows the malicious guest’ s CHIP Tool to become invisible to the owner in the SmartThings app. Hence, even after the guest leaves, the owner can remove the guest’ s normal controller, but cannot identify or remove this hidden CHIP Tool controller in the SmartThings UMCCI, allowing the guest to retain covert control over the devices.

More PoC and Videos：

https://sites.google.com/view/mattercontrollerflaws/

Automatic Detection of UMCCI Flaws

UMCCI Checker

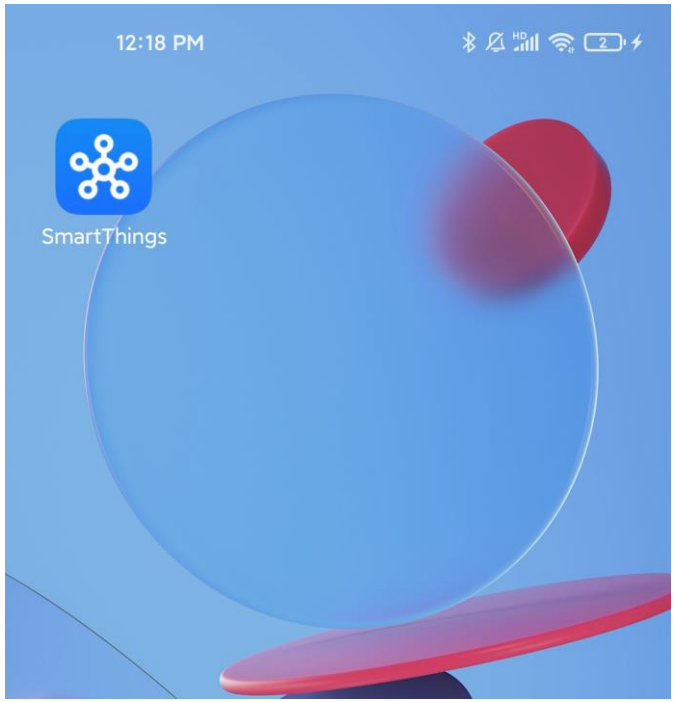


- Virtual Matter Device Environment (VMDE)
- Automatic Device Pairing (ADP)
- Efficient Automatic UI Exploration (EAUE)
- Flaw Analysis and Reporting (FAR)
- LLM-based Matter Agent (L-MA)

UMCCI Checker: One Example – Flaw Type 1

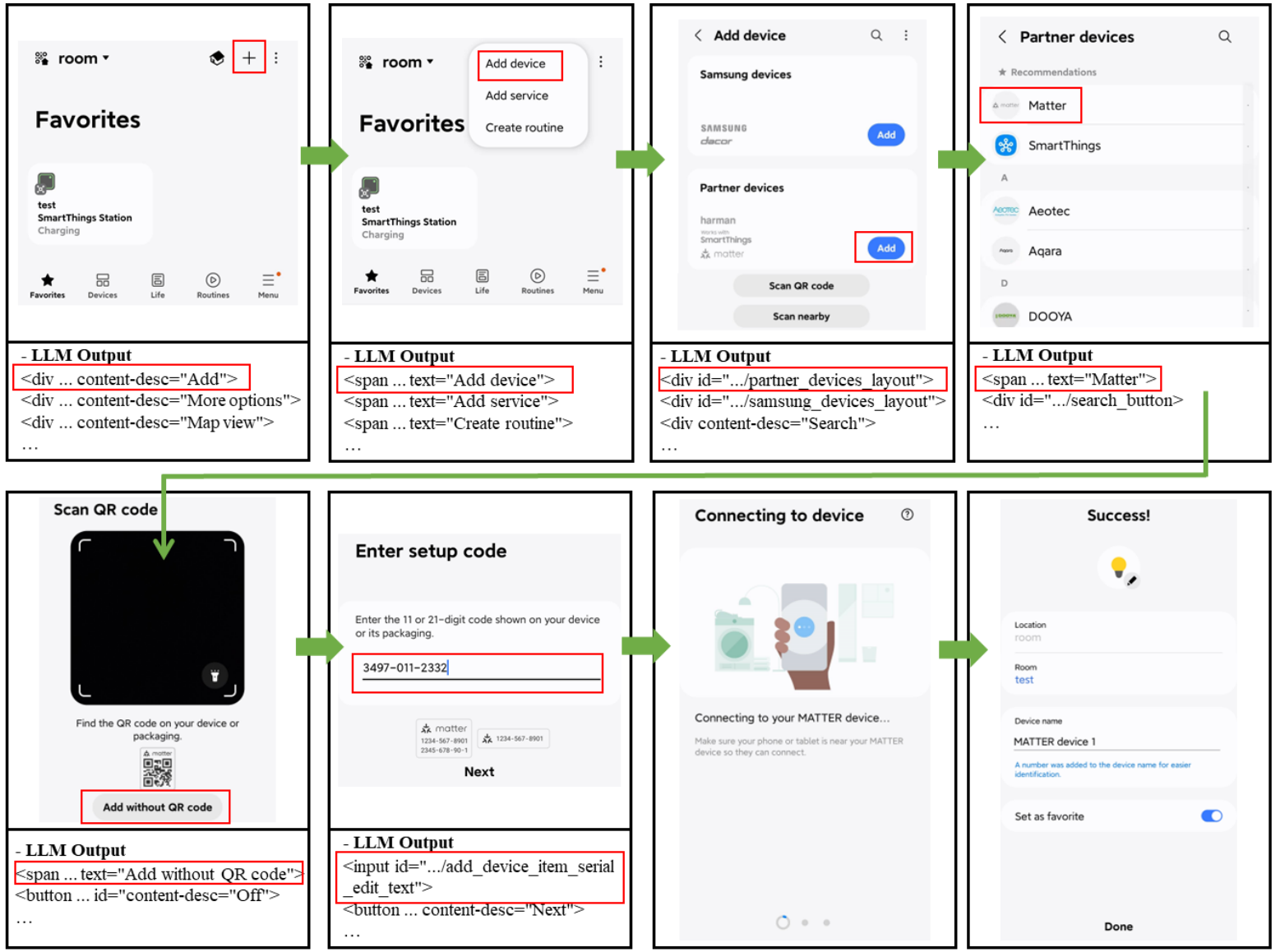
Step 1: Initializing the Virtual Matter Device Environment (VMDE).

Step 2: Initializing the SmartThings mobile app.



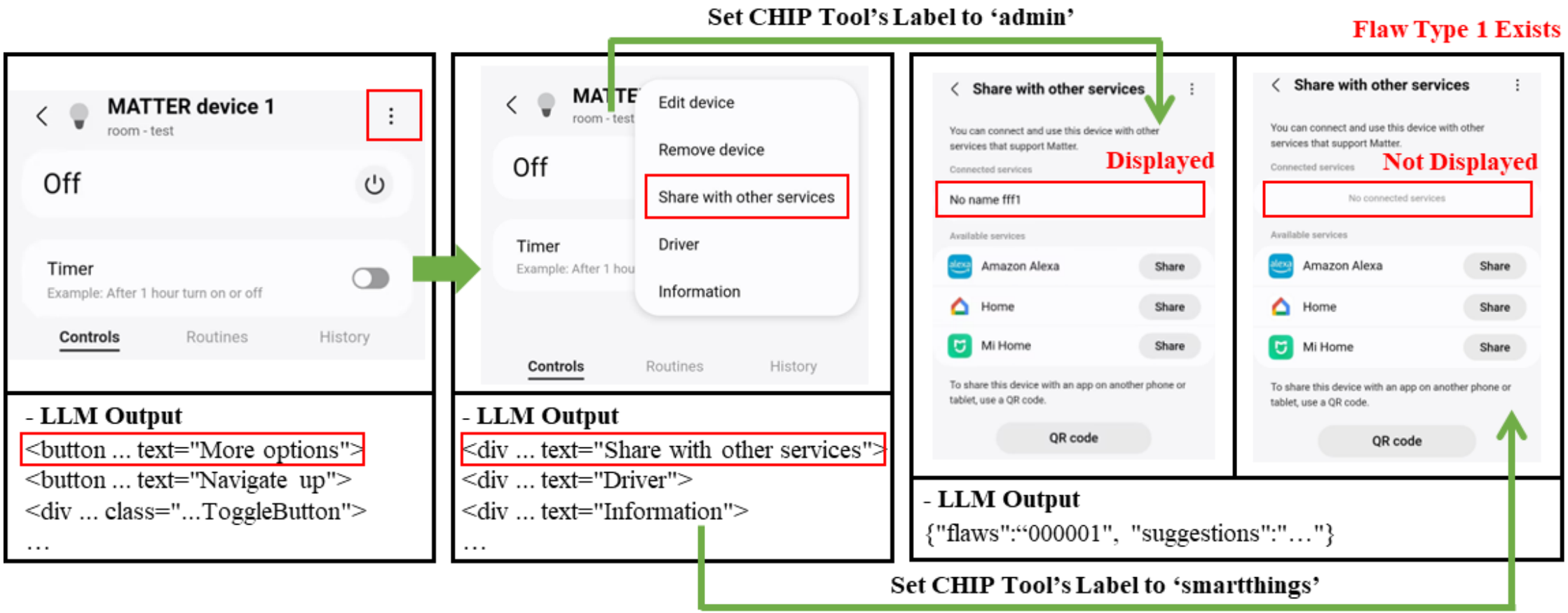
UMCCI Checker: One Example – Flaw Type 1

Step 3:
Automatic Device Pairing (ADP).



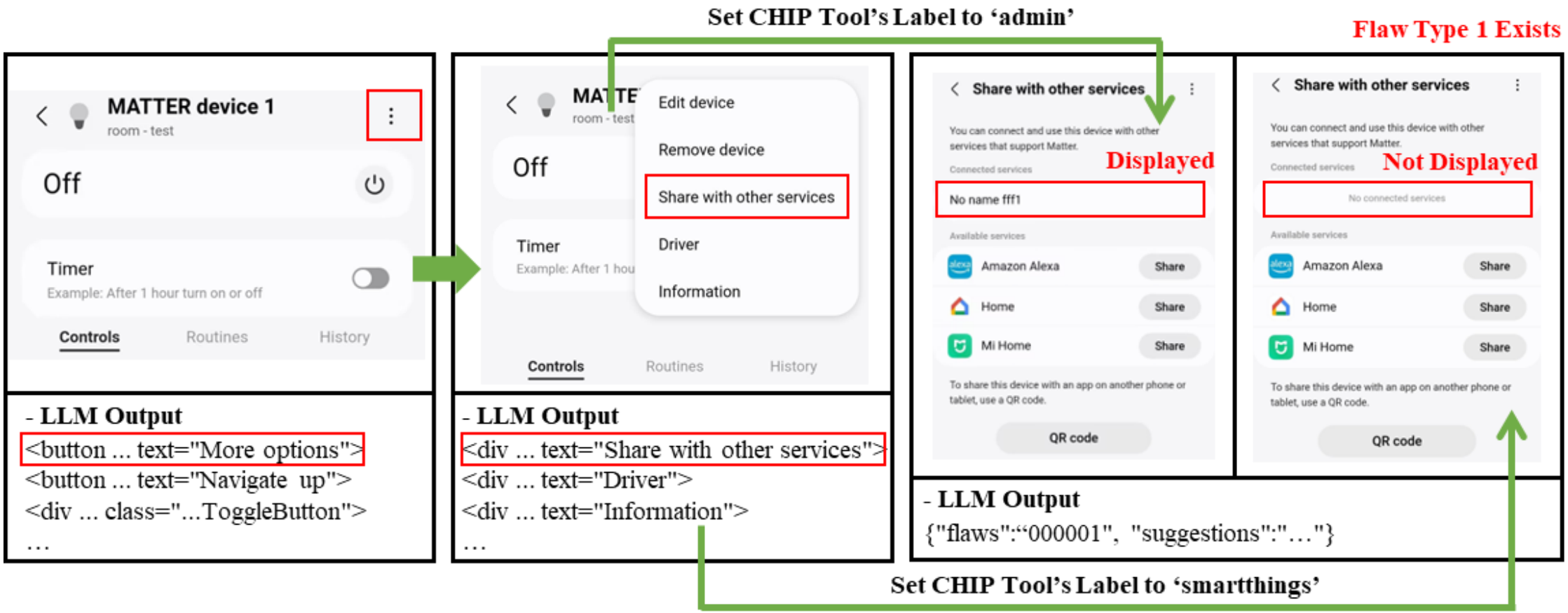
UMCCI Checker: One Example – Flaw Type 1

Step 4: Efficient Automatic UI Exploration (EAUE) explores and identifies all UMCCI pages in the SmartThings app.



UMCCI Checker: One Example – Flaw Type 1

Step 5: Flaw Analysis and Reporting (FAR).



Summary

- **New understanding and new attacks.**
  1. How vendors integrate Matter standard to IoT devices and applications
  2. The error space of vendors' Matter integration
  3. Novel root causes of security risks in vendors' integration of Matter

- **New detection and mitigation techniques.**
- **We discovered UMCCI flaws from 8 top-of-the-line IoT vendors that integrated the Matter standard, performed PoC attacks with 11 real devices, which have been acknowledged by CSA, Apple, Tuya, Aqara, etc.**

Thanks

Yichen Liu
Indiana University Bloomington
liuyic@iu.edu

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

中国科学院信息工程研究所
INSTITUTE OF INFORMATION ENGINEERING,CAS

INDIANA UNIVERSITY

STEVENS
INSTITUTE of TECHNOLOGY
THE INNOVATION UNIVERSITY