Security Analysis of Trust on the Controller in the Matter Protocol Specification

Kumar Shashwat*, Francis Hahn*, Xinming Ou*
*Department of Computer Science and Engineering
University of South Florida
Tampa, Florida, USA
Email: (kshashwat, fhahn, xou)@usf.edu

Anoop Singhal†
†National Institute of Standards and Technology
Gaithersburg, Maryland, USA
Email: anoop.singhal@nist.gov

***Abstract*—Matter is an open-source connectivity standard allowing smart home IoT (Internet of Things) devices from different vendors to interoperate with one another. A controller[1] in a Matter system commissions new devices into the Matter fabric. The device needs to present a credential called Device Attestation Certificate (DAC), indicating that it is from a trusted vendor and has gone through the necessary testing to be compliant with the Matter standard. However, the controller is not required to prove to the device that it is from a trustworthy vendor. We verified through experimentation that anyone can create a Matter controller that can commission a commercial Matter device. We analyze the security implication of this design choice in Matter, and present a few scenarios where a malicious controller can exert harm to an otherwise healthy Matter ecosystem.**

I. Introduction

IoT devices that possess various "smart" capabilities are proliferating rapidly into people's homes. New houses are being built pre-equipped with a myriad of smart devices for lighting, cameras, door locks, thermostats, door bells, etc., with communication components and wiring setup for quick installation. It is estimated [9] that the global smart home market size will grow at an annual rate of 27.07%, reaching USD 400 billion by 2030. Various vendors have created their own smart home ecosystems, such as Google Home, Apple HomeKit, Amazon Alexa, and Samsung SmartThings. There is heavy competition in the IoT space where device manufacturers try to support as many ecosystems as possible to increase their market reach. Such rapid development leads to lack of best practices for security in IoT devices as demonstrated by large-scale IoT botnets such as Mirai [2]. Having to support various ecosystems is not just a hassle for device manufacturers but also for end users. As a smart home user, using only one ecosystem will limit smart home devices to the ones compatible with it; whereas using multiple ecosystems poses a challenge for device interactions.

To address the above device interaction problem, Matter [5] was introduced as an open-source connectivity standard for smart home devices and released in November 2022. Matter leverages established secure communication standards: Public Key Infrastructure (PKI) and authenticated session establishment based on certificates, to ensure the confidentiality and integrity of communication between devices and to provide device authentication. In the Matter protocol specification, a special device called a Matter controller is responsible for commissioning a device into a "Matter fabric," where all devices share the same root certificate authority (CA) used for secure communication. Devices in the same fabric can discover one another and communicate through a secure protocol using standardized syntax and semantics. This allows devices from different vendors to inter-operate with one another through a standard interface. For example, a smart light switch from vendor A can control a smart light bulb from vendor B, as long as they are commissioned into the same Matter fabric. Matter solves the issue of interoperability for both device vendors and consumers. Device vendors only need to support one protocol, Matter, as opposed to the various and widely differing ecosystems. Consumers only need to use one ecosystem as long as the ecosystem also supports Matter in addition to its proprietary protocol. As of late 2022, the major ecosystem vendors – Google, Apple, Amazon, and Samsung have announced that their products will be Matter-compatible.

While Matter provides a promising future where IoT devices from all vendors work seamlessly together in a smart home environment, the increased connectivity also increases the attack surface for all devices. A device vendor may be hesitant to support Matter if it fears that exposing its devices to those from other vendors may increase the security risks. If some devices become "bad actors" – either through malice or incompetence in secure development, devices from "good" vendors will have an increased attack surface compared to the situation in a closed ecosystem. The Matter protocol design (Matter 1.0) has considered such concerns and incorporated a number of measures to control this risk. Each Matter device must present a Device Attestation Certificate (DAC) signed by Product Attestation Intermediate (PAI), typically held by the manufacturers. This PAI is further signed by Product Attestation Authority (PAA). Matter keeps the list of PAAs of trusted vendors in the Distributed Compliance Ledger (DCL), a blockchain ledger maintained by the Connectivity Standards Alliance (CSA) behind the Matter protocol. During commissioning a Matter

[1]Throughout this paper the term "controller" refers to the controller component in the Matter protocol specification. It does not refer to any specific controller from any vendor.

device must present the commissioner the DAC of the device and the commissioner must verify that its root certificate (PAA) is present in DCL. In addition, each Matter device is configured an access control list (ACL) specifying which other devices in the fabric are allowed to communicate with it.

This trust model of Matter implicitly assumes that controllers (commissioners) are to be trusted, and the main potential threats come from devices. When a device is commissioned, there is no verification on the device side whether the controller is from a trustworthy source. Since the controller has full control over any device it commissions into its Matter fabric, this poses questions of whether a malicious controller can cause harm on other well-behaving players in the ecosystem. In this paper we conduct an analysis of the various scenarios to examine a malicious controller's impact. Our contributions are:

1) We conducted an experiment on a market-available Matter device to verify that a malicious controller can commission and control the Matter device.
2) We present a number of attack scenarios which allow the commissioning of a victim Matter device into a stealth Matter fabric and uses it to produce adverse interactions on another Matter fabric.
3) We discuss potential mitigations for the malicious controller problem.

II. Background

Devices commissioned by a Matter controller into a Matter fabric can communicate locally (without going through a cloud service) between one another using well established secure protocols. The development of the Matter protocol involves collaboration between major industry players such as Apple, Google, Amazon, and Samsung. These vendors all have substantial market share and use their proprietary ecosystem to communicate and control the devices. Smaller device vendors typically choose to support the ecosystem of one or multiple major vendors, to increase the chance that consumers may choose their products. Matter will alleviate those small vendors' burden of supporting multiple major smart home ecosystems – they just need to support Matter and all these major players' ecosystems will be able to commission and use their products.

An IoT device must present a valid Matter DAC to be commissioned into a Matter fabric. The commissioner must check that the DAC is signed by a trusted PAA, i.e., one that is recorded in the Distributed Compliance Ledger. For a new vendor to be Matter-certified and have their product listed in the DCL, they need to go through the following process.

1) The new vendor needs to become a member of the CSA, and request a vendor ID. This step involves paying a financial fee and requires a certification where the vendor undergoes compliance testing.
2) After the initial step is met a vendor can request CSA to add their PAA to the DCL. The DCL acts as a data store for five specific fields for a Matter device including information on the vendor, model type, software versioning, compliance results, and the PAA certificates. The DCL is owned by CSA, and thus all of its members, which enforce restricted write access and public read access policies for DCL.
3) Once CSA approves a vendor's device, it writes the product's DAC to the DCL.

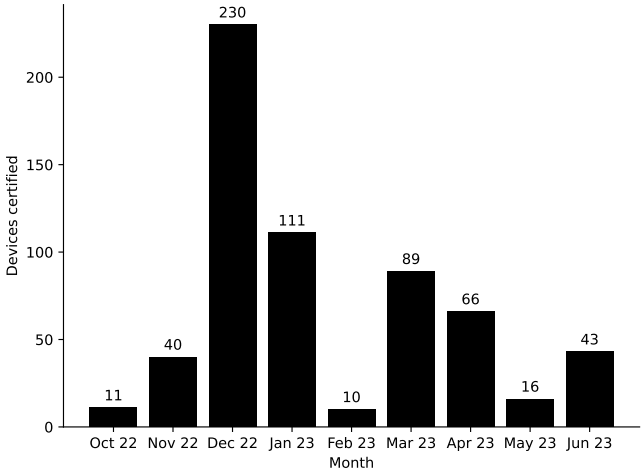

Fig. 1. New Matter-certified products by months.

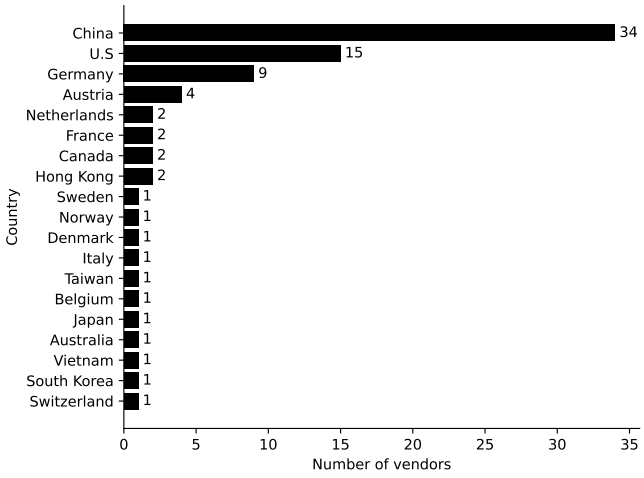

Fig. 2. Matter-certified vendors by countries

A. Matter Adoption

We did an analysis on the DCL on June 16, 2023. As shown in Fig. 1, there was an initial surge of new device models in December, 2022, right after the Matter protocol was released. The appearance of new Matter device models has been slowing down since January, 2023. As of the date above there were in total 81 vendors and 616 products that were Matter-certified (Fig. 1 and 2). Fig. 3 shows that the vast majority of Matter-certified products were switches and light bulbs.

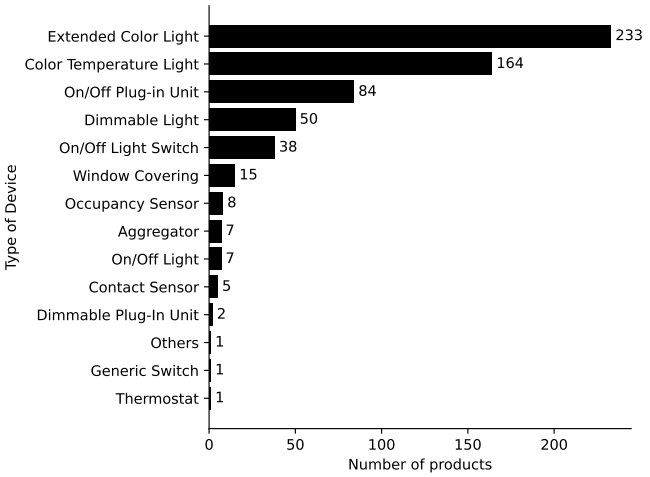

Fig. 3. Matter-certified products by types

III. Matter Protocol Design

A. Basic Matter Terminology

- **Matter fabric:** A Matter fabric, identified by a Fabric ID, is a collection of devices communicating together in a Matter ecosystem. They share a common cryptographic credential that allows secure session establishment.
- **Node:** Matter node is a device or device component that is participating in the Matter fabric. For a smart home, it includes the IoT devices, controller devices such as Amazon Alexa, and the mobile application that was used to commission the device to the Matter fabric. Each Matter node is uniquely identified with a Node ID.
- **Controller:** Controller is a Matter node that has admin privilege on some or all devices in the Matter fabric. In a smart home, a controller is likely a physical device like Amazon Alexa or Google Home Hub.
- **Commissioner:** Commissioner is a matter node used to commission an IoT device to the Matter fabric. For a smart home user, it is typically a mobile application. By default, the commissioner has admin privilege to the devices it commissioned. In this paper, we use the term commissioner and controller interchangeably.

B. Trust among the entities

Matter devices do not trust each other unless specified by the controller. For example, it would not make sense for a door lock to trust the commands coming from a light bulb. Matter protocol leverages access control lists to establish trust among devices. As shown in Fig. 4, the light bulb has the light switch's node id in its ACL, whereas the light switch has the node id of the bulb in its binding list.

It is left to the user to configure which device can talk to whom. In the case of one device becoming malicious or simply malfunctioning there can be ripple effects on other devices. Misconfigured ACLs that result in more devices than necessary

Fig. 4. Access Control and Binding List

able to communicate with one another can amplify security problems caused in this situation. It can become particularly tricky if the smart home system employs automation rules where events automatically trigger actions on IoT devices, whose effect may cause more automation rules to be triggered, creating a chain reaction among devices. A recent work [4] has comprehensive discussion on the various scenarios. All these indicate that it is important that a Matter system only allow trustworthy devices to enter. Moreover, only those devices can initiate and establish communication with the other devices in the system.

1) Device Attestation Certificate: Device Attestation Certificate (DAC) is used to uniquely identify a product. Its primary role is to ensure that a new device joining a Matter system is Matter certified. It is burned into the persistent storage of each device. Each DAC is signed by a Product Attestation Intermediate certificate which is further signed by a Product Attestation Authority (PAA). Matter stores all the PAAs on the Distributed Compliance Ledger. During the device's commissioning process, the controller checks the DAC against the DCL to ensure that the product is Matter certified.

2) Node Operational Credentials: A Node Operational Credential (NOC) is an X.509 certificate and the associated private key. NOCs are unique to each device. Communication between two Matter devices happens through a secure session. The session is encrypted through a negotiated key using the devices' NOCs. This process is called Certificate Authenticated Session Establishment (CASE) [5] and it is based on the SIGMA [7] protocol. The devices which share the same Root Certification Authority (RCA) for their NOCs can talk to each other and are said to belong to a single Matter fabric. The RCA usually resides in the controller which generates and assigns the NOC to each device during commissioning.

C. Commissioning a new device

Commissioning is the process of onboarding a new device into a Matter fabric. In most cases, users will use their smartphone to commission a new device. An app on the phone will perform the Matter new device commissioning protocol. Once the commissioning process is finished, it will transfer the credential information to the controller.

1) The device is turned on and starts broadcasting either through Bluetooth Low Energy advertisement or DNS-based Service Discovery [3] service.
2) Commissioner recognizes the advertisement. To communicate with the device it needs a password. The Quick

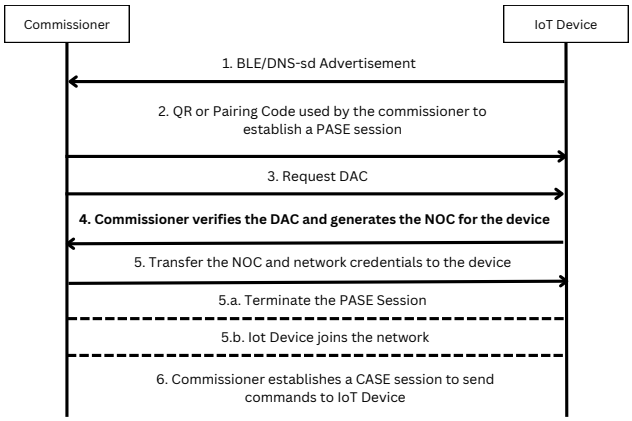

Fig. 5. Commissioning Process

Response (QR) code with which each Matter device is shipped with contains the password. Scanning the QR code or entering the password manually establishes a Password Authenticated Session (PASE).

3) The commissioner requests DAC from the device.
4) The commissioner verifies the DAC against the DCL.
5) After successful verification, the commissioner generates a NOC for the device and transfers the NOC along with the network credentials, which could be Wi-Fi credentials, through the PASE session before closing the PASE session.
6) The device uses the network credentials to get onto the network. Once the device is on the network the commissioner establishes a certificate authenticated session using CASE to send subsequent commands to control the device.

One design choice Matter made is that while the commissioner verifies a Matter device's DAC, there is no similar check on the device's part for the controller. The protocol does not provide a way for a device to verify if it is talking to a Matter-certified commissioner.

D. Multiple Matter fabrics in a smart home

For a smart home, the controller will likely be a smart phone app or a physical device like Alexa. A single device can be on multiple fabrics at the same time. The diagram above shows that there are three controllers in a smart home. The controllers can be mobile apps or physical devices like Amazon Alexa or Google Home. The thermostat, lighting system, and door lock are in Google Home's Matter fabric. The lighting system, thermostat, and IoT camera are in Apple Home's fabric. The IoT camera and thermostat are in the Amazon Controller's fabric. Here, the thermostat has NOCs with three fabrics, the lighting system and the IoT Camera with two, and the door lock with only one.

IV. Malicious Controller

Matter vendors need to go through Matter certification to ensure that their devices meet the standards of Matter protocol. However, through our experimentation we found that the commissioner is not vetted. Commissioner will usually be an application running in the user's mobile device. The commissioner not only commissions the device but has full control over it – acting equivalently as a controller. Since commissioner is typically an app installed by the user on their mobile device, it is assumed by default to have the user's trust. However, this trust could be misplaced and can lead to a new way for malicious apps to attack a user's smart home devices. The user may install the app through some third-party app stores, which may not have a rigorous level of vetting. We present some scenarios below.

A. The malicious Matter controller is limited to its own fabric

1) Malicious app has access to all the devices on a Matter fabric: Under this example, the user used the malicious application to commission all the devices in their home. The device trusts the commissioner by default therefore, the app has full control over all the devices in their home.

2) App has access to some devices on the Matter fabric: Under this scenario, it is expected that the user already has a Matter fabric controlled by a legitimate controller. The user bought a new device, and decided to download a malicious app to control it because it offers some features not present in the official app. Under this case, the malicious app is only limited to the device that it can control. In Fig. 7, the malicious app has access to a thermostat. In this scenario the app, through a remote Command and Control (C&C) server, is capable of issuing commands which could lead to physical damage – electrical hazards and property damage for a homeowner.

B. The malicious Matter controller controls a device which is shared with a benign fabric

In these scenarios the user chooses to trust an app to control a device. The app may masquerade as something attractive to

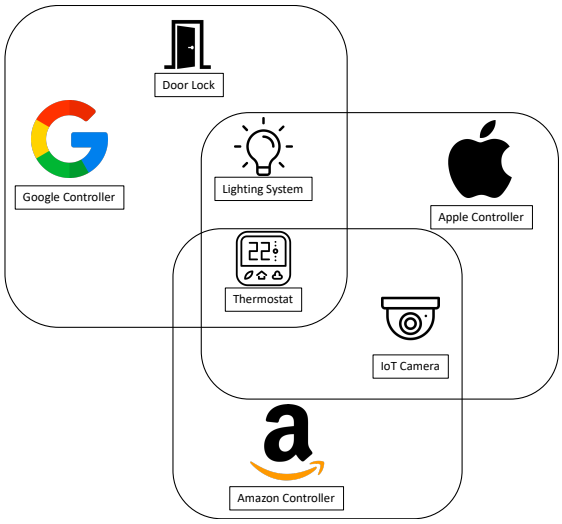

Fig. 6. Smart home with multiple Matter fabrics

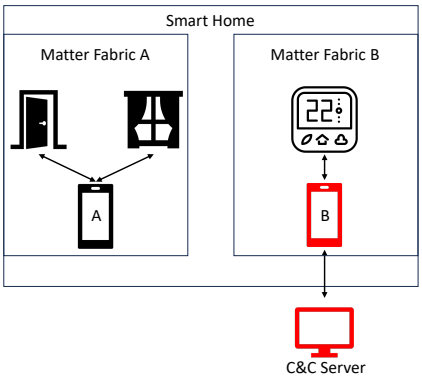

Fig. 7. A benign fabric (A) and a malicious fabric (B) isolated from one another.

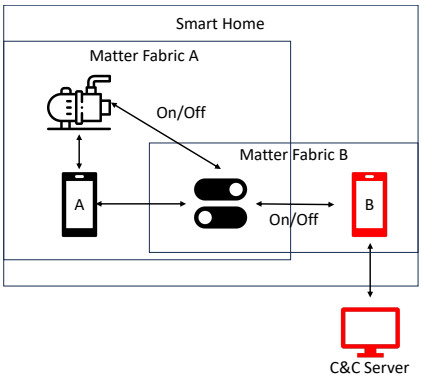

Fig. 8. A benign fabric (A) and a malicious fabric (B) sharing a switch.

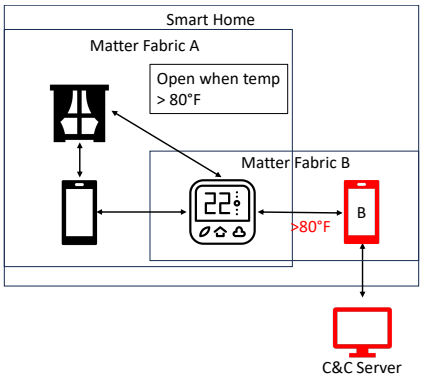

Fig. 9. A benign fabric (A) and a malicious fabric (B) sharing a thermostat.

the user, e.g., energy optimizer for a device, and it commissions the device and puts it under its own control. As shown in Fig. 6, a Matter device can exist in multiple Matter fabrics at the same time. This can lead to another scenario where a device is both connected to the malicious app's Matter fabric and a legitimate Matter fabric. This provides an entry point for the attacker to impact other devices in the legitimate fabric.

3) Malicious app controls a device which triggers another device: As shown in Fig. 8, the malicious app is used to commission a switch which can talk to a water pump. A water pump is a critical device where the occurrence of a malfunction can lead to severe property damage. With a malicious controller an attacker can initiate a DoS attack on the Matter switch, which can result in a malfunction.

4) Malicious app controls some devices with automation rules between devices: In Fig. 9, the thermostat is shared between two ecosystems A & B. Ecosystem A is the legitimate ecosystem whereas ecosystem B is the malicious application's ecosystem. There is also a window in the home which is present in ecosystem A but not ecosystem B. Suppose there is an automation rule in ecosystem A which states that "If the temperature rises over 80°F then open the window." Since the malicious app controls the thermostat it can set the temperature to be more than 80°F so the windows open up for the intruder to get in.

C. User's perspective

In the third and fourth scenario, the user might blame the water pump and the window for the malfunction, not being aware that they are caused by a malicious controller the user inadvertently used on another device. This can present a challenge for Matter vendors who have to consider the risk that another device under the control of a malicious entity may incur damage to their own products, and reputation.

V. Experimentation

The goal of the experimentation was to create a malicious app able to commission a Matter IoT device bought from the market. For the experiment, we used an off-the-shelf Matter Smart Wi-Fi Plug from a Matter-certified vendor. We were able to commission it using the Google Home application thus confirming that the plug is indeed Matter-compatible.

For creating our own commissioner, we used the sample chip-tool commissioner code provided by the Matter consortium [1]. We were able to commission the Matter Smart Wi-Fi Plug with our controller, even though we do not possess any Matter vendor credential. Once the device was commissioned, our app can send commands to turn the switch on or off. Our experiment verifies that any app developer can write a commissioner for commercially available Matter devices.

VI. Discussion

During the Matter device commissioning process, the commissioner checks the device DAC against the Matter DCL. However the device does not have an option to check the DAC of the commissioner. This allows third-party unverified Matter vendors to create Matter-based mobile applications that function as a Matter commissioner. Moreover, a Matter commissioner implementation can also skip checking the device DAC as well, which will allow non-Matter certified devices to join the Matter fabric. This design choice, while creating flexibility to allow more third-party vendors to be part of the Matter ecosystem, does open up some attack vectors as discussed in this paper.

A. Possible Mitigations

1) Providing DAC check on commissioner by device: One option to address the malicious controller issue is to amend the protocol so a Matter device has the option of requesting the commissioner to also present a valid DAC, and check the DAC against the DCL. This would require developers of apps that function as Matter commissioners be Matter-certified, as is the case for device vendors. The commissioning process can be modified as a two-way verification process as shown in Fig. 10. The device requests the DAC of the commissioner and verifies it against the DCL (step 7 and 8). If verification fails, the commissioning should be aborted and the device should be reset.

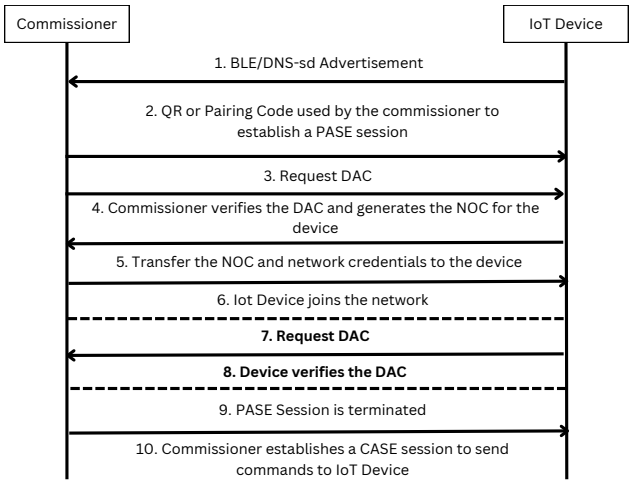

Fig. 10. Proposed amended Matter commissioning protocol

2) Checking commissioner credential by app market: The likely route for malicious Matter commissioners is through mobile app markets. If Matter can provide a separate credential for app developers who are trusted to develop Matter commissioners, this credential can be used instead of DAC. One option is for the app market to check that a Matter application's developer possess a valid credential, and if so the app will be given a visible label on the app market so the user is informed that it is safe to use this app on a Matter device. This will still provide open-source developers a way to work on Matter applications, and a lightweight process to obtain a credential so their app can be Matter-certified, without the need to modify the current Matter protocol.

VII. Related Work

Loos [8] discusses the issues and attack surface of the Matter protocol, and points out that a rogue commissioner is possible due to an inability to distinguish between legitimate and illegitimate DNS advertisements, leading to an attack analogous to that of evil-twin rogue wifi access points. This attack would require the rogue commissioner to steal the password credential used in the PASE phase of the commissioning process (see section III-C). Our malicious commissioner is assumed to have the PASE credential since the user voluntarily uses the malicious commissioning app and would provide the credential by presenting the product QR code to it. Chi et al. [4] present IoTMediator, a system for identifying and handling IoT interaction threats in multi-platform multi-control-channel smart homes. Those IoT interaction threats could be exacerbated by the malicious commissioner problem discussed in this paper. In particular, a device inadvertently falling under the control of a malicious commissioner could impose harm to other devices to an otherwise benign Matter ecosystem through the interaction threats. Wei et al. [10] study the interactions between the IoT cloud, the IoT devices and the mobile apps. They present how improperly configured interactions in a smart home can lead to hazardous scenarios for the user. Yunhan et al. [6] present ContexIoT, a context based permission model which presents the user with real-time prompts to perform effective access control. Our work focuses on the Matter protocol and examines the security risks posed by the trust placed on the Matter controller.

Conclusion

We demonstrated that Matter's commissioning process places inherent trust on the controller (commissioner) and there is no check on the trustworthiness of the controller. This provides a potential new attack surface for Matter ecosystems due to the possible interactions of devices across Matter fabric boundaries. We discussed a number of these scenarios and present some potential mitigations.

Acknowledgment

We thank the valuable comments from the anonymous reviewers, as well as comments from multiple NIST researchers on an earlier draft of the paper. This work was partially supported by the National Science Foundation under award no. 2235102, and Office of Naval Research under award no. N00014-23-1-2538. Any opinions, findings and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the above funding agencies.

Disclaimer: Certain equipment, instruments, software, or materials are identified in this paper in order to specify the experimental procedure adequately. Such identification is not intended to imply recommendation or endorsement of any product or service by NIST, nor is it intended to imply that the materials or equipment identified are necessarily the best available for the purpose.

References

[1] Connectivity Standard Alliance. Matter github repository. https://github.com/project-chip/connectedhomeip, 2022.
[2] A. Stavrou C. Kolias, G. Kambourakis and J. Voa. DDoS in the IoT: Mirai and other botnets. *IEEE: Xplore*, 2017.
[3] Stuart Cheshire and Marc Krochmal. RFC 6763: DNS-based service discovery, 2013.
[4] Haotian Chi, Qiang Zeng, and Xiaojiang Du. Detecting and handling IoT interaction threats in multi-platform multi-control-channel smart homes. In *Proceedings of the 32nd USENIX Security Symposium*, 2023.
[5] Connectivity Standards Alliance. *Matter Specification Version 1.0*, Sept 2022.
[6] Yunhan Jack Jia, Qi Alfred Chen, Shiqi Wang, Amir Rahmati, Earlence Fernandes, Zhuoqing Morley Mao, and Atul Prakash. ContexIoT: Towards providing contextual integrity to appified IoT platforms. In *Network and Distributed System Security (NDSS) Symposium*, 2017.
[7] Hugo Krawczyk. Sigma: The 'sign-and-mac' approach to authenticated diffie-hellman and its use in the IKE protocols. In Dan Boneh, editor, *Advances in Cryptology*. Springer Berlin Heidelberg, 2003.
[8] Melissa Loos. Security analysis of the Matter protocol. Master's thesis, Ulm University, 2023.
[9] Grand View Research. Smart home market size, share and trends analysis report by products (lighting control, security and access controls), by application (new construction, retrofit), by protocols (wireless, wired), by region, and segment forecasts, 2023 - 2030, 2023.
[10] Wei Zhou, Yan Jia, Yao Yao, Lipeng Zhu, Le Guan, Yuhang Mao, Peng Liu, and Yuqing Zhang. Discovering and understanding the security hazards in the interactions between IoT devices, mobile apps, and clouds on smart home platforms. In *28th USENIX Security Symposium*, pages 1133–1150, Santa Clara, CA, August 2019. USENIX Association.