Poster: An Investigation of Matter Smart Home Mechanisms to Mitigate Denial-of-Service (DoS) Attacks

Andrew Losty
andrew.losty.23@ucl.ac.uk
University College London

Anna Maria Mandalari
a.mandalari@ucl.ac.uk
University College London

Abstract

The rapid expansion in the use of Internet-of-Things (IoT) devices in smart homes has introduced numerous security challenges, due to their diverse architectures, lack of standardized protocols, and differing security implementations. These challenges make IoT devices particularly vulnerable to security and privacy attacks. The introduction of the Matter IoT standard represents a significant shift in the architecture of the smart home ecosystem, prompting important security questions to be raised regarding the adoption of a unified multi-vendor protocol. While adopting a single ecosystem can reduce the attack surface and enhance scrutiny across devices, it also raises the risk of widespread security breaches if a single vulnerability is exploited. This research identifies a potential threat to home security by demonstrating viable security attacks on Matter smart home devices. Specifically, the research explores how DoS flooding attacks are capable of selectively incapacitating Matter devices, such as security cameras, door locks, and sensors.

CCS Concepts

• **Networks** → **Network protocol design**; • **Security and privacy** → **Denial-of-service attacks**;

Keywords

Security, Privacy, Matter, Internet of Things, Denial of Service

1 Introduction

The growing adoption of Smart Home IoT devices, their proliferation in critical applications and an increasingly sophisticated security threat model has led to increased concerns regarding the threat from Denial-of-Service attacks. This was highlighted by Chen et all., who observed that "DoS is one of the most catastrophic attacks against IoT devices" [1]. Matter is a new Smart Home IoT specification that aims to build a common highly secure communication framework that can be adopted by a large range of manufacturers[2]. The adoption of a single ubiquitous protocol may however potentially increase risk as any vulnerability may be exhibited by a far larger and more diverse range of devices.

The research acknowledges that the limited CPU and storage resources of smart appliances may impact their resilience to DoS attacks. Matter devices have a suggested minimum of 1MB of flash memory / 256kB of RAM.

We aim to answer the following three research questions:
RQ1: How effective are Matter Smart-Home DoS mitigation techniques when evaluated in a controlled laboratory environment?
RQ2: What research or commercial information is available that defines Matter DoS defence mechanisms?
RQ3: How can an effective methodology be developed to evaluate Denial-of-Service (DoS) exploits against Matter Thread 802.15.4 connections?

Our research focuses on evaluating the security mechanisms of Matter devices, specifically their ability to withstand DoS attacks. We conducted lab experiments with multiple Matter ecosystems and devices from three vendors. A reconnaissance of Matter devices is performed over IPv4/IPv6 to identify open ports and services. Wireless Matter devices are then subjected to DoS attacks. Testing shows that 802.11-connected Matter devices are vulnerable and rendered inoperable during attacks. These DoS attacks could potentially exploit compromised consumer routers to target local Matter devices.

By conducting laboratory experiments and reviewing existing literature, we aim to provide a deeper understanding as to the level of resilience that Matter devices exhibit under such conditions. Furthermore we plan to perform DoS testing on Thread IEEE 802.15.4 devices [3], in order to reveal if additional vulnerabilities are present.

2 Background

The goals of the Matter Smart Home protocol are hugely ambitious. Matter is an open-source, unified IPv6 based Smart Home protocol that provides increased levels of connectivity and security. Matter supports local operation without the need for an Internet connection, however cloud connectivity is required for device commissioning.

The Matter protocol aims to provide inter-connectivity of Smart Home IoT allowing devices to be shared between ecosystems, with the formation of a single ecosystem that supports devices from over 270 manufacturers [4]. Prior to the release of Matter, Smart Home environments were formed from multiple separate isolated proprietary ecosystems each with their own applications, communications framework, and security mechanisms. Matter is an open-source, royalty-free framework that "enables developers and device manufacturers to build reliable, secure ecosystems and increase compatibility". In December 2019 a working group founded by Amazon, Apple, Google and the Zigbee Alliance, collaborated to develop a new open-source Smart Home IoT environment that supported a range of devices with a single management protocol. The development group was formalised as the 'Connectivity Standards Alliance' (CSA) and went on to release the initial specification of Matter 1.0 in October 2022. There have since been three revisions of the Protocol: 1.1, 1.2 and 1.3. The CSA white paper 'Matter Security and Privacy Fundamentals' is a 9-page document that defines the need to protect Matter devices from Distributed-Denial-of-Service (DDoS) attacks. The paper describes how "Several mechanisms have been built in the Matter definition to prevent the most common DoS

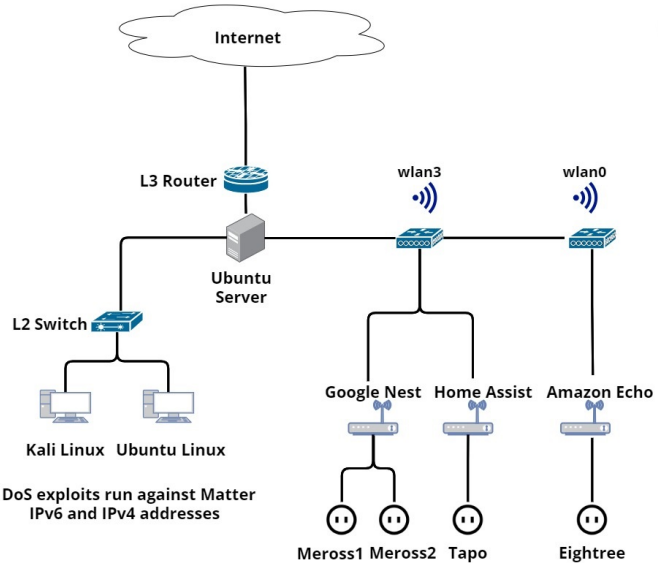

Figure 1: Matter DoS Test Environment.

attacks" and goes on to describe how Matter introduces a sophisticated message counter mechanism to offer this resilience. It details how Matter uses 32-bit message counters in order to protect Matter communications by providing both Duplicate Message Detection and Replay Prevention. Although the CSA outlines a mechanism to prevent DoS outages, it does not define the mechanism or the attack methods.

3 Experimentation Environment

We establish a Matter test environment that includes three ecosystems and a range of Matter devices. The chosen ecosystems are Google Nest, Amazon Echo and Home Assist. The devices from three manufacturers Meross, Eightree and Tapo, are all smart plugs and all connect via 802.11 Wireless connections. Having Matter devices with the same functionality allows for a direct comparison of results. We perform DoS testing from an Ubuntu 22.04.4 LTS server, running a Xeon(R) 4114 CPU 2.20GHz and with Wireless AR9462 2.4GHz 300Mbps adapters.

The attacks described in this research focus on DoS exploits where an attack is launched from a specific possibly compromised host to selected Matter devices.

A network reconnaissance using NMAP(7.8), Nessus Expert(10.7.4) and ZenMAP (7.94) identify details of the Matter devices, this is followed by the execution of a suite of DoS exploits to the IPv4/IPv6 addresses of the Matter devices.

4 Denial of Service (DoS) Exploits

Matter control and data communications are limited to IPv6 using UDP port 5540 and TCP/UDP port 5353 for multicast network/neighbour discovery. While not required for core operations, Matter devices obtain an IPv4 address and utilise ports for both DNS(53), and NTP(123).

We select three utilities to allow custom packets generation and flooding: these are Hping3 (3.0.0), Metasploit (6.3.55) and Scapy (2.5.0). The utilities allow packet manipulation with changes made to the source MAC address and data payload size.

Device	Type
Google Nest Hub (2nd Gen)	Smart Hub
Amazon Echo (DOT 5)	Smart Hub
Home Assistant	Smart Hub
Meross Smart Plug (1) (MSS315)	Smart Plug
Meross Smart Plug (2) (MSS315)	Smart Plug
Eightree Smart Plug (ET36)	Smart Plug
Tapo Smart Plug (P110M)	Smart Plug

Table 1: Matter Controllers and Devices

We perform DoS Syn-flooding using Scapy on the IPv6 address of the target devices, resulting in the Meross and Eightree devices losing connectivity or causing the application to halt communication. While the Tapo device does not fully lose connectivity, it suffers significant intermittent loss and delays operation. We observe that a requirement for a successful DoS attack is crafting the packets to appear as though they originate from the Matter controller. We perform a wider range of exploits using IPv4 utilities against the target devices. The DoS Syn, UDP, ACK floods, IP-Fragment, and LAND attack tests are successful in incapacitating the selected Matter devices within a 10-minute time window. The Tapo device appears more resilient, with only the IP-Fragment attack being successful.

5 Conclusion

Our research identifies a significant vulnerability in Matter Smart Home devices, highlighting the potential for DoS attacks that compromise security. During controlled testing in a lab environment, devices from Meross, Eightree, and Tapo were successfully rendered inoperable during the DoS attack. The research suggests that security devices such as cameras, door locks and security sensors may be targeted in real-world scenarios. A possible attack vector could include the hijacking of consumer internet routers from which targeted DoS attacks are launched.

Further research is proposed to enhance understanding of the identified vulnerabilities by expanding testing to a broader range of Matter devices, including those that connect via Thread (IEEE 802.15.4). This research will reveal whether low power mesh Thread-connected devices, are similarly vulnerable to DoS attacks. We plan to refine the testing framework to incorporate automated tools to identify Matter devices for more targeted attack mechanisms. This research area is original, with no existing literature found regarding DoS vulnerabilities in Matter devices. This suggests it offers new insights into the security of the Matter protocol.

References

[1] Q. Chen, H. Chen, Y. Cai, Y. Zhang, and X. Huang, "Denial of Service Attack on IoT System," in *2018 9th International Conference on Information Technology in Medicine and Education (ITME)*, Oct. 2018, pp. 755–758, iSSN: 2474-3828. [Online]. Available: https://ieeexplore.ieee.org/document/8589403

[2] "What is Matter?" [Online]. Available: https://developers.home.google.com/matter/overview

[3] I. Unwala, Z. Taqvi, and J. Lu, "Thread: An IoT Protocol," in *2018 IEEE Green Technologies Conference (GreenTech)*, Apr. 2018, pp. 161–167, iSSN: 2166-5478. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8373620

[4] "Our Members | Promoters | Participants | Adopters." [Online]. Available: https://csa-iot.org/members/