WIP: Delegation Related Privacy Issues in Matter

***Abstract*—In the evolving landscape of smart home technologies, the Matter protocol is a significant advancement, enhancing device interoperability within the Internet of Things (IoT) ecosystems. While it promises to unify and secure user experience, it also introduces complexities with respect to user privacy, especially in delegation scenarios. This paper specifically examines the delegation-related privacy issues inherent in the Matter protocol, with a focus on its practical application and interaction with third-party applications and services such as Apple Home and Tuya SmartHome. Our research scrutinizes the delegation mechanisms within the Matter protocol, exploring how device control is shared and transferred among users and the subsequent privacy implications of these actions. By investigating these delegation processes, particularly in their operational context and integration with third-party platforms, we reveal potential vulnerabilities and privacy concerns that may not be immediately apparent. The aim is to provide a critical analysis of the privacy trade-offs encountered in the delegation features of the Matter protocol, offering insights and considerations for users, developers, and stakeholders in the smart home ecosystem to enhance privacy awareness and protection in these increasingly complex networks.**

I. Introduction

In the dynamic and rapidly expanding domain of smart home technologies, the Matter protocol [3] represents a significant stride forward. As a unifying standard, Matter is designed to ensure broad compatibility and streamlined communication among a diverse array of devices. It stands at the forefront of Internet of Things (IoT) innovation, aiming to simplify the complexities traditionally associated with smart home setups and to foster a more cohesive, user-friendly, and secure environment. However, as the protocol promotes enhanced device interoperability and improved user experience through a unified and secure framework, there emerges a need for a deeper understanding of the potential implications for user privacy and data security.

As an IPv6-supported protocol [4], Matter primarily anchors its access control mechanisms within the device itself [7]. As illustrated in Figure 1, a Matter device is capable of being accessed by multiple entities, maintaining a nearly independent and coequal relationship amongst them. This design highlights the protocol's commitment to decentralized access and equitable control across various users and devices.

Through our investigations, we have conducted an in-depth analysis of the operational mechanisms inherent in the Matter protocol, with a particular focus on the intricacies of device pairing, sharing, and the pivotal aspect of control delegation. Our exploration is methodically segmented into three distinct delegation scenarios: Single Delegation, Transitive Delegation in Separate Fabrics, and Transitive Delegation within the Same Fabric. Each scenario offers a unique lens through which to understand how devices authorize and share access, as well as the consequent implications for user privacy. We have made the video demos available online at our website [1].

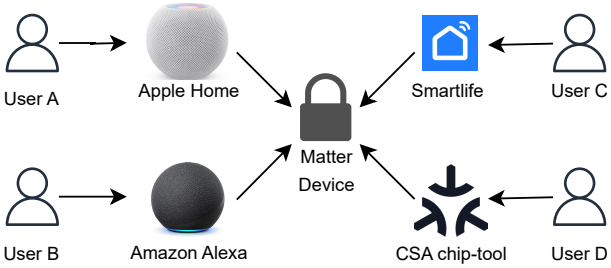

Fig. 1. The Control Architecture of Matter Protocol

Contributions: Our contributions in this paper are multi-faceted and can be delineated as follows:

- We identify and articulate the specific privacy risks associated with these operational mechanisms, especially in the context of third-party integrations. Through the simulation of real-world sharing and delegation scenarios, we demonstrate the potential privacy vulnerabilities inherent in the protocol's current structure.
- We offer recommendations aimed at both the Matter protocol's governing body and its major stakeholders. By suggesting these collaborative efforts.

II. Background

A. Matter Protocol

The Matter protocol, formerly known as Project CHIP (Connected Home over IP), represents a significant milestone in the evolution of smart home technology. Spearheaded by the Connectivity Standards Alliance [2], formerly the Zigbee Alliance, Matter was developed collaboratively by industry giants such as Apple, Google, Amazon, and many others. Its development history is a testament to the increasing need for interoperability and security in the smart home market. Launched to address the fragmented nature of the smart home ecosystem, Matter aims to create a unified, open-source connectivity standard that ensures devices from different manufacturers can work seamlessly together while maintaining robust security and reliability. This protocol is designed to be the foundation for future IoT innovations, promising a

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.2024.23xxx
www.ndss-symposium.org

more cohesive and user-friendly smart home experience. As it continues to evolve, Matter is set to revolutionize how devices communicate, paving the way for a truly connected world.

B. Basic Concept of Matter Protocol

The Matter protocol introduces a series of innovative concepts essential for enhancing IoT functionalities [10]. To facilitate a comprehensive understanding of the protocol, we delineate several fundamental Matter concepts that are pivotal for both developers and researchers.

Fabric: This refers to the interconnected environment of multiple nodes, sharing a common root of trust for secure operation.

Nodes and Node ID [5]: A physical device in Matter may represent one or more nodes, each with a unique Operational Node ID, facilitating distinct identification across the Matter fabric. Nodes embody the complete application functionality and can directly communicate within the network. It is important to note that within different fabrics, the Node remains completely isolated, allowing a single device to possess distinct node IDs across these separate contexts.

Endpoints and Clusters: Each node comprises numbered endpoints, representing specific functionalities. These endpoints consist of clusters that define the attributes, events, and commands for the single feature set of the endpoint, allowing for modular control and functionality of devices.

III. Assessing Risks in Delegation Scenario

A. Overview

The Matter protocol is primarily implemented within a LAN network, where devices are orchestrated through a namespace termed “Matter fabric” [6]. Under this framework, control is decentralized from a user’s centralized account to their application or mobile device, serving as the active controller during device interaction. This is in stark contrast to conventional IoT ecosystems, which are predominantly cloud-centric and designate the user’s account within the application as the definitive owner, irrespective of the specific mobile device employed for access. Consequently, safeguarding privacy within the Matter protocol presents notable challenges. The primary concern is the extensive permission sharing among applications at a foundational level (facilitated by the Matter protocol within a LAN), leading to potential privacy vulnerabilities.

B. Pairing and Authorization in Matter protocol

In the Matter protocol, the locus of authorization resides within the device itself, marking a significant departure from the prevalent cloud-based IoT architectures, particularly those ubiquitous in the smart home domain. This approach enables Matter devices to directly record and manage critical information, including the identity of the owner, the associated vendor, and the owner’s public key or certificate. Such an architecture provides a more direct and potentially secure method of managing device access and ownership.

Furthermore, the Matter protocol introduces the concept of ”fabric” to effectively handle scenarios involving multiple owners. This concept allows for different controllers to operate within distinct ”fabrics,” essentially serving as separate contexts for device interaction and management. Alternatively, when users employ the same application or are aligned with the same vendor, they can opt to share the same fabric, thereby accessing and managing devices within a unified context. This flexible approach to managing multiple owners and controllers reflects the protocol’s commitment to providing a versatile yet secure framework for device interaction and authorization within the evolving IoT landscape.

However, the distinct separation of contexts between different fabrics presents challenges in sharing information across them. Our findings indicate that a user from one fabric, say fabric A, can only recognize the existence of another, fabric B, and discern its vendor through the vendor ID list. It is important to note that while this vendor ID can be managed by the application, the accuracy and reliability of this information hinge upon the conscientiousness of the manufacturer.

When a device is reset and prepared for initial binding, it automatically enters a network-configurable state. At this juncture, a user can pair with the device by scanning a QR code or manually entering the device initialization string. However, complexities arise when a device is to be shared between applications from different manufacturers. In such cases, the owner who maintains control over the device must manually reconfigure it into a network distribution mode and generate a new pairing code. Subsequently, a user from a different application can use this pairing code to assume ownership and initiate a new fabric, thereby controlling the device within a new and independent context. This process underscores the nuanced balance between the robust security measures and the operational flexibility offered by the Matter protocol, necessitating careful consideration and management in cross-vendor device sharing scenarios.

C. Privacy Concerns in Single Delegation Scenarios

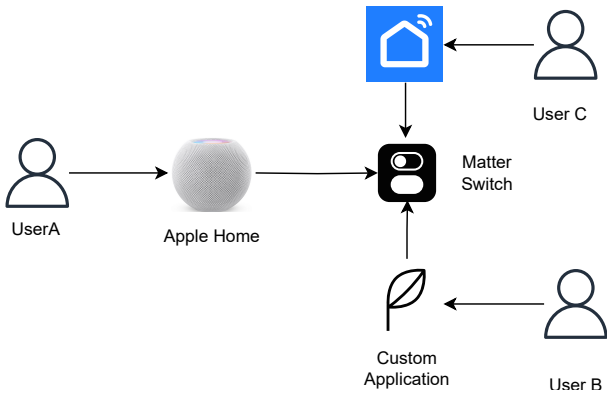

Fig. 2. Transitive Delegation Across Isolated Fabrics

We explored scenarios of delegation through the sharing of Matter devices to understand the intricacies of this process. Our empirical study utilized the Tuya Smartlife application as the designated delegate. In this context, as Figure 2 shows,

we initially paired the Matter device with Apple Home, then proceeded to facilitate access sharing with Tuya Smartlife. The sharing mechanism for Matter devices is operationalized through a pairing code, an inherent feature of the Matter protocol and supported by Apple Home. During the sharing process, users navigate to the device's settings page, activate pairing mode, and subsequently receive a pairing code. This code is then conveyed to the delegated client user—in our case, a user of Tuya Smartlife. With the pairing code, the delegated user can complete the pairing process, thus integrating the device with Tuya Smartlife and facilitating shared control and access.

An intriguing aspect we noted is that Apple Home facilitates awareness of additional controllers to the device owner. We investigated the mechanism behind this feature. The Matter protocol introduces a control namespace known as a "fabric," enabling the device owner or primary controller to identify other associated fabrics and thereby discern additional controllers. However, due to the protocol's limited granularity in this context, Apple can only identify the fabric and retrieve the vendor IDs of other controllers. Consequently, the Apple Home application will merely indicate the presence of an additional controller, such as another Tuya Smart client, without detailed identification.

D. Privacy Implications of Transitive Delegation Across Separate Fabrics

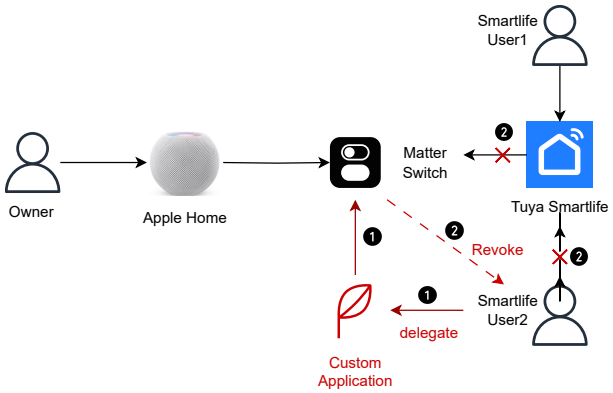

Fig. 3. Transitive Delegation within the Same Fabric

The principle of transitive delegation is well-established, wherein User A (the original owner) delegates certain permissions to User B, who is then able to further delegate these permissions to User C. Consequently, User C inherits permissions from User B rather than directly from User A, a characteristic feature of transitive delegation [11]. Interestingly, the Matter protocol represents a departure from this traditional delegation paradigm. Within the Matter framework, access control is integrally associated with the device itself, leading to a scenario wherein if User B delegates access to User C, User C assumes the same level of permission as User A. This holds true even if User A subsequently revokes the permissions granted to User B, with User C maintaining their access. Such a departure from conventional delegation mechanisms necessitates a thorough examination of its unique implications for user permission structures and privacy within the Matter protocol ecosystem.

To explore these dynamics practically, we conducted an experiment using the Apple Home app and the Tuya SmartLife app, incorporating an Apple HomePod Mini and a official Matter.js [9] virtual light compatible with the Matter protocol. This setup was instrumental in observing and analyzing the nuanced operational behaviors and privacy implications inherent to the Matter protocol's approach to delegation and access control. The potential impact on the owner's privacy.

In our experiment, we postulate that the primary user of Apple Home is the device's rightful owner, while the official Matter controller chip-tool [8] is designated as the secondary user (User B). Additionally, the Tuya Smartlife application is utilized as the tertiary user (User C). Initially, the Apple Home user is responsible for device binding, and upon successful completion, can generate a pairing code. Subsequently, the chip-tool (User B) employs this code to bind the device. Thereafter, the chip-tool is used to generate an alternative pairing code, which is shared with the Tuya device. However, upon revoking the permissions of User B through User A's operations, it has been observed that the Tuya Smartlife app user retains the ability to control and monitor the device. This revelation indicates a potential breach of the owner's privacy.

E. Privacy Concerns in Transitive Delegation Within the Same Fabric

In §III-D, we discussed the transitive delegation scenario that three users from three separate applications. Now we disscuss that at least two users are using the same application (the same fabric).

Mirroring the structure of the previous experiment, we designated the Apple Home user (User A) as the original owner. However, in this iteration, both User B and User C utilize the Tuya Smartlife application. Specifically, User A shares the device with User B utilizing the pairing code. Subsequently, User B extends the administrator access to User C using Tuya's room function, which involves inviting User C to the room. In this arrangement, User B and User C operate within the same fabric, yet possess distinct private keys or certificates to control the device, ostensibly more secure.

Despite the presumed security of this configuration, our findings reveal a potential risk. User C retains the capability to generate a new pairing code, effectively enabling them to initiate the device's pairing mode and independently share the device within their own Tuya room. Consequently, even though User A has visibility over the device being controlled by two separate Tuya clients, it leads to ambiguity and confusion. User A might struggle to discern the specific sharing dynamics or erroneously perceive this as a standard feature of the system. This scenario underscores the importance of a clear and manageable understanding of device-sharing mechanisms, as well as the potential for security risks in seemingly secure configurations.

F. Possible Improvement Discussion

As articulated in our analysis, a significant source of privacy risk within the Matter protocol arises from its fabric concept. Each fabric's distinct and isolated context has the potential to be misappropriated for unauthorized retention of permissions. In response to this vulnerability, we recommend that the Matter organization consider measures to enhance transparency across different fabrics.

The current method of relying on a predefined vendor ID for authentication is inherently flawed. A more secure and reliable authentication process for vendor IDs should be instituted. Moreover, it is crucial that users within one fabric (fabric A) possess the capability to discern who has control or monitoring rights over a device in another fabric (fabric B). Enhanced cross-fabric visibility would empower device owners to more effectively identify and neutralize potential unauthorized access, thereby reinforcing the security and privacy of the entire system. These recommendations are directed toward the Matter Foundation for consideration and action.

In addressing the major vendors of the Matter protocol, we suggest a careful consideration of the user interface design. A simplistic approach, while seemingly user-friendly, may inadvertently obscure vital information about privacy risks or vulnerabilities from the owner. It is essential that the interface, while being intuitive and accessible, does not sacrifice the depth of information necessary for users to understand and manage potential security and privacy implications. Vendors should therefore strive to strike a balance, crafting an interface that both elucidates and empowers users to effectively safeguard their privacy and security while leveraging the full potential of the Matter protocol.

IV. Discussion

As an emergent protocol, Matter garners substantial support from major industry players including Apple, Google, Amazon, and others, positioning it as a promising solution for the integration of the IoT ecosystem. However, while the novel features of the Matter protocol hold the potential for significant advancements, they also introduce new risks, particularly in the domain of privacy. This paper represents a pioneering effort to analyze and address the privacy concerns specifically arising within Matter's delegation scenarios. We have identified several potential risks that could lead to serious vulnerabilities or breaches of privacy.

Furthermore, we advocate for the implementation of new features that enhance the protocol's capabilities, particularly in terms of fine-grained access control information. Such advancements are critical for making the delegation process more transparent and secure. By illuminating these privacy concerns and suggesting pathways for improvement, we aim to contribute to the ongoing development and refinement of the Matter protocol, ensuring it can deliver on its promise of a unified, efficient, and secure IoT ecosystem without compromising user privacy.

V. Conclusion

Our study has examined the Matter protocol's privacy implications in single and transitive delegation scenarios, including within the same fabric. We have identified distinct vulnerabilities and challenges that arise in each context, emphasizing the complexity and importance of privacy considerations in IoT delegation mechanisms. Our findings advocate for heightened awareness and improved privacy safeguards from both the Connectivity Standards Alliance (CSA) and major vendors. As the smart home technology landscape continues to evolve, ensuring robust privacy protections in the face of increasingly sophisticated delegation scenarios is paramount. We encourage ongoing research and development to address these identified concerns and to advance the secure and responsible implementation of the Matter protocol.

References

[1] Authors, "Supported Materials," https://sites.google.com/view/wip-delegation-privacy-matter, 2023, accessed: 2024-1-04.

[2] Connectivity Standards Alliance, "Homepage - Connectivity Standards Alliance," https://csa-iot.org/, 2023, accessed: 2023-12-31.

[3] ——, "Matter - The Connectivity Standard for the Future of IoT," https://csa-iot.org/all-solutions/matter/, 2023, accessed: 2023-12-31.

[4] Google Developer Center, "Access Control Guide," https://developers.home.google.com/matter/primer/thread-and-ipv6, 2022, accessed: 2024-1-08.

[5] Google Developers, "Device Data Model - Understanding Matter," https://developers.home.google.com/matter/primer/device-data-model, 2023, accessed: 2023-12-31.

[6] ——, "Matter Primer: Understanding Fabric - Google Home Developers," https://developers.home.google.com/matter/primer/fabric, 2023, accessed: 2023-12-31.

[7] Nordic, "Access Control Guide," https://developer.nordicsemi.com/nRF_Connect_SDK/doc/latest/matter/access-control-guide.html, 2024, accessed: 2024-1-08.

[8] Project CHIP, "Connected Home over IP," https://github.com/project-chip/connectedhomeip, 2023, accessed: 2023-12-31.

[9] ——, "matter.js - JavaScript Library for Project CHIP," https://github.com/project-chip/matter.js/, 2023, accessed: 2023-12-31.

[10] K. Shashwat, F. Hahn, X. Ou, and A. Singhal, "Security analysis of trust on the controller in the matter protocol specification," in *2023 IEEE Conference on Communications and Network Security (CNS)*, 2023, pp. 1–6.

[11] B. Yuan, Y. Jia, L. Xing, D. Zhao, X. Wang, D. Zou, H. Jin, and Y. Zhang, "Shattered chain of trust: Understanding security risks in cross-cloud iot access delegation," in *29th USENIX Security Symposium, USENIX Security 2020, August 12-14, 2020*, S. Capkun and F. Roesner, Eds. USENIX Association, 2020, pp. 1183–1200. [Online]. Available: https://www.usenix.org/conference/usenixsecurity20/presentation/yuan