WIP: Security Vulnerabilities and Attack Scenarios in Apple Home with Matter

***Abstract*—The Matter protocol is a new communication standard for smart home devices, aiming to enhance interoperability and compatibility among different manufacturers. However, manufacturers may encounter unanticipated security issues during development and deployment phases centered around the Matter protocol. In this paper, we focus on examining vulnerabilities within Apple Home framework when implementing the Matter protocol, identifying several attack scenarios that can exploit these vulnerabilities to perform unauthorized actions and conceal their identities. We also compare the design of Apple Home with Google Home, highlighting the differences and implications for security. Our work reveals the challenges and risks associated with adopting the Matter protocol, and provides suggestions for improving its security design and implementation.**

I. Introduction

The Matter protocol is an emerging IoT connectivity standard designed to enhance interoperability and compatibility among smart home devices. Led by the Connectivity Standards Alliance (CSA), it is a collaborative effort involving major tech giants such as Apple, Google, and Amazon. The primary aim of the Matter protocol is to ensure that smart home products from different manufacturers can seamlessly connect and interact, providing users with a more convenient and unified smart home experience.

The Matter protocol is under active development and adoption by IoT manufacturers in the wild. Follow the new Matter standard, users are required to adapt and learn how to effectively utilize IoT devices featuring the Matter protocol, while manufacturers need to gain deep understanding about the protocol and securely adopt it for IoT devices. The manufacturers face challenges associated with transitioning from existing IoT protocols to the Matter protocol. Indeed, it is the manufacturers' struggle with the correct usage of the Matter protocol that leads to numerous defects in the framework and application design due to their initial lack of experience. These defects subsequently give rise to security issues that can be exploited by attackers.

This paper aims to analyze security weaknesses of the Matter protocol in the context of Apple Home, a popular smart home framework that integrated the Matter protocol. We identify several design flaws in Apple Home that allow attackers to establish covert control channels, obfuscate their identities, and gain access to devices that they are not authorized to access. We demonstrate the feasibility of these attacks by conducting proof-of-concept experiments using real devices supporting Matter. We also compare the design of Apple Home with that of Google Home, another smart home framework that supports the Matter protocol, and highlight the differences and implications. We envision that our findings can raise awareness of the security challenges and risks associated with the Matter protocol, and provide insights and suggestions for improving its security and usability.

II. Background

To better understand the security challenges and risks posed by the Matter protocol, we review some of its key features and components. Matter is a new, open smart home protocol that supports existing, familiar technologies, including Bluetooth Low Energy for device setup and Wi-Fi, Thread, and Ethernet for connecting devices. Matter supports a variety of popular smart home device categories, such as lighting, HVAC, security, media, and more. Matter also enables interoperability and compatibility among smart home products from different manufacturers and platforms, such as Apple, Google, Amazon, and others [4].

Network architecture and roles. The network architecture of the Matter protocol encompasses several principal concepts and roles as depicted in Figure 1 [3]. Devices within any protocol's network must coalesce in either a tangible or intangible form; such an aggregation in Matter is termed 'Fabric', which is a collective of Matter devices sharing a trusted root, identifiable by a Root Certificate Authority's public key and a unique 64-bit identifier designated as the Fabric-ID. Node is a fundamental entity within the network, which is an addressable unit that supports the Matter protocol stack. In each node there are lists called Clusters that define specific functions that the device can do. Once commissioned, it possesses its own Operational Node ID and Operational credentials, which are vital for its identity and secure communication within the fabric. The role of a node is defined differently from the perspectives of network configuration and device control, permitting a single node to assume multiple identity roles. The network configuration process, known as Commissioning, is aimed at integrating a node into the fabric. From the standpoint of Commissioning, the roles of node are categorized as Commissioner and Commissionee. The Commissioner acts as the initiator and principal conductor of the Commissioning activities, typically manifested as an application provided by the manufacturer, which involves the integration of a new entity as a node within the fabric. The Commissionee is the recipient of network configuration, generally representing various types of end devices such as light bulbs, door locks, etc. Following the completion of Commissioning, the phase transitions to device control. In the context of device control, the roles of node are differentiated

as Controller and Controllee. The Controller initiates device control commands, often represented by traditional gateway devices. The Controllee is usually the same variety of end devices that are equivalent to Commissionee [6].

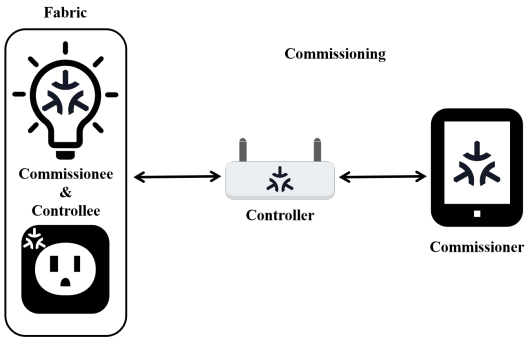

Fig. 1. The Node-Role overview illustrates the interconnections between different node roles within Matter network.

Security features. Matter employs a comprehensive security model, covering aspects such as device identity, authentication, authorization, encryption, and attestation. Matter uses X.509 certificates to establish device identity and trust. Each device has a unique node ID and a corresponding node operational credential, which is a certificate signed by a fabric authority. The fabric authority is a trusted entity that issues and revokes certificates for devices within a fabric. Matter also supports manufacturer attestation, which allows devices to prove their provenance and firmware information using manufacturer certificates [7].

Matter implements a secure session establishment protocol, called Sigma, to enable authenticated and encrypted communication between devices. Sigma is based on the Secure Remote Password protocol (SRP), which is a password-authenticated key exchange protocol that does not require public-key cryptography [5]. Sigma involves three phases: session initiation, key exchange, and secure transport. In the session initiation phase, the initiator and the responder exchange hello messages that contain their respective node IDs and random nonces. In the key exchange phase, the initiator and the responder use SRP to derive a shared secret and a session ID, and also verify each other's node operational credentials. In the secure transport phase, the initiator and the responder use the session ID to derive encryption keys and use AES-CCM to encrypt and authenticate their messages [7].

Matter also provides a flexible and granular authorization mechanism, based on the concept of subjects, targets, and privileges. Subjects are entities that can initiate requests, such as commissioners and controllers. Targets are entities that can process requests, such as devices. Privileges are actions that subjects can perform on targets, such as read, write, or execute. Matter defines an access control list (ACL) for each device, which specifies the privileges that different subjects have on different targets. The ACL can be configured by the device owner or the commissioner, and can be updated dynamically [7].

The Matter protocol exhibits robust security in its foundational design. However, due to its novelty and offering an complex array of IoT functionalities, manufacturers may create unanticipated security issues during development and deployment phases using the Matter protocol. Even in the absence of inherent security flaws within the Matter protocol and the devices that implement it, vulnerabilities may arise from incorrect invocation methods. For example, manufacturers may be prone to logical errors in functionality during the design process of client applications, resulting in the execution of undefined privilege escalation operations. Attackers can exploit these vulnerabilities to perform unauthorized actions and conceal their identities, ultimately gaining full control of devices without the owner's knowledge. In this paper, we focus on examining vulnerabilities within Apple's Apple Home framework when implementing the Matter protocol, identifying the following vulnerabilities and attack scenarios:

- Threat Model
- Covert Control Channels
- Fabric Manufacturer Name Obfuscation
- Comparison with the Google Home

We also discuss the possible mitigation strategies and recommendations for improving the security of the Matter protocol and its applications.

III. Attacks

In this section, we focus on examining vulnerabilities within Apple Home framework when implementing the Matter protocol. We identify the following vulnerabilities and attack scenarios.

A. Threat Model

We consider real-world device-sharing scenarios, assuming that the adversary can have temporary access to the Matter devices in a host's room. The adversary is capable of using apps and development tools to connect with and interact with the Matter devices, as well as collecting and analyzing network traffic. We assume that the infrastructure systems of the IoT and the Matter protocol (including IoT hardware and device firmware and so on) are benign, and the adversary cannot eavesdrop on or affect the communication of other users' Matter devices or apps.

B. Covert Control Channels

Chip-tool is an open-source development tool for the Matter protocol, functioning as a comprehensive command-line Matter control terminal for device debugging. However, chip-tool can be used to construct covert control channels to control the Matter devices. To facilitate our experiments, we compiled chip-tool and utilized it throughout our study. In Apple Home, pairing with Matter devices is achieved either by scanning their QR codes or entering their pairing codes. A similar process can be employed in chip-tool.

We paired a Matter light bulb (Abbreviated as L) with both Apple Home and chip-tool. Under normal circumstances, once a device is paired with a controller, it joins the controller's

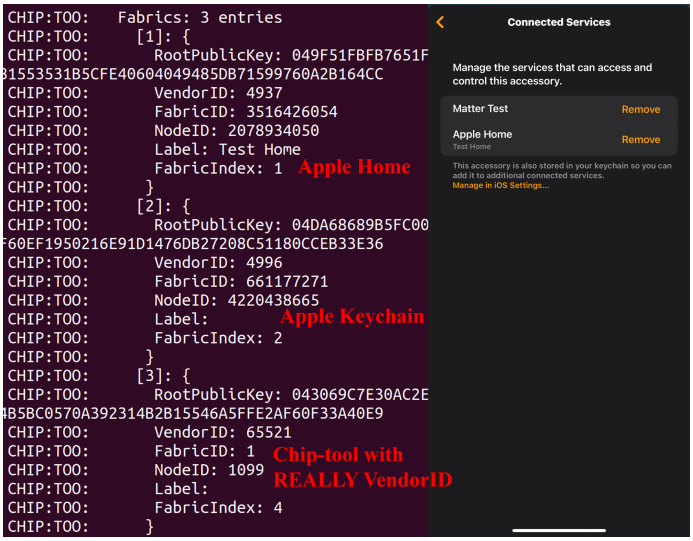

Fig. 2. Upon examining the fabric information of L through both the chip-tool and Apple Home, it is observed that the existence of the Apple Keychain is obfuscated within Apple Home.

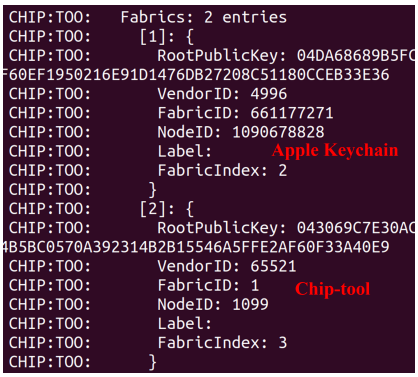

Fig. 3. Devices removed from Apple Home retain the fabric of the Apple Keychain.

fabric. Thus, L should be part of two fabrics, one each for Apple Home and chip-tool. This was confirmed upon inspecting L's connected services in Apple Home. However, the reality was different. Utilizing the operationalcredentials cluster in chip-tool to read L's fabric revealed the existence of three fabrics (Figure 2) . VendorID represents the manufacturer number certified by the CSA organization. Upon investigation, it was ascertained that 4937 denotes Apple Home, 65521 represents chip-tool, while the additional 4996 corresponds to the Apple Keychain service. It is evident that Apple Home actively conceals the fabric of Apple Keychain service in its list of connected services. Upon reviewing Apple's developer documentation, the Apple Keychain service is designed to facilitate the quick re-pairing of Matter devices after their removal by the device owner [2][1]. Subsequently, when L was removed from Apple Home, a further inquiry into L's fabric using chip-tool revealed that the fabric associated with Apple Home, having the VendorID 4937, had disappeared. However, the fabric corresponding to the Apple Keychain, identified by VendorID 4996, remained present as depicted in Figure 3. The root cause of this flaw is the absence of authentication for the VendorID.

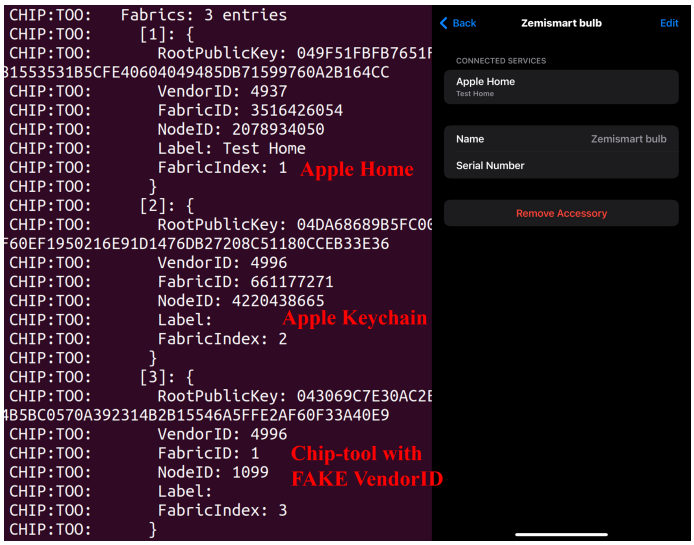

Fig. 4. Attackers can exploit the characteristic of Apple Keychain being concealed within the list of connected services in Apple Home to establish a covert control channel to the device.

In light of the identified display flaw in Apple Home, we have devised several potential attack scenarios.

PoC exploit 1. We utilized the –commissioner-vendor-id parameter in chip-tool to arbitrarily assign chip-tool's VendorID during device pairing, setting it to 4996 to masquerade chip-tool as the Apple Keychain. After resetting L to factory settings, we repeated the pairing process with both Apple Home and the chip-tool with the modified VendorID. When querying L's connected services via Apple Home, we noticed that only the Apple Home fabric was visible, with the chip-tool disguised as Apple Keychain remaining undetected (Figure 4) . This led us to construct an attack scenario: An owner using Apple Home shares the device pairing code with a guest, who is actually an attacker, through the Matter protocol. The attacker can freely choose their Matter control terminal, including chip-tool. By altering the VendorID to 4996 during the pairing process with the owner, the attacker becomes invisible in Apple Home, effectively establishing a covert control channel within the Matter protocol.

PoC exploit 2. The prerequisite for using Apple Home is the necessity of a HomePod or Apple TV as Home Hub for its functionality. As mentioned earlier, the purpose of the Apple Keychain service is to facilitate quick re-pairing of Matter devices after their removal. However, this feature can be exploited by attackers to regain control of unbound devices without permission. We set up two HomePod minis, each paired with a different iPhone and iPad logged into separate Apple IDs. We paired the Matter device L with the Apple Home on both the iPhone and iPad, and observed that L appeared in the connected device list of both (representing the iPhone and iPad). After removing the iPad's control terminal

for L from the iPhone's Apple Home, the device disappeared from the iPad's Apple Home. However, L remained in the iPad user's Apple Keychain fabric. By attempting to add a device in the iPad's Apple Home, L appeared in the recently added devices, allowing the iPad to regain full control over L without the iPhone's permission. Figure 6 in Appendix A is a demonstrative schematic representation of the entire attack process. This led us to construct an attack scenario: An attacker, posing as a guest, brings their own HomePod, which facilitates the attack. The host, using Apple Home, shares the device pairing code with the attacker through the Matter protocol. The attacker can then pair with the host's device using Apple Home and their own HomePod. Even if the host removes the attacker's control terminal from Apple Home, the invisibility of Apple Keychain in Apple Home prevents the host from fully unbinding the attacker, who can regain control over the host's devices anytime nearby via Apple Home and HomePod.

C. Fabric Manufacturer Name Obfuscation

The VendorID specifically refers to the manufacturer in the Matter protocol. When querying connected services of a device in Apple Home, the connected control terminal's manufacturer name and Label information are displayed, but not the specific VendorID. In contrast, chip-tool displays detailed information such as VendorID, NodeID, and more. We have noted that the –commissioner-vendor-id parameter in chip-tool can be used to simulate a different manufacturer. Similarly, we can utilize the update-fabric-label command in the operationalcredentials fabric to customize Label information. When a host shares a device to an attacker who using with a chip-tool that has modified manufacturer-related data, the attacker can tailor their manufacturer information, potentially misleading the host with false information in the connected services list, leading to erroneous actions. This display flaw in Apple Home allows us to construct the following attack scenario.

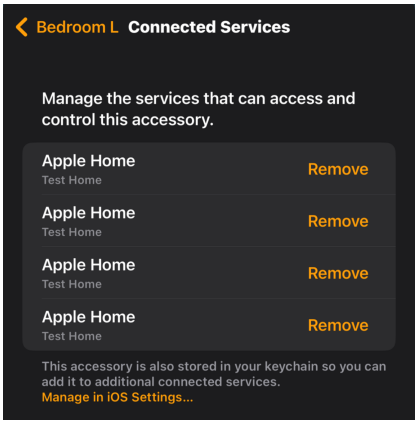

Fig. 5. The host is entirely incapable of discerning which is his own Apple Home and which belongs to the attacker.

PoC exploit. We employed multiple instances of chip-tool, each set with the VendorID 4937, identical to that of Apple Home. Subsequently, the genuine Apple Home and these modified chip-tools were individually paired with the Matter device L. Upon inspecting L's connected services list through Apple Home, an unusually high number of Apple Home manufacturers were observed. Since Label information can also be customized, it became challenging for the host to discern the authentic Apple Home service as depicted in Figure 5. This allows us to construct an attack scenario: The host, using Apple Home, shares the device's pairing code with a guest, who is an attacker, through the Matter protocol. The attacker can then pair multiple chip-tools, with altered manufacturer information, with the host's device. Consequently, the host may struggle to distinguish the real manufacturer from the forged ones in the list of connected services.

D. Comparison with the Google Home

To validate the existence of design flaws in Apple Home, we also conducted tests on the connected services query function of Google Home. In Google Home, connected services do not display the manufacturer's name, but only the VendorID and Label. Moreover, Google Home's own services are distinctly marked with special explanatory labels, replacing the regular Label information, and services from the same VendorID but not belonging to Google Home are indicated with a different string, "Added by another user." as depicted in Figure 7, Appendix B. This approach effectively prevents attacks that might involve masquerading as Google Home using tools like chip-tool. Consequently, it is evident that Google Home has incorporated thoughtful design considerations in this aspect, thus affirming the presence of display flaws in Apple Home's design.

IV. Conclusion

In this study, we've analyzed the security issues in the Matter protocol, a new IoT standard, particularly focusing on Apple Home's vulnerabilities. We demonstrated attack scenarios that could exploit these weaknesses, and compared Apple Home with Google Home, noting Apple Home's design flaws. Our research suggests that despite Matter's robust design, implementation challenges persist. These vulnerabilities may not be unique to Apple Home but prevalent across various smart home frameworks using the Matter protocol. Manufacturers should adopt best practices to mitigate these risks, and users should remain vigilant. Additionally, the CSA and Matter protocol developers need to address these security gaps. Future work will involve a broader security analysis of Matter, covering aspects like network protocols and encryption, and exploring further countermeasures to enhance security and privacy.

References

[1] Apple., "Set up iCloud Keychain," 2023, accessed: 2023-12-30. [Online]. Available: https://support.apple.com/en-us/HT204085
[2] Apple, "Use iCloud Keychain to keep information safe on your Mac, iPhone, and iPad," 2023, accessed: 2023-12-30. [Online]. Available: https://support.apple.com/en-us/102135
[3] Connectivity Standards Alliance. (2023, Oct.) Matter 1.2 core specification. [Online]. Available: https://csa-iot.org/wp-content/uploads/2023/10/Matter-1.2-Core-Specification.pdf

[4] CSA-IOT, "Matter FAQs — Frequently Asked Questions," 2023, accessed: 2023-12-30. [Online]. Available: https://csa-iot.org/all-solutions/matter/matter-faq/
[5] Espressif, "Matter Security Model. Espressif Matter Series #7," 2023, accessed: 2023-12-30. [Online]. Available: https://blog.espressif.com/matter-security-model-37f806d3b0b2
[6] Infineon, "The Matter Standard: Implementing Improved Security and Connectivity," 2023, accessed: 2023-12-30. [Online]. Available: https://www.infineon.com/dgdl/Infineon-Matter_Connected_Things-Whitepaper-v02_00-EN.pdf?fileId=5546d46279cccfdb017a0ae13d3427c3da=t
[7] Security Boulevard, "Q&A: Here's how the 'Matter' protocol will soon reduce vulnerabilities in smart home devices," 2022, accessed: 2023-12-30. [Online]. Available: https://securityboulevard.com/2022/08/qa-heres-how-the-matter-protocol-will-soon-reduce-vulnerabilities-in-smart-home-devices/

APPENDIX

A. Covert Control Channels

Attackers can regain control over Matter devices that have been removed from Apple Home without the homeowner's permission.

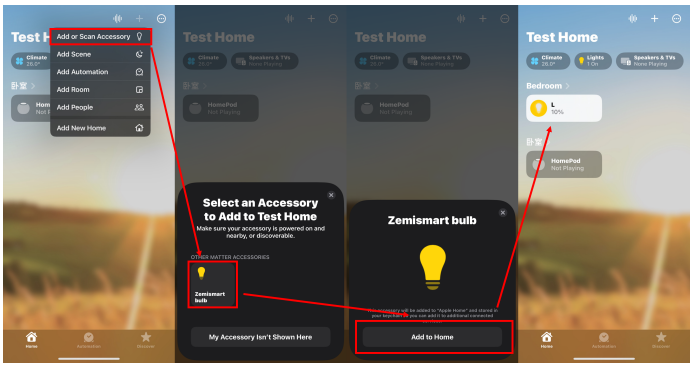

Fig. 6. Utilizing the Apple Keychain service, attackers can restore control over devices that have been compromised using the method illustrated in this figure.

B. Comparison with the Google Home

Google has taken security considerations into account regarding the display of information such as VendorID in the query list of connected services for Matter.

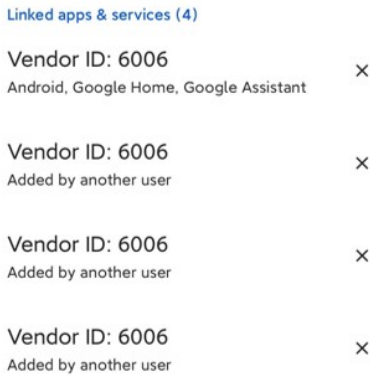

Fig. 7. Google Home employs unique string markers to circumvent potential display flaws.