An Investigation of Matter Smart Home mechanisms to mitigate Denial-of-Service (DoS) attacks

Andrew Losty , Anna Maria Mandalari

Department of Electronic and Electrical Engineering (EEE)

UCL

Researcher background

My PhD research focuses on the investigation of Internet of Things (IoT) protocols that influence online security with the objective of improving both the personal privacy and the protection of IoT devices.
I previously completed Masters degrees in Telecommunications (UCL) and Information security (Royal Holloway)

I have worked in industry for many years and have gained experience in a number of networking and security roles.

Matter Introduction

Matter is a newly-released open-source connectivity protocol that provides a common architecture for Smart Home devices. The Matter standard has been developed by many leading Smart Home technology providers including Google, Amazon, Apple and Samsung. Matter is controlled by the CSA (Connectivity Standards Alliance) and has over 600 members. It is estimated that 5.5 Billion Smart Home Matter-Compliant Devices will Ship Between 2022 and 2030 [1].

Matter Protocol Stack

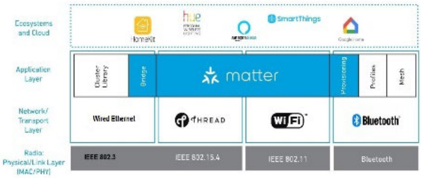

Figure 1 Matter Protocol Stack [2]

Matter runs at the Application layer and supports device communications running over IPV6 on Wired (802.3), Wi-Fi (802.11) and Thread (802.15.4) connections. Bluetooth LE is only used for device management / commissioning**.**

Matter Architecture and DoS execution path

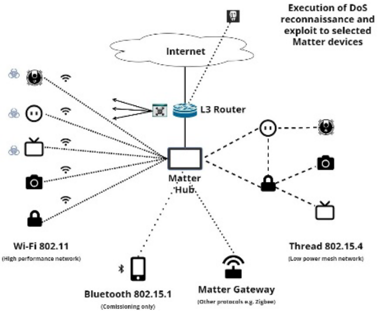

Figure 2 Matter Architecture – Controller / devices over Wireless, Thread and "other protocols".

Stage1: Exploit control Home router, install malicious code.
Stage2: Launch flooding and packet manipulation attacks
up selected Matter devices.

Research Questions.

- **How effective are Matter Smart-Home DoS mitigation techniques when evaluated in a controlled laboratory environment?**

- **What research or commercial information is available that defines Matter DoS defence mechanisms?**

DoS exploit

The study evaluates the resilience of Matter devices against DoS flood and packet manipulation attacks originating from compromised home internet routers. A test environment includes ecosystems like Google Nest, Amazon Echo, and Home Assistant, integrating Matter-compatible smart plugs from Meross, Eightree, and Tapo via 802.11 Wi-Fi. Network.

Reconnaissance is first performed using tools such as NMAP in order to identify both Matter device and Controllers. DoS attacks, including SYN-Flood, UDP-Flood, ACK-Flood, IP-Fragment, and LAND attacks, are executed with Hping3, Metasploit, and Scapy, targeting both IPv4 and IPv6 using spoofed MAC and IP addresses mimicking the Matter controller.

Results

Whan subject to DoS attacks in a lab environment Matter devices were seen to become inoperative within 60 seconds. There was however some variation in results between device manufacturers.

The success of the attack relied on DoS traffic spoofing the MAC and IP addresses, making it appear to originate from Matter controller.

Research Challenges

There have been challenges in accessing detailed protocol information. Despite the specification being an 899-page document, gaps remain. Inquiries to the Connectivity Standards Alliance (CSA) often result in responses stating that certain details are not publicly disclosed.

Additional hurdles include limited published research material, the immaturity of the market, with more products available in the U.S. There is also a scarcity of Thread 802.15.4 network interfaces, which are essential for Matter's full implementation and testing.

References
[1] A. B. I. Research, 'More Than 5.5 Billion Smart Home Matter-Compliant Devices will Ship Between 2022 and 2030'. Accessed: Dec. 07, 2023. [Online]. Available: https://www.prnewswire.com/news-releases/more-than-5-5-billion-smart-home-matter-compliant-devices-will-ship-between-2022-and-2030--301477876.html

[2] https://www.rfwireless-world.com/Terminology/Thread-vs-Matter-Protocol.html

E: andrew.losty.23@ucl.ac.uk
E: a.mandalari@ucl.ac.uk

University College London, Roberts Building - Department of Electronic & Electrical Engineering, 1108 Torrington Place, London, WC1E 7JE, United Kingdom