Seamlessly Insecure: Uncovering Outsider Access Risks in AiDot-Controlled Matter Devices

Narmeen Shafqat
Northeastern University
Boston, USA
shafqat.n@northeastern.edu

Aanjhan Ranganathan
Northeastern University
Boston, USA
aanjhan@northeastern.edu

***Abstract*—Matter is the recently proclaimed standard for seamless interoperability among connected Internet of Things (IoT) devices, seeking to unify the fragmented IoT landscape. In this paper, we analyze a range of Matter-enabled devices, uncovering a critical security flaw within the manufacturer's implementation of the device commissioning process. This flaw allows the adversary to exploit an unenrolled manufacturer channel on an operational Matter device to enable unauthorized access, without notifying the user or compromising the existing Matter connection. Our research expands the discourse beyond the traditionally emphasized insider threats by eliminating the need to know specific in-home devices and the victim's WiFi credentials, thereby opening the door to malicious outsiders. Through comprehensive testing, we demonstrate that alarmingly, 5 out of 15 commercial Matter devices, from 4 distinct manufacturers, are vulnerable to unauthorized access by outsiders, facilitated through a singular smart platform app, AiDot. While the immediate impact is evident in smart bulbs and plugs, the ramifications become increasingly severe as manufacturers extend Matter implementation to critical devices, such as security cameras, door locks, and thermostats. In light of our findings, we advocate for urgent remedial measures, recommending the enforcement of a single active device channel at any given time, thereby enhancing the security of the IoT environment.**

***Index Terms*—Matter, smart home, outsider, unauthorized access, AiDot**

I. Introduction

The Internet of Things (IoT) landscape is burgeoning, with an array of devices like smart bulbs, door locks, and smart plugs from various manufacturers, each utilizing diverse data formats, and communication protocols, such as Wi-Fi, Bluetooth, Thread, and Zigbee. While users can control Wi-Fi and Bluetooth devices directly through the manufacturers' apps, centralized control requires compatibility with leading home automation platforms, like Apple's HomeKit [1], Google Home [2], Amazon's Echo Dot [3], and Samsung's SmartThings [4]. The challenge stems from the intricate diversity of the IoT ecosystem, where each platform also supports multiple communication standards. Consequently, users first register third-party devices with the respective manufacturer's apps before integrating them with their preferred home automation platform's app. Unfortunately, this results in a clutter of manufacturer apps on the users' phones. Recognizing these issues, manufacturers are actively exploring ways to facilitate device interoperability, streamline the onboarding process for users, and reduce reliance on individual manufacturer apps.

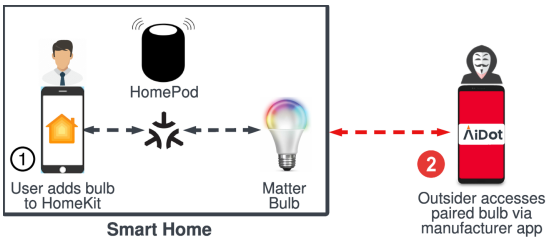

Fig. 1. Manufacturer Oversight Exposes Operational Matter Devices to Unauthorized Access via Unenrolled Manufacturer's DMC.

The various methods available to users for device control create different Device Management Channels (DMCs). An increase in the number of DMCs increases the potential for security risks. Recent research indicates that improper configuration of DMCs, referred to as Chaotic Device Management (Codema), exacerbates these risks [5]. Consequently, individuals like Airbnb guests, who are familiar with in-home devices, could potentially exploit unenrolled DMC by installing the respective manufacturer's app. This could lead to unauthorized control of smart devices utilizing HomeKit code (identified as Codema Flaw 1 in [5]) or through Bluetooth/ Zigbee/ Zwave technologies (Codema Flaw 2 in [5]). Notably, while the former flaw necessitates access to the victim's Wi-Fi network, the latter is specific to Philps Hue devices.

Matter [6], a recently embraced industry standard aimed at unifying the IoT landscape, allows users to seamlessly connect Matter devices to any Matter-compatible smart hub platform by simply scanning the device's QR code. While this streamlines device connectivity, enhances cross-compatibility, and reduces reliance on manufacturer apps, it introduces another DMC. However, Matter is designed with security as a foundational element. It establishes a robust immutable identity for each device through digital certificates, alongside implementing encryption and secure onboarding procedures. Hence, Matter devices are resistant to unauthorized pairing.

In this study, we demonstrate how Codema can inadvertently facilitate unauthorized access to operational Matter devices, extending beyond the realm of malicious insiders. This exposes smart homes to external attacks, allowing individuals who lack knowledge of in-home devices or access to the victim's Wi-Fi network to compromise user privacy and

security (Fig. 1). The core of this issue lies in the fact that devices once paired using a Matter QR code can be later discovered and onboarded via an alternative physical communication channel, such as Bluetooth Low Energy (BLE), which remains unenrolled even after establishing a Matter connection. The outsider can exploit this gap by connecting to the unenrolled manufacturer's DMC via the AiDot App [7]. The AiDot app is a widely used smart home platform tailored for non-hub setups, that enables users to control devices from various brands through a unified interface [8], without installing manufacturer-specific apps. The decision to leave the manufacturer's DMC open might be a deliberate choice by the manufacturer to offer users device control without a central hub, or it could be an unintentional oversight.

To substantiate our findings, we conducted extensive experiments on a diverse set of commercially available IoT devices, across 3 popular smart hubs. As anticipated, non-Matter devices exhibited resilience against the described attack, as the initial linking of the device with the manufacturer app effectively occupied the manufacturer DMC. However, 5 out of the 15 unique Matter devices, from four different brands — Orein, Linkind, Mujoy, and Consciot were discovered to be vulnerable to unauthorized pairing attacks by outsiders, via AiDot app without requiring advanced technical expertise. The remaining Matter devices required either physical device access or victim's Wi-Fi credentials for successful exploitation.

We responsibly reported our findings to AiDot and the manufacturers of the impacted devices. Presently, Matter is implemented in specific device types; smart bulbs, plugs, and some sensors. However, as Matter continues to expand, this vulnerability presents significant privacy implications, including unauthorized access to or deletion of camera feeds, manipulation of smart door locks, or unwanted actions such as over-ordering groceries on smart refrigerators. Given that the AiDot app has over 100k downloads solely on the Play Store [9] and AiDot has sold over 10 million Matter bulbs [10], our research underscores the pressing need for immediate action. To mitigate these risks, we emphasize the critical necessity of discontinuing manufacturer apps for Matter devices, particularly the AiDot app, or implementing a restriction to allow only one DMC to operate at any time. This could involve either a direct Wi-Fi connection with the manufacturer app or a Matter over Wi-Fi connection with the smart hub, ultimately enhancing the overall security of the IoT ecosystem.

The contributions of our research are twofold.

- We demonstrate the first practical Codema attack on *certified Matter devices*, from the vantage point of a malicious outsider. The attack occurs discreetly, leveraging a flaw in the manufacturer's implementation, all without disrupting the user's Matter connection or requiring knowledge of in-home devices or the user's Wi-Fi credentials.
- We evaluate this attack on 15 commercial Matter devices across three major smart hubs, highlighting its ease of execution on AiDoT-controlled Matter devices. We also identify security challenges and provide actionable mitigation strategies for device manufacturers to enhance security, including proper management of DMCs and the prompt closure of the pairing window after setup.

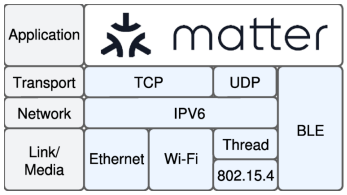

Fig. 2. Mapping Matter in the Device Protocol Stack

II. Background

This section introduces key concepts essential for understanding subsequent sections.

A. IoT Device Onboarding

It refers to the process of integrating a new device into a network, encompassing device initialization, authentication, and configuration. Onboarding is crucial for the establishment of DMC, which extends to cover continuous device management, control, and communication post-onboarding. Common onboarding approaches for IoT devices include:

- Manufacturer-Centric Approach: It uses the manufacturer's app to pair with the device, providing local control (through BLE or Wi-Fi), cloud-based control (via the manufacturer's cloud), or hub-based control (via the manufacturer's hub and cloud).
- Setup Code Configuration: Apple's HomeKit uses a setup code to pair devices with the Apple Home.
- Voice-Activated Devices Setup: Smart speakers like Amazon Alexa use a combination of local (e.g., Bluetooth) and cloud-based connectivity for pairing. Hence, devices are initially paired with manufacturer apps and then integrated with the speaker app.
- Hub-Based Onboarding: Zigbee/Z-Wave devices rely on a central hub to mediate connections.
- Matter QR Code Scanning: QR code is printed on the device and stored in its memory and contains information like vendor ID, product ID, and passcode. Users simply scan the code to complete onboarding.

B. Matter Standard

Matter, formerly known as CHIP (Connected Home over IP), is a collaborative effort led by the Connectivity Standard Alliance (CSA) with around 600 participating companies [11]. It was introduced in Oct 2022 to facilitate seamless interconnectivity among IoT devices, prioritizing security and reliability. Matter implements the Application Layer of the OSI model, leveraging BLE for setup and Wi-Fi and Thread [12] protocols for communication (Fig. 2).

1) Matter Ecosystem:: A Matter network features a Matter controller integrated into leading smart speakers and hubs, such as Apple HomePod and Amazon Echo, capable of interpreting Matter packets. Matter devices come pre-provisioned

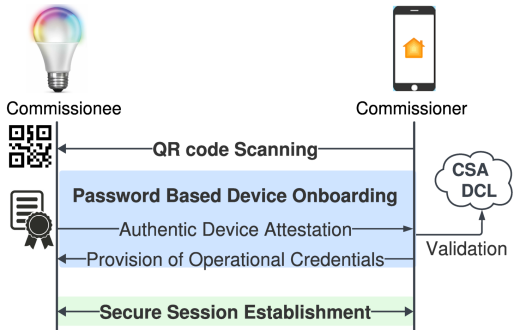

Fig. 3. Matter's Secure Device Commissioning Flow

with essential components, including a QR code and a Device Attestation certificate (DAC) for ensuring authenticity. Each entity in the network has a unique 64-bit identifier. The network may utilize a Thread Border Router [13] for Thread devices or a Matter Bridge to support non-Matter devices, such as those using Zigbee or Z-Wave.

2) Secure Communication Workflow: A Matter device advertises itself using BLE or Domain Name System Service Discovery (DNS-SD). Upon receiving the advertisement or scanning the QR code, the Commissioner, responsible for pairing, obtains the out-of-band passcode and performs Password Authenticated Session Establishment (PASE) with the Matter device, i.e., Commissionee (Fig. 3). The device's DAC is authenticated using a Distributed Compliance Ledger (DCL), which is CSA's blockchain-based network for authorized vendors to document device information. The commissioner then provides information like Root CA Certificate, Node Operational Certificate (NOC), network details, and Access Control List (ACL) to the device. Next, Certificate Authenticated Session Establishment (CASE) is initiated for negotiating symmetric encryption keys. Upon receiving a command, the node validates the sender's NOC using the Root CA Certificate and checks ACL for authorized actions.

Matter's multi-admin feature securely recommissions a device with another Matter ecosystem. As the QR code is intended for first pairing only; subsequent commissioning uses a time-limited pairing code generated by the first hub app. Matter devices only support digitally signed over-the-air updates. Importantly, Matter's security is independent of communication technology, ensuring resilience against unsecured maintenance and remote attacks during operation [14].

III. Exploiting Outsider Access Vulnerability in Matter Devices

This section outlines the threat scenario and the adversary's approach to gaining unauthorized device access.

A. Threat Scenario

We consider a practical scenario where a smart home is equipped with various Matter-enabled devices. The user has seamlessly paired all devices with a Matter-compatible smart hub, such as Google Home, using the devices' QR codes. This enables centralized management through the Google Home app, eliminating the need for individually pairing devices with manufacturer apps. To prevent unauthorized individuals, such as guests from illicitly connecting to the devices, the user has removed the device's QR code stickers and strategically connected devices to a dedicated IoT network, distinct from the default Wi-Fi network.

We envision the adversary as an external entity (e.g., a neighbor or potential burglar) aiming to gain unauthorized, covert, and persistent control over IoT devices for remote access or data exposure. Notably, the adversary lacks knowledge of Wi-Fi credentials, QR codes and has never had prior or current physical access or shared rights to the smart devices, distinguishing them from individuals like Airbnb guests or babysitters who might have had such access. Consequently, all devices and their respective apps remain untampered with and free from physical alterations.

B. Outsider Access Vulnerability

Pairing third-party non-Matter devices with smart hubs requires an initial configuration via the manufacturer's app, before linking with the hub app. This ensures the manufacturer's DMC is closed to unauthorized pairing. In contrast, Matter devices use a QR code for seamless setup with the hub, bypassing the need for configuring the manufacturer's app. Hence, if the manufacturer's DMC is left unenrolled, it could expose the device to unauthorized access.

C. Exploitation Methodology

A straightforward approach is to download various manufacturer apps and utilize their *Add Device* feature to identify devices with open pairing windows. A more sophisticated approach involves capturing wireless traffic from Matter devices by activating monitor mode on the laptop, identifying manufacturers through the organizationally unique identifier of the MAC addresses (particularly if they are not randomized), and downloading respective manufacturer apps to find unsecured devices. In contrast, our strategic approach leverages the widely used AiDot app. We selected it based on our evaluation in the following section, which reveals that all Matter devices vulnerable to unauthorized access are compatible with the AiDot App, regardless of their model or brand (e.g., Linkind, Orein, Mujoy, or Consciot). Hence, the adversary does not need to install multiple manufacturer apps to detect paired devices with unenrolled DMCs.

The adversary initiates the attack by installing the AiDot app and registering an account with self-selected credentials. Enabling Bluetooth and tapping "Add Device" in the app triggers an automated discovery that uncovers pre-configured Matter devices with the manufacturer's DMC inadvertently left open. The adversary then illicitly connects to these devices over Wi-Fi, without alerting the user or disrupting their Matter connection. As the attack originates from a distinct network, it is challenging for the user to detect the intrusion via network logs. Unlike the hub app, which may have limited capabilities (e.g., supporting specific colors for the bulb), the AiDoT app

grants full control over the device. It also discloses critical device information, including its current status, user's complete activity record, MAC address, and IP address. Furthermore, the app reveals network specifics, including the SSID and the router's MAC address belonging to the user's Matter network, which it erroneously retrieves from the bulb's memory.

IV. Evaluation

A. Experimental Setup

We conducted an extensive study to validate that although Matter devices are inherently secure, the manufacturer's oversight in leaving the manufacturer DMC unenrolled after connection establishment potentially compromises the security of their Matter devices. We acquired 15 distinct commercially available Matter devices, such as smart plugs, bulbs, LED strips, and contact sensors, from leading manufacturers like TP-Link, Meross, Sengled, and Govee, as well as from AiDot-specific brands like Linkind, Orien, Consciot, and Mujoy. These devices supported either Matter over Wi-Fi or Matter over Thread protocol. Additionally, to determine if the unauthorized access risks were specific to AiDot-controlled *Matter* devices or extend to standard AiDot devices, we also included AiDot-branded standard Wi-Fi bulbs in our device set. Our evaluation spanned three prominent smart home ecosystems: Apple HomePod Mini, Amazon Echo (4th gen), and Google Nest Hub (2nd gen). Additionally, we used two smartphones connected to two different Wi-Fi networks: one phone served as the user's device with hub and manufacturer apps installed, while the other phone equipped with manufacturer apps served as the outsider's device. Separate email addresses were used to create user and outsider profiles on all apps.

1) Initial Device Setup: The user paired all devices with one hub at a time. Matter devices were seamlessly paired to the hub app by scanning their QR codes. As for AiDot's non-Matter devices, the only option was to link the devices with the AiDot app and integrate them into the hub app.

2) Re-Pairing Attempt by Outsider: User manuals for certain Matter devices suggest pairing within 35-inch proximity to the device and within 15 minutes of activating it, after which the pairing mode deactivates, necessitating a power cycle to reinitiate pairing [15]. As an adversary, the tests were conducted 24 hours after the user paired devices with the hub, and from a distance of nearly 30 feet away from the smart home, with no direct line of sight. Each experiment was replicated thrice to ensure consistency.

3) Ethical Considerations: The research strictly adhered to ethical standards; all IoT devices and smartphones used in the research belonged to us, and no unauthorized connections were established with any device beyond our established network. Consequently, approval from the Institutional Review Board (IRB) was not required.

B. Experiments and Results

First, we employed manufacturer apps for devices to determine if they could scan, identify, and pair with pre-configured devices on a distinct network without requiring any commissioning requisites, such as the device's QR code, the user's Wi-Fi credentials, or physical access to the device. Essentially, the manufacturer's failure to implement these prerequisites facilitates outsiders to attain unauthorized access to the device over direct Wi-Fi or Bluetooth. Once paired, we examined the possibility of outsiders remotely controlling the device without interrupting the user's Matter connection. We summarized our findings for Matter devices in Table I.

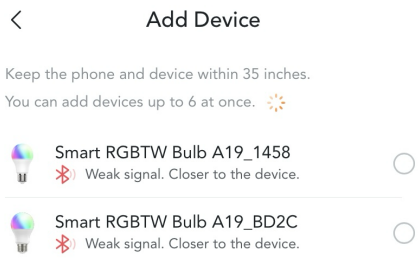

Fig. 4. Outsider Using AiDot App to Gain Unauthorized Access to AiDot-controlled Matter Devices from 30 ft Outside the Smart Home.

1) AiDot-Controlled Matter Devices: All 5 AiDot's Matter devices in our device set were CSA-certified [16]. They do not rely on brand-specific apps; rather, they are controlled through the AiDot app. Upon utilizing the "Add device" feature in the AiDot app, it was surprising to discover that all five devices remained discoverable via Bluetooth even 30 feet away from the smart home. This observation suggests that the devices' pairing window remained open even after the user configured the devices over Matter. In addition, these devices did not require commissioning prerequisites such as QR code, user's Wi-Fi credentials, or device access, and hence any malicious outsider can connect to these devices without requiring technical expertise (see Fig. 4).

Once paired, the outsider can remotely control and monitor these devices without alerting users or disrupting their Matter connection. The results remained consistent across all hubs, irrespective of whether the device operates on Matter over Wi-Fi or Matter over Thread protocol. This underscores a fundamental security issue with the implementation of AiDot devices; where the outsider instead of compromising Matter's robust security can simply bypass it to attain unauthorized access to the device.

2) Non-AiDot Matter Devices: As evident from Table I, the remaining Matter devices exhibited varying security levels. Like Aidot devices, the pre-configured Nanoleaf bulb and Govee LED strip were discoverable via their apps by outsiders, yet re-pairing required fulfilling specific conditions, thereby restricting outsiders' access. For instance, the Nanoleaf app required the device's QR code while the Govee Light required pressing the power button, making them vulnerable mainly to malicious insiders and not outsiders. Similarly, Tp-Link Tapo Plug and Meross Plug, although remained open for re-pairing, were only detectable and paired if the outsider knew the user's Wi-Fi credentials, thereby restricting unauthorized

TABLE I
EVALUATING THE FEASIBILITY OF UNAUTHORIZED PAIRING ATTACK ON PAIRED MATTER DEVICES USING MANUFACTURER APPS. HERE, CONN = CONNECTION, MOW = MATTER OVER WI-FI AND MOT = MATTER OVER THREAD.

Matter Device	Device Conn	Device App	Outsider Detects		Commissioning Requisite			Outsider Attack Feasible?	Stops User Conn?	Limitation
			Distance	Time	QR Code	User Wi-Fi	Device Access			
AiDot's Matter Devices										
Linkind Plug [17]	MoW	AiDot [7]	$>$ 30 ft	Any	No	No	No	Yes	No	None
Linkind Bulb [18]										
Orein Bulb [19]										
Consciot Bulb [20]										
Mujoy Bulb [21]	MoT									
Other Matter Devices										
NanoLeaf Bulb [22]	MoT	NanoLeaf [23]	$>$ 30 ft	Any	Yes	No	No	No	N/A	QR code
Govee LED Strip [24]	MoW	Govee [25]			No		Yes			Press Button
TpLink Tapo Plug [26]		Tapo [27]	No	No	No	Yes	No			User Wi-Fi Access
Meross Plug [28]		Meross [29]								
Sengled Bulb [30]		None				No				App not compatible
Vuytret Plug [31]										
Caupureye Bulb [32]		UHome+ [33]								Pairing Window Closed
Moes Plug [34]		Tuya [35]								
Onvis Plug [36]	MoT	Onvis [37]								
Eve Contact Sensor [38]		Eve [39]								

outsider access to these devices.

Furthermore, certain manufacturer apps do not support their Matter devices such as Sengled Matter Bulb and Vuytret Matter Plug, significantly reducing the attack surface. In contrast, the Caupureye Bulb, Meos Plug, Onvis Plug, and Eve Contact Sensor were unreachable via the app even on the local network, indicating their pairing windows were securely closed after establishing a Matter connection. These findings were consistent across all tested smart hubs.

3) AiDot's Non-Matter Devices: To investigate if the AiDot's unauthorized access issue is linked to flawed Matter standard implementation, we also analyzed AiDot's legacy devices, such as Linkind [40] and Orein [41] Wi-Fi bulbs using the AiDot app. As the user had previously paired the devices with the hub using the standard pairing method, the manufacturer's DMC was occupied, and the pairing window was inaccessible. Consequently, the AiDot app could not detect any unenrolled AiDot devices, effectively shielding them from unauthorized access by an outsider. The results were consistent across Google Nest Hub and Amazon Echo. However, these devices lacked HomeKit code, rendering them incompatible with Apple HomePod.

V. DISCUSSION

Matter addresses security as a foundational tenet [14], advocating for prompt closure of the device's pairing window following commissioning to deter unauthorized access [6]. However, our evaluation demonstrated that some manufacturers do not adhere to the guidelines, allowing outsiders to bypass Matter's robust security and access devices. It is important to understand that while Matter sets the security framework, it does not dictate the manufacturer's decision to offer multiple pairing options to the users. Therefore, the responsibility to implement Matter's security recommendations effectively lies with the manufacturers.

Our understanding is that the rush to bring Matter-compatible devices to market may have resulted in insufficient security checks and testing, leading to overlooked vulnerabilities. AiDot-controlled Matter devices likely share vulnerabilities due to commonalities in their codebases or standardized implementations that contain intrinsic flaws. Given the uniformity in structural design and the standardized approach to channel management, it stands to reason that a vulnerability in one device, such as the Linkind Bulb A, might also affect similar models, like the Linkind Bulb B, and even extend to other Matter-compatible devices from the same manufacturer, such as Linkind plugs.

The AiDot's Matter product line, which currently features bulbs and plugs, is set to expand rapidly to additional device types, like cameras and smart locks. However, this unauthorized pairing flaw, if unresolved, could lead to serious security breaches, including the exposure of confidential content, like camera feeds, to the malicious outsider. It could also jeopardize the integrity of devices, allowing the outsider to potentially tamper with or delete data, such as camera recordings. The potential for physical security breaches, like unauthorized access through smart locks, further underscores the urgency. Therefore, device manufacturers and the research community must focus on enhancing IoT security by actively identifying and addressing such vulnerabilities.

A. Responsible Disclosure

We responsibly disclosed the identified vulnerability to AiDot, CSA, and the manufacturers of the affected devices, three months ago. Despite our efforts to engage through follow-up communications, we received no response from AiDot, Linkind, and Consciot. In contrast, Orein and Mujoy offered replacements for the impacted devices, without recognizing that the security flaw affects their entire product line. According to the CSA, the issue is outside the scope of Matter specification, since the CSA can not dictate how

manufacturers incorporate their software stacks into their devices. Following AiDot's prescribed protocol for reporting vulnerabilities [42], we escalated the issue to the Amazon Vulnerability Research Program [43]. The issue was promptly recognized by Amazon, earning a high vulnerability rating of 8.8 out of 10. Regrettably, the vulnerability remains unresolved as it pertains to third-party devices, which is beyond the direct control of Amazon.

B. Mitigation

Device manufacturers can enhance the security of their Matter devices through the following measures:

1) Implementing Commissioning Prerequisites: Based on our assessment, while some devices were discoverable over Bluetooth, outsider attacks were effectively prevented due to certain prerequisites, such as scanning a QR code, obtaining the victim's Wi-Fi credentials, or physically pressing the power button. Therefore, AiDot devices should implement a commissioning prerequisite at a minimum to deter outsider attacks. Additionally, for enhanced protection against internal threats, users are advised to remove the device's QR code stickers and establish a dedicated network for IoT devices, distinct from their primary Wi-Fi network.

2) Discontinue Manufacturer Apps: Like Sengled and Vuytret, manufacturers should discontinue their proprietary apps for Matter devices, as these apps inadvertently enable outsiders to establish unauthorized connections.

3) Enforce Single Pairing: Manufacturers may provide users with various methods to pair devices, but only one method must be active at a time. This means users can either connect via Wi-Fi using the manufacturer's app or utilize QR codes for Matter connection, but not both simultaneously. For this, it is important to promptly close the pairing window after establishing a connection.

To further fortify device security, manufacturers can integrate CGuard, a centralized access control system designed for IoT devices, to regulate the accessibility of pairing channels at the application level [5]. However, note that integrating it into Matter-enabled devices would require custom development.

C. Limitations

While our demonstrated attack highlights legitimate security concerns, it pertains specifically to AiDot's Matter devices where the manufacturer's DMC remains unenrolled post-pairing. Moreover, while unlikely, should a user set up their device over Wi-Fi using the AiDot app as well as over Matter using the hub app, the device's pairing window would be closed for outsiders.

VI. Related Work

Researchers have extensively investigated security and privacy issues tied to IoT devices utilizing diverse protocols, such as Wi-Fi, Zigbee, and Thread [44], [45]. The primary emphasis of these studies has been on thwarting unauthorized access to devices and their data [46], [47] and detecting such attacks through network traffic analysis [48], [49]. Despite considerable efforts, these methods fall short of identifying and preventing our proposed unauthorized pairing attack, which originates from a distinct network.

In parallel, researchers have developed experimental frameworks that allow devices to self-assess the security of the operating DMC [50], [52] or explore malicious interactions among DMCs [53], [54]. Notably, some studies have showcased how an adversary could gain unauthorized access to smart devices using unused Bluetooth [51], [55] or Wi-Fi-associated DMCs [5]. The *Codema Flaw 1 and 2*, previously identified [5], are particularly relevant to our scenario. It is crucial to note that Codema Flaw 1 targets devices using HomeKit code and necessitates access to the victim's Wi-Fi network and knowledge of the devices, while Codema Flaw 2 specifically affects Philips Hue devices [5]. In contrast, our research marks the first practical demonstration of the Codema attack on *CSA-certified Matter devices*, executed covertly from an outsider's viewpoint and without the need for advanced technical skills.

Considering Matter's recent emergence, CSA has publicly released key resources such as the Matter specification [6], Matter Cluster Library [56], Matter Device Library Specification [57] and Matter SDK [58] to foster research and development of Matter-compatible devices. While some theoretical studies on Matter have attempted to identify potential security and privacy vulnerabilities within the standard [59], [60] and provided security considerations for developers [61], no prior study has practically demonstrated any attack on real Matter devices to date.

VII. Conclusion

While Matter emerges as a promising standard for the IoT landscape, our experiments have compellingly demonstrated that the manufacturer's failure to leave any DMC unenrolled allows adversaries to effortlessly bypass Matter's security and gain unauthorized access to already-paired Matter devices. Our analysis highlights the heightened susceptibility of AiDot's Matter-enabled devices to this covert attack, neither requiring physical device access nor the victim's Wi-Fi credentials. This raises significant privacy and security risks to smart home environments, particularly as the company expands Matter to critical surveillance devices, such as cameras and door locks, all of which inherently become vulnerable to unauthorized access by outsiders. We have responsibly disclosed our discoveries to AiDot and the manufacturers of the affected devices. In light of these findings, it is imperative for device manufacturers to promptly address this vulnerability by enforcing the activation of a single DMC at any given time and conducting rigorous security assessments to ensure the overall robustness of Matter-enabled devices.

Acknowledgment

We would like to thank the reviewers for their invaluable feedback. This research was supported by the National Science Foundation under grant numbered 2144914.

REFERENCES

[1] Apple Inc., *HomePod Mini*, Retrieved Jan 2024 from https://www.apple.com/homepod-mini/, 2023.

[2] Google, *Google Nest and Home device specifications*, 2023, [Online]. Available: https://support.google.com/googlenest/answer/7072284.

[3] Amazon, *Amazon Echo & Alexa Devices*, 2023, [Online]. Available: https://www.amazon.com/b?&node=9818047011.

[4] SmartThings, *Works with SmartThings*, 2023, [Online]. Available: https://www.smartthings.com/works-with-smartthings.

[5] Y. Jia, B. Yuan, L. Xing, D. Zhao, Y. Zhang, X. Wang, Y. Liu, K. Zheng, P. Crnjak, Y. Zhang, and others, *Who's in control? On security risks of disjointed IoT device management channels*, Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security, pages 1289–1305, 2021.

[6] CSA, *Matter Core Specification Version 1.2*, 2024, [Online]. Available: https://csa-iot.org/developer-resource/specifications-download-request/.

[7] AiDot Inc, *AiDot - Connecting Home Devices*, 2023, [Online]. Available: https://apps.apple.com/us/app/aidot/id1580685276.

[8] AiDot, *AiDot Matter Products*, 2022, [Online]. Available: https://www.aidot.com/matter-product.

[9] AiDot Inc, *AiDot - Smart Home Life*, 2024, [Online]. Available: https://play.google.com/store/apps/details?id=com.iotsolution.aidot.

[10] IoT Insider, *AiDot introduces the 'world's first' Matter-certified air purifier WELOV*, 2024, [Online]. Available: https://www.iotinsider.com/smart-world/aidot-introduces-the-worlds-first-matter-certified-air-purifier-welov/.

[11] CSA, *Matter - The Power of Membership*, 2023, [Online]. Available: https://csa-iot.org/members/.

[12] Thread Group, *Thread 1.3.0 Features White Paper*, 2022, [Online]. Available: https://www.threadgroup.org/Portals/0/documents/support/Thread1.3.0WhitePaper_07192022_3990_1.pdf.

[13] Espressif, *Matter: Thread Border Router in Matter*, 2023, [Online]. Available: https://blog.espressif.com/matter-thread-border-router-in-matter-240838dc4779.

[14] CSA, *Matter Security and Privacy Fundamentals*, 2022, [Online]. Available: https://csa-iot.org/wp-content/uploads/2022/03/Matter_Security_and_Privacy_WP_March-2022.pdf.

[15] Tapo, *Matter Setup Guides for Alexa, Google and Apple*, 2023, [Online]. Available: https://www.tapo.com/us/faq/294/.

[16] PR Newswire, *Smart light bulbs and Smart Plug from AiDot Ecosystem are one of the First to be Matter-certified*, 2022, [Online].

[17] Linkind, *Linkind Matter Smart Plug, Matter over Wi-Fi*, 2024, [Online]. Available: https://www.amazon.com/Linkind-SmartThings-Automation-Control-Schedule/dp/B0C371HB66/.

[18] Linkind, *Linkind WiFi Smart Light Bulb*, 2022, [Online]. Available: https://www.amazon.com/Linkind-Matter-Certified-A19-Equivalent/dp/B0BHS2QG6C.

[19] OREiN, *Orein Matter Smart Light, Matter over Wi-Fi*, 2022, [Online]. Available: https://www.amazon.com/OREiN-Reliable-Changing-Assistant-SmartThings/dp/B0BLTWFJWY/.

[20] Consciot, *Consciot Smart Light bulb, Matter over Wi-Fi*, 2023, [Online]. Available: https://www.amazon.com/Consciot-Bluetooth-Changing-Google-Equivalent/dp/B0CBK9JZWZ/.

[21] Mujoy, *Mujoy Smart Light Bulbs, Matter over Thread*, 2023, [Online]. Available: https://www.amazon.com/mujoy-Matter-Changing-A19-Equivalent/dp/B0BTY1DHKD/.

[22] Nanoleaf, *Nanoleaf Essentials Smart Color-Changing Bulb*, 2023, [Online]. Available: https://www.amazon.com/Nanoleaf-Essentials-Smart-Color-Changing-Light/dp/B0C1JD5YXW.

[23] Nanoleaf, *Nanoleaf - Smarter by Design*, 2020, [Online]. Available: https://apps.apple.com/us/app/nanoleaf/id1049333656.

[24] Govee *Govee M1 RGBIC LED Strip Lights with Matter*, 2022, [Online]. Available: https://www.amazon.com/dp/B0B42BWVLM.

[25] Shenzhen Intellirocks Tech Co. Ltd, *Govee Home*, 2023, [Online]. Available: https://apps.apple.com/us/app/govee-home/id1395696823.

[26] TpLink, *TP-Link Tapo Matter Compatible Smart Plug Mini*, 2022, [Online]. Available: https://www.amazon.com/dp/B0BNWGZ545?ref_=cm_sw_r_cp_ud_dp_22YETC5PYMKFXH9DSZ11.

[27] TpLink Global Inc, *TP-Link Tapo*, 2022, [Online]. Available: https://apps.apple.com/us/app/tp-link-tapo/id1472718009.

[28] Meross, *meross Matter Smart Plug Mini*, 2024, [Online]. Available: https://www.amazon.com/dp/B0CJFJG124?_encoding=UTF8&psc=1&ref_=cm_sw_r_cp_ud_dp_RC2GFNMK66PGRE3PDYEH.

[29] Chengdu Meross Technology Co.,Ltd, *Meross*, 2017, [Online]. Available: https://apps.apple.com/gb/app/meross/id1260842951.

[30] Sengled, *Sengled LED Smart Light Bulb (A19)*, 2023, [Online]. Available: https://www.amazon.com/Sengled-Matter-Enabled-Multicolor-Equivalent-Instant/dp/B0C6QY1DRW.

[31] Vuytret, *Vuytret Matter Smart Plug Mini, Matter over Wi-Fi*, 2023, [Online]. Available: https://www.amazon.com/Vuytret-Matter-Google-SmartThings-Certified/dp/B0C822VMZM/.

[32] Caupureye, *Caupureye Light Bulbs with Matter*, 2023, [Online]. Available: https://www.amazon.com/dp/B0CDZQVL2Q?_encoding=UTF8&psc=1&ref_=cm_sw_r_cp_ud_dp_8YQ3G5BR9A3NZMB7F64T.

[33] Universal Ascent Holdings Limited, *uHome+ Smart Home Assistant*, 2022, [Online]. Available: https://apps.apple.com/us/app/uhome/id1629607697.

[34] MOES, *MOES Matter Smart Plug with Energy Monitoring*, 2023, [Online]. Available: https://www.amazon.com/MOES-Matter-Monitoring-Assistant-Compact/dp/B0CF887Z9P.

[35] Tuya Smart Inc, *Tuya Smart*, 2017, [Online]. Available: https://apps.apple.com/us/app/tuya-smart/id1034649547.

[36] Onvis, *Onvis Smart Plug, Matter Over Thread*, 2023, [Online]. Available: https://www.amazon.com/dp/B0C143YZY6?_encoding=UTF8&psc=1&ref_=cm_sw_r_cp_ud_dp_Z9WQ9Q85S3H70KCW62S1.

[37] Shenzhen Champon Technology Co., Ltd, *Onvis Home*, 2019, [Online]. Available: https://apps.apple.com/us/app/onvis-home/id1434369138.

[38] Eve, *Eve Door & Window (Matter) – Smart Contact Sensor*, 2023, [Online]. Available: https://www.amazon.com/dp/B0BZSY26WP?ref_=cm_sw_r_cp_ud_dp_PS07ERXPQWW5GXHJVXHC.

[39] Eve Systems GmbH, *Eve for Matter & HomeKit*, 2015, [Online]. Available: https://apps.apple.com/us/app/eve-for-matter-homekit/id917695792.

[40] Linkind, *Linkind Smart Light Bulbs, Smart Bulb That Work with Alexa & Google Home*, 2022, [Online]. Available: https://www.amazon.com/dp/B0BC8N7QXN?ref_=cm_sw_r_cp_ud_dp_R02Y7RJBZAMXS6H3VSRN.

[41] Orein, *OREiN Smart LED Edison Light Bulb* , 2022, [Online]. Available: https://www.amazon.com/dp/B0B7WYXFT9?_encoding=UTF8&psc=1&ref_=cm_sw_r_cp_ud_dp_RFN4EYJBEGH6MJ0MN18M.

[42] AiDot, *AiDot Privacy and Security*, 2022, [Online]. Available: https://www.aidot.com/page/security/index/.

[43] HackerOne, *AiDot Privacy and Security*, 2023, [Online]. Available: https://hackerone.com/amazonvrp, 2023.

[44] B. Yuan, J. Wan, Y. Wu, D. Zou, and H. Jin, *On the Security of Smart Home Systems: A Survey*, Journal of Computer Science and Technology, volume 38, number 2, pages 228–247, Springer, 2023.

[45] N. Shafqat, D. J. Dubois, D. Choffnes, A. Schulman, D. Bharadia, and A. Ranganathan, *Zleaks: Passive Inference Attacks on Zigbee Based Smart Homes*, in *International Conference on Applied Cryptography and Network Security*, pages 105–125, 2022, Springer.

[46] B. Janes, H. Crawford, and TJ. OConnor, *Never ending story: Authentication and access control design flaws in shared IoT devices*, In IEEE Security and Privacy Workshops (SPW), pages 104–109, 2020.

[47] D. Granata, M. Rak, G. Salzillo, U. Barbato, and others, *Security in IoT Pairing & Authentication protocols, a Threat Model, a Case Study Analysis*, ITASEC, pages 207–218, 2021.

[48] M. Chowdhury, B. Ray, S. Chowdhury, and S. Rajasegarar, *A novel insider attack and machine learning-based detection for the internet of things*, ACM Transactions on Internet of Things, volume 2, number 4, pages 1–23, ACM New York, NY, USA, 2021.

[49] A. Y. Khan, R. Latif, S. Latif, S. Tahir, G. Batool, and T. Saba, *Malicious insider attack detection in IoTs using data analytics*, IEEE Access, volume 8, pages 11743–11753, IEEE, 2019.

[50] Z. B. Celik, P. McDaniel, and G. Tan, *Soteria: Automated {IoT} safety and security analysis*, 2018 USENIX Annual Technical Conference (USENIX ATC 18), pages 147–158, 2018.

[51] J. Wu, Y. Nan, V. Kumar, D. Jing Tian, A. Bianchi, M. Payer and D. XU, *{BLESA}: Spoofing attacks against reconnections in Bluetooth low energy*, 2018 14th USENIX Workshop on Offensive Technologies (WOOT 20), 2020.

[52] J. Lee, S. Kang, and S. Kim, *Study on the smart speaker security evaluations and countermeasures*, Advanced Multimedia and Ubiquitous Engineering: MUE/FutureTech 2019 13, pages 50–70, 2020.

[53] W. Zhou, Y. Jia, Y. Yao, L. Zhu, L. Guan, Y. Mao, P. Liu, and Y. Zhang, *Discovering and Understanding the Security Hazards in the Interactions between IoT Devices, Mobile Apps, and Clouds on Smart Home Platforms*, 28th USENIX Security Symposium (USENIX Security 19), pages 1133–1150, 2019.

[54] H. Chi, Q. Zeng, and X. Du, *Detecting and Handling IoT Interaction Threats in Multi-Platform Multi-Control-Channel Smart Homes*, in *32nd USENIX Security Symposium (USENIX Security 23)*, pages 1559–1576, 2023.

[55] D. Antonioli, N. O. Tippenhauer, K. Rasmussen, and M. Payer, *BLURtooth: Exploiting Cross-Transport Key Derivation in Bluetooth Classic and Bluetooth Low Energy*, in Proceedings of the 2022 ACM on Asia Conference on Computer and Communications Security, pp. 196–207, 2022.

[56] CSA, *Matter Application Cluster Specification, Version 1.2*, CA, USA, 2023.

[57] CSA, *Matter Device Library Specification, Version 1.2*, CA, USA, 2023.

[58] CSA, *Matter SDK*, 2024, [Online]. Available: https://github.com/project-chip/connectedhomeip.

[59] M. Loos, *Security Analysis of the Matter Protocol*, 2023, [Online]. Available: https://oparu.uni-ulm.de/xmlui/bitstream/handle/123456789/49010/Matter_MLO2023.pdf?sequence=5.

[60] S. Singh, *Intercompatibility of IoT Devices Using Matter: Next-Generation IoT Connectivity Protocol*, International Conference on Advances in IoT and Security with AI, pages 49–58, Springer, 2023.

[61] Schutzwer, *Security Considerations for Matter Developers*, 2023, [Online]. Available: https://www.schutzwerk.com/en/blog/matter-security-considerations/.