WIP: Hidden Hub Eavesdropping Attack in Matter-enabled Smart Home Systems

Song Liao
Clemson University
liao5@g.clemson.edu

Jingwen Yan
Clemson University
jingwey@g.clemson.edu

Long Cheng
Clemson University
lcheng2@clemson.edu

***Abstract*—The rapid evolution of Internet of Things (IoT) technologies allows users to interact with devices in a smart home environment. In an effort to strengthen the connectivity of smart devices across diverse vendors, multiple leading device manufacturers developed the Matter standard, enabling users to control devices from different sources seamlessly. However, the interoperability introduced by Matter poses new challenges to user privacy and safety. In this paper, we propose the Hidden Eavesdropping Attack in Matter-enabled smart home systems by exploiting the vulnerabilities in the Matter device pairing process and delegation phase. Our investigation of the Matter device pairing process reveals the possibility of unauthorized delegation. Furthermore, such delegation can grant unauthorized Matter hubs (*i.e.*, hidden hubs) the capability to eavesdrop on other IoT devices without the awareness of device owners. Meanwhile, the implementation flaws from companies in device management complicate the task of device owners in identifying such hidden hubs. The disclosed sensitive data about devices, such as the status of door locks, can be leveraged by malicious attackers to deduce users' activities, potentially leading to security breaches and safety issues.**

I. Introduction

The emerging Internet of Things (IoT) technologies allow users to seamlessly interact and control their smart devices within their homes. In 2023, there are 16.7 billion connected IoT devices worldwide [4]. Through mobile apps or other interfaces, users can effortlessly manage and operate their devices, such as lighting, cameras, door locks, and thermostats. However, IoT devices made by different vendors typically work within their own ecosystems, compelling users to manage them using different vendors' official apps. This fragmentation significantly impacts the user's experience and diminishes their enthusiasm to explore and adopt new devices.

To bridge the gap between various vendors and alleviate the inconvenience of users in interacting with devices from diverse companies, multiple vendors, including Apple, Amazon, Google, and Samsung, introduced and developed the Matter standard [3]. Matter is an open-source connectivity standard based on internet protocol for smart home and IoT devices, aiming to improve interoperability and compatibility between different manufacturers. With Matter, users can control devices with any Matter-compatible platform from diverse ecosystems to manage Matter devices within a home efficiently, as depicted in Figure 1.

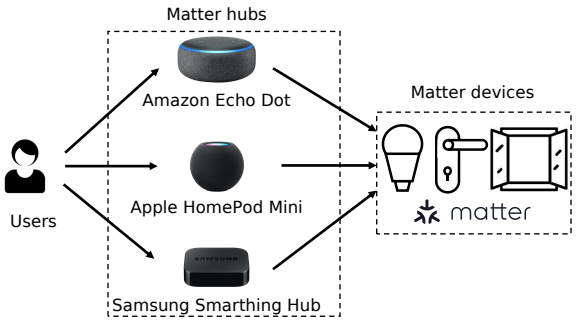


Fig. 1: Utilizing hubs from different ecosystems to control Matter devices with a Matter logo.

While the Matter standard enhances the connectivity and interoperability of devices, it also aggregates the risk of device data leaks. IoT devices, particularly Matter-enabled devices, often require sharing with multiple users, such as tenants and Airbnb guests. These users need Matter controllers (also known as "hubs") [1] to communicate with Matter devices. The owner of the device (the primary user) can directly add a Matter device to the hub, while subsequent users (secondary users) are required to request permission access from the primary user. Once connected, each connected hub has the capability to obtain the update of device status. Existing researchers [12] have demonstrated that such status changes of IoT devices (typically defined as an event), *e.g.*, lights and door locks, can be exploited by malicious users to deduce users' daily activities. This susceptibility may give rise to further malicious behaviors, including potential break-ins by burglars, posing risks to users' privacy and physical safety. In such a scenario, the trustworthiness of the Matter hub and the effectiveness of the delegation procedure become critically important.

In this work, we reveal the vulnerabilities in the pairing process of Matter devices and hubs. We uncover that the Matter hub delegation procedure poses a real-world threat, leading to the existence of unauthorized hubs beyond the

Workshop on Security and Privacy in Standardized IoT (SDIoTSec) 2024
26 February 2024, San Diego, CA, USA
ISBN 979-8-9894372-6-9
https://dx.doi.org/10.14722/sdiotsec.2024.23089
www.ndss-symposium.org

[1] In this work, we refer to the Matter-enabled IoT devices as "Matter device" and Matter controller as "Matter hub".

control of the primary owner of IoT devices. Given that device data is shared among all hubs connected to a device, users' device data could be exposed to an unintended party. Malicious users can connect such an unauthorized hub to devices and hide it to retrieve data from IoT devices stealthily. We intend to disclose these vulnerabilities to vendors and Matter manufacturers.

II. Background

In recent years, there has been an emergence of more protocols related to IoT devices, *e.g.*, Zigbee [7], Z-Wave [6], and Thread [5]. To simplify the development for smart home product brands and manufacturers and increase the compatibility of the products for consumers, Amazon, Google, Apple, Samsung and other members of CSA (Connectivity Standards Alliance), the formerly Zigbee Alliance, started to collaborate and format the group of Project Connected Home over IP [1], [2]. The first version of the Matter was published on 4 October 2022 (Version 1.0), which supports lighting products (*e.g.*, plugs, lights, and switches), door locks, thermostats and heating, and air conditioning controllers, etc. Different from Zigbee, which runs on the physical, data link and network layer, Matter is a local IPv6-based wireless connectivity technology on the application layer, designed to enhance connectivity and interoperability among IoT devices made by different manufacturers.

III. Vulnerabilities in Matter Device Pairing

A. Matter-Supported Devices and Hubs

To help users easily distinguish Matter devices from existing devices with protocols like Zigbee or Bluetooth, Matter devices typically have the Matter logo on their packaging, as presented in Figure 1. A comprehensive list of device types that Matter supports by the end of October 2023 is provided in Table I. Concurrently, various smart home manufacturers, *e.g.*, Amazon, Google and Apple, are incorporating Matter support into their existing devices with software updates.

Matter-supported Device Types
Light bulbs and light switches, Plugs and outlets, Locks, Thermostats and other HVAC controllers, Room air conditioners, Air purifiers, Fans, Blinds and shades, Robot vacuums, Refrigerators / Freezers, Washing machines, Dishwashers, Televisions and media devices, Smoke and CO alarms, Safety and security sensors, Air quality sensors, Bridges

TABLE I: Matter-supported devices.

Users need a Matter hub to effectively interact with and manage Matter devices. Typically, such a hub should be a smart device always with WiFi connection to the network. Multiple vendors have implemented updates to enable their devices to function as Matter hubs. Table II shows the devices from prominent vendors that can function as a Matter hub.

B. Device Pairing and Delegation

Once setting up a Matter hub, users can connect a Matter device to the hub using the corresponding mobile app. Figure 2 illustrates the necessary steps of the pairing process between the device and the hub. The app first asks users whether the device supports Matter and has a Matter logo. Subsequently, users are required to scan the QR code on the device or manually input the unique 11 or 21-digit numeric code associated with the device. For the device that is initialized for the first time, the pairing process concludes and the connection is established, after which users can control the device using the Matter protocol through their mobile apps.

Company	Matter-Supported Hubs
Amazon	Amazon Echo, Echo Pop, Echo Dot, Echo Studio, Echo Show, Echo Input, Flex, and Plus, Echo, Eero
Google	Google Home, Google Home mini, Nest Mini, Nest Audio, Nest Hub, Nest Hub Max, Nest Wifi Pro
Apple	Apple HomePod, Apple HomePod Mini, Apple TV
Samsung	Samsung SmartThings Hub, Family Hub fridge, Smart Monitors, Smart TVs
Others	Nabu Casa Home Assistant Yellow, Home Assistant (Sky Connect dongle), Comcast xFi Advanced Gateway, Hubitat Elevation Model C-8 hub, Home Assistant software, Mui

TABLE II: Matter-supported hubs.

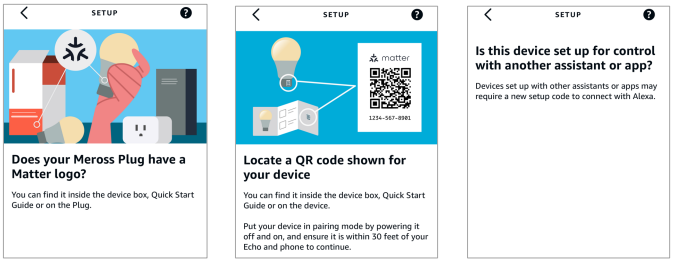


Fig. 2: Device pairing steps

The Matter standard is primarily designed to establish connectivity bridges among IoT devices operating in diverse IoT platforms (*e.g.*, Amazon Alexa, Google Home, and Samsung Smartthings). Therefore, it is possible that multiple users can manage the same Matter device using their respective hubs within a shared smart home environment. For instance, one user can use Amazon Alexa while another user may use a different hub (*e.g.*, Google Assistant) to control the same lighting bulb. When a Matter device is already connected to a hub owned by a primary user, the pairing process to add the device to the second hub involves an additional step, which requires a pairing code from the hub that is already associated with the device, as indicated in Figure 2. The primary user has the option to generate the pairing code through the mobile app, afterward sharing it with the secondary user, thereby delegating the control of the device to the secondary user. The pairing code has a 15-minute valid period, a security measure that is intended to protect devices' integrity and prevent arbitrary connection.

Upon establishing device connections with different hubs, multiple users can operate the same device through different Matter hubs. When one of the hubs changes the device status, *e.g.*, turning on a light, other connected hubs will promptly receive a message to update the status of the device accordingly.

C. Unauthorized Delegation Vulnerabilities

As we discussed above, Matter makes an effort to improve compatibility and interoperability between devices and protect the delegation phase. However, we found the following vulnerabilities in this procedure, leading to the potential Hidden Hub Eavesdropping Attack (details in Section IV).

Unauthorized delegation: During the pairing stage, the secondary user requires a pairing code from the primary user to establish the delegation and connect a hub to a device (with a limitation of at most five hubs per device). However, we found that the secondary user possesses the capability to delegate the device to additional users by generating a pairing code on his/her mobile app without seeking permission from the primary user. This can result in unauthorized delegations occurring beyond the primary's control.

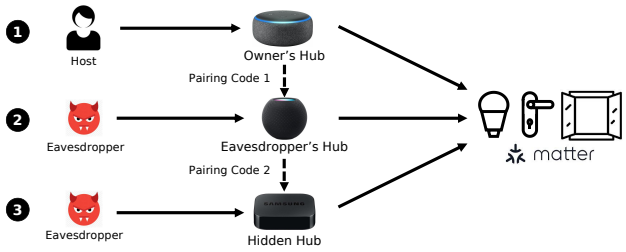
Eavesdropping risk by unauthorized hubs: Matter devices have the capability to connect with multiple hubs, each of which can retrieve the status of devices, *e.g.*, whether a light is on or a door lock is closed. However, by exploiting the unauthorized delegation vulnerability, the presence of a malicious hub poses a significant threat, allowing unauthorized monitoring of IoT device status in a smart home. A more severe situation appears when certain sensitive devices like door locks are monitored, which could be exploited by an attacker to cause a potential problem of break-in [10].

Implementation flaws in device management: In the context of hidden hub eavesdropping, the primary user may identify such a hidden hub by inspecting the device connections through mobile apps. However, our study reveals that several prominent vendors, including Amazon and Google, don't provide a friendly function for device management in their apps, leading to users having difficulty managing hubs to which devices connect. Although Matter does provide this functionality, several companies haven't implemented it into their apps, which provides attackers the potential to launch the hidden hub eavesdropping attack.

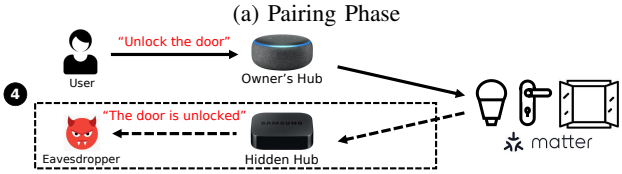
IV. Hidden Hub Eavesdropping Attack

Threat Model: Today, IoT devices often need to be shared with multiple users, such as patients, tenants, and Airbnb guests. These users will be granted temporary access and such temporary permission is realistic in the real world, such as vocational rental services [13], [11], [9]. Therefore, we assume that malicious users may temporarily come in close proximity to target victim Matter devices. For example, an Airbnb guest checks into a home equipped with a smart door lock and a Matter hub. In our attack, we assume that the host shares the pairing code with malicious users (*e.g.*, temporary tenants) so that they can connect devices to their own hub. We also assume that the host does not manually remove the QR code on devices so that malicious users can scan it and add devices to their hubs.

Figure 3 illustrates the hidden hub eavesdropping attack scenario, which includes the following two phases: **Pairing Phase** and **Eavesdropping Phase**.



(a) Pairing Phase



(b) Eavesdropping Phase

Fig. 3: Two phases in hidden hub eavesdropping attack

(1) In an Airbnb room, the host has installed Matter devices, *e.g.*, smart lock and lights, and linked them to a Matter hub, allowing guests to utilize the hub for smart device control.

(2) After malicious users temporarily come into the room, they can claim to utilize their own hubs for smart device control through their mobile app and promise to terminate the hub connection upon departure. The host may share the pairing code with malicious users through the host's management app. With the QR code on the device and the pairing code from the host, malicious users can set up their first hub (Eavesdropper's hub in Figure 3) and use it to control the device in the home.

(3) Malicious users can arbitrarily integrate authorized Matter devices within the room into their second hub (Hidden hub) or even more hubs without the awareness of the host. This process can be easily executed by scanning the QR codes on devices and sharing the pairing code generated by the first hub (Eavesdropper's hub), all without obtaining permission from the host due to the vulnerability of unauthorized delegation.

(4) When malicious users check out and leave the room, they can disconnect the first hub (Eavesdropper's hub) in the presence of the host, creating a deceptive impression that the devices in the room are already disassociated from the malicious users' hub. Meanwhile, malicious users can hide their second hub (Hidden hub) in close proximity to the room, ensuring a persistent connection to the devices within the room to exploit the eavesdropping risk. After that, malicious users can use the hidden hub to eavesdrop on the status of IoT devices in the smart home, including the instances of turning lights on/off and unlocking the lock. The gathered information can be leveraged to deduce the host's timeline and determine the host's absence, resulting in the potential problem of a break-in.

V. Case Study

To validate whether the Hidden Hub Eavesdropping Attack is realistic, we implemented an experiment following the steps in our attack scenario. The host set up two benign hubs in a room - an Amazon Echo and a Google Nest Mini - both connected to a Matter-enabled light and a plug. The malicious user possesses two hubs, an Amazon Echo and an Amazon

Echo Dot. The objective is to connect a hidden hub to the devices and monitor the hosts' devices. It is noteworthy that any other Matter hubs in Table II can also be deployed in our experiments.

As a result, the malicious user successfully established the hidden hub, exploiting it to monitor the device status during another hub disconnection discreetly. Figure 4 presents the device management interface on the malicious user's mobile app. Upon the host changing his/her devices (a plug and a light), the malicious user's hidden hub and app promptly received the device status update. In contrast, the host was unable to locate the hub management on his/her mobile app, remaining unaware of the existence of the hidden hub. A demo video of our experiment is available at https://github.com/Matter-attack/Matter-attack.

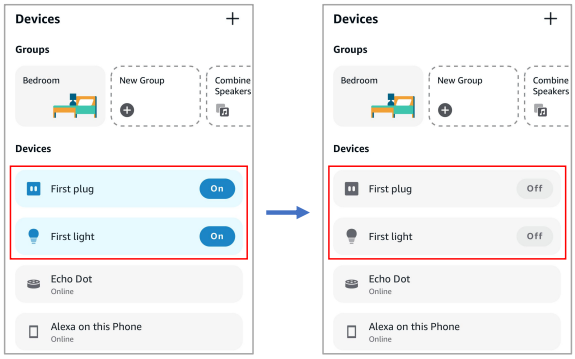


Fig. 4: Device status on the hidden hub changed after the host changed the status of the devices.

VI. Discussion

A. Implication

Matter protocol is designed to bridge the gaps among various vendors, aiming to enhance the connectivity between manufacturers. However, the convenience and the potential risk associated with data sharing represent a trade-off. This integration poses potential risks and vulnerabilities to the security of sensitive device data. Inevitably, as device data is shared with more devices to enhance convenience, the higher risk of unauthorized leaks intensifies privacy concerns. Focusing on the risky delegation process, this work reveals the vulnerabilities in Matter devices and hubs pairing procedure. Malicious users can monitor device status using hidden hubs without being detected, as presented in our experiments. Given that smart home devices have the potential to make an impact on the physical world, such data leaks may lead to severe consequences and pose a threat of harm to users. Under such a scenario, vendors are supposed to make more effort to safeguard user data and assist users in effectively managing their devices.

B. Possible Mitigation

Based on the vulnerabilities we found and the proposed attack scenario, we provide the following recommendations to mitigate the issues in Matter device management:

Authorization from the host: When delegating devices to other users, the authorization, including the pairing code, should be obtained from the initial hub, which is intended to be the primary owner of the devices rather than the secondary or subsequently authorized hubs. This configuration enhances the host's ability to effectively manage each hub that establishes a connection and controls the device.

Better device management for owners: While Matter incorporates the functionality for device owners to ascertain the number of hubs their devices are connected to, this feature has not been universally integrated into various vendors' apps. For instance, Amazon Alexa app doesn't provide such a function while Google Home only provides the vendor IDs of each device instead of the device name. Apple, however, already offers such a complete function. This capability empowers smart device owners to inspect the connection status of their devices, revealing the details about hub behaviors. Once the owner identifies suspicious hubs connected to his device, they can promptly remove them.

Abnormal network traffic detection: In addition to hub management, device owners can examine the network traffic of connected devices. Upon owners detect unusual network activity from a device, they can remove the connection or reinitialize the device to erase all associated connections.

Guest mode for delegated hubs: If the previous mitigation is not implemented, Matter should consider incorporating a guest mode and implementing a time restriction for guest hubs. In this approach, Matter can terminate the connection between devices and non-owner hubs after a designated time.

VII. Related Work

As one of the most advanced and newest IoT standards, Matter has already been the focus of several research works despite being published only one year ago. Shashwat *et al.* [15] analyzed the security risks and the trustworthiness of Matter controllers. Different from our work, this work investigated the risk of users installing malicious controllers inadvertently. Basyal *et al.* [8] constructed a Linux-based virtual platform for the exploration of Matter protocol and conducted a security scan to identify breaches and vulnerabilities. Zegeye *et al.* [16] presented that Matter protocol can be used to solve the long-standing heterogeneity problem in smart homes. Mihaeljans *et al.* [14] provides an overview of the IoT framework focusing on the Matter protocol and Thread technology.

VIII. Conclusion

In this work, we identified real-world vulnerabilities in the Matter-enabled device pairing process. By exploiting these vulnerabilities of unauthorized delegation and device management, we proposed the hidden hub eavesdropping attack, which allows malicious users to keep eavesdropping on device status using a hidden hub that the host is unaware of. We demonstrated the realism of the attack in our experiments and discussed potential mitigation to the Matter vendors.

Acknowledgment

The work is supported by National Science Foundation (NSF) under the Grant No. 2239605, 2228616 and 2114920.

REFERENCES

[1] Apple, Google, Amazon Want One Language for Smart Devices. https://www.bloomberg.com/news/articles/2019-12-18/apple-google-amazon-want-one-language-for-smart-home-devices.

[2] Apple, Google and Amazon are cooperating to make your home gadgets talk to each other. https://www.cnbc.com/2019/12/18/apple-google-amazon-zigbee-partner-on-smart-home.html.

[3] Matter: The Foundation for Connected Things. https://csa-iot.org/all-solutions/matter/.

[4] State of IoT 2023:. https://iot-analytics.com/number-connected-iot-devices/.

[5] What is Thread. https://www.threadgroup.org/What-is-Thread/.

[6] Z-Wave. https://www.z-wave.com/.

[7] Zigbee. https://csa-iot.org/all-solutions/zigbee/.

[8] Lochan Basyal, Chenglong Fu, and Xiaojiang Du. Iot security with matter protocol: Exploring a secure and reliable home automation.

[9] Dongmei Cao, Yan Sun, Edmund Goh, Rachel Wang, and Kate Kuiavska. Adoption of smart voice assistants technology among airbnb guests: A revised self-efficacy-based value adoption model (svam). *International Journal of Hospitality Management*, 101:103124, 2022.

[10] Wenbo Ding and Hongxin Hu. On the safety of iot device physical interaction control. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, pages 832–846, 2018.

[11] Check-Yee Law, Kah-Ong Goh, Wei-Siang Ng, Chee-Yung Loh, and Yong-Wee Sek. The integration of smart lock in vacation rental management system. In *2020 IEEE 20th International Conference on Communication Technology (ICCT)*, pages 846–850. IEEE, 2020.

[12] Yuan Luo, Long Cheng, Hongxin Hu, Guojun Peng, and Danfeng Yao. Context-rich privacy leakage analysis through inferring apps in smart home iot. *IEEE Internet of Things Journal*, 8(4):2736–2750, 2020.

[13] Shrirang Mare, Franziska Roesner, and Tadayoshi Kohno. Smart devices in airbnbs: Considering privacy and security for both guests and hosts. *Proc. Priv. Enhancing Technol.*, 2020(2):436–458, 2020.

[14] Martins Mihaeljans and Andris Skrastins. Iot concept and sdn fusion in consumer products: Overview. In *2023 3rd International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME)*, pages 1–6. IEEE, 2023.

[15] Kumar Shashwat, Francis Hahn, Xinming Ou, and Anoop Singhal. Security analysis of trust on the controller in the matter protocol specification. In *2023 IEEE Conference on Communications and Network Security (CNS)*, pages 1–6. IEEE, 2023.

[16] Wondimu Zegeye, Ahamed Jemal, and Kevin Kornegay. Connected smart home over matter protocol. In *2023 IEEE International Conference on Consumer Electronics (ICCE)*, pages 1–7. IEEE, 2023.