4. Methodology

According to Matter's developers, it is claimed that "This industry-unifying standard is a promise of reliable and secure connectivity" (CSA, N.D.a). In particular, the users of the new communication standard are relieved of responsibility. CSA (2022a) states that “Customers buying Matter devices will not have to think about security: it is just there”.

These statements can be rated as particularly interesting since Matter is currently based on the communication standards Wi-Fi, BLE and Thread and these each have known vulnerabilities (Bernal et al., 2018; CVE, N.D.a; CVE, N.D.b). This raises the question of whether Matter is able to overcome the vulnerabilities of Bluetooth sniffing, de-authentication attacks and replay attacks of the communication standards on which the new standard is based.

4.1 Type of research and approach

To investigate this question, experiments have been carried out in a Matter network, which are based on known and dominant vulnerabilities in the Wi-Fi and BLE communication standards. Therefore, the present project can be classified as an analytical project. An analytical approach makes sense in this context, since known vulnerabilities in the old communication standards have already been examined in depth, so that penetration testing procedures that have already been developed and tested for these standards can be transferred to the new standard Matter.

The project approach follows deductive reasoning, since the experiments are intended to evaluate CSA's claim regarding the security of Matter and thus whether central security aspects based on known vulnerabilities have been taken into account. A quantitative data collection was carried out, based on a comparison of the results of known penetration testing methods of established communication standards and the new Matter standard. This made it possible to determine in direct correlation whether a threat can also be applied to Matter by using the accuracy metric.

Various communication networks were set up to collect data. These were a Matter network, as well as the control networks of the Wi-Fi and BLE standards. With the help of the control networks, penetration testing procedures were carried out with regard to explicit vulnerabilities, so that comparative data were available for the subsequent experiments. The tests were then carried out in a Matter network using the same procedure. Based on the control experiments, it was then possible to validate whether Matter demonstrates better security with regard to the selected penetration tests.

4.2 Specific research details

To create and carry out the experiments, Matter networks were created, which consisted of the three components AP, control device (hub) and Matter device as shown in Figure 8. A home WiFi router that supports the WiFi standards 802.11g/n/ac/w was used as the AP for the Matter network. This formed the basis of the network.

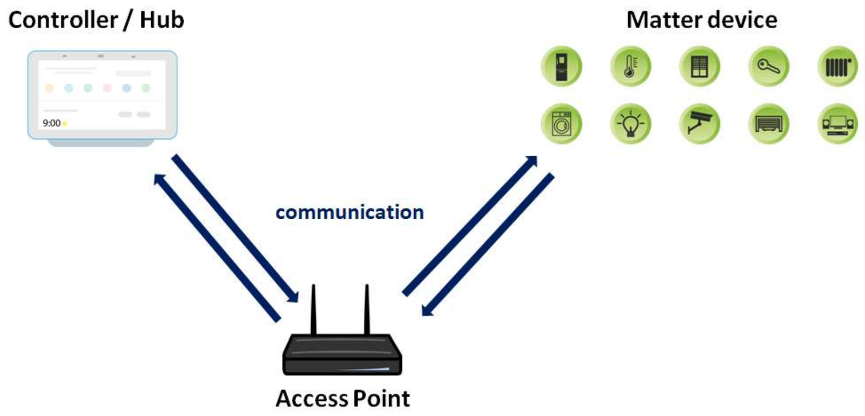

Figure 8: Matter network architecture diagram

The ESP32-S3-DevKitC-1 microcontroller was used as the Matter device (Espressif Systems, 2023). Matter supports ESP32 microcontrollers and states in their Github repository that the ESP32-S3 series can be used for the applications all-cluster-app and lighting-app (Patil et al., 2023). The microcontroller used has a built-in LED, which can be controlled via Matter. It should be noted that in addition to the ESP32 controller, Matter also supports a large number of other device types. However, the choice fell on an ESP32 microcontroller, as this offers a cost-effective way to create Matter-compatible devices.

Various devices were tested and used as control devices for the Matter-based network. These include the devices Google Nest Hub (2nd generation) and iPad (3rd generation), which are explicitly intended as a hub, as well as a computer running the Ubuntu 22.04 TLS operating system, which can be used as a test hub using the chip tool (Kajor et al., 2023).

Appropriate devices corresponding to the experiments were used as comparison networks. A smartphone (Huawei P30) and an AppleWatch were used as part of the Bluetooth testing. Furthermore, the nRF52840 semiconductor was used to carry out the BLE sniffing, which enables the detection of BLE packets via Wireshark (Nordic, 2023; Wireshark Foundation, N.D.). Thus, the collected packets could be analysed using Wireshark.

For the de-authentication attack, an Ubuntu 22.04 TLS computer (acer Aspire V7 series ZRQ), as well as the home Wi-Fi router and an AP provided by a smartphone (Huawei P30) were used as a test network. The execution of the de-authentication attack was realised by the DSTIKE Deauther MiNi V3 (DSTIKE, N.D.).

The comparison test of the replay attack was carried out using a client-server setup between two Ubuntu 22.04 TLS computers. As in the Matter network experiment, Wireshark was used, which allowed the data packets sent to be recorded. Furthermore, an attempt was made to remotely record the packets sent via the Wi-Fi network using the corresponding Wi-Fi dongles tp-link TL-WN722N and BrosTrend AC1200. The Python-based Scapy tool (version 2.5.0) was used to execute the replay attack, which is able to read, manipulate and resend the information packets collected by Wireshark (Scapy, N.D).

4.3 Risk assessment

Regarding possible challenges and risks related to this project, some aspects had to be considered to guarantee the success of the project.

First of all, it had to be taken into account that although Matter was in a published version at the start of the project, there were regular changes to the open source Matter repository over the course of the project. The risk had to be taken into account that by the time the project was completed, the outcomes resulting from the project could no longer be transferred to the updated version of Matter and would therefore be outdated. To minimise this risk, the data collection processes were recorded in detail so that the experiments can be repeated shortly before the project is completed using the latest version of the Matter Repository, so that changes in the test results can be adjusted accordingly. However, it cannot be guaranteed that the research results will be comparable with the newest version of Matter after the project has been completed.

Another risk is that the data collected could have only limited meaning in relation to the research question. Matter is a comparatively new communication standard, so there is currently hardly any scientific literature focusing on the security of Matter that can be used for comparison. The project was therefore subject to the risk that sufficient validation was not possible on the basis of the experiments. In order to counteract this risk, procedures and penetration testing of vulnerabilities were chosen which are typical for the communication standards compatible with Matter. This guaranteed as a minimum goal that an assessment could be made as to whether the successful hacking attempts of the other standards were also successful with Matter.

Furthermore, the cost factor represented another risk for this project. Devices had to be purchased to carry out the experiments. It had to be taken into account that the planned experiments were also feasible from a financial point of view. A risk would have emanated from tests that would have included Thread in addition to the Wi-Fi and BLE communication standards, since a compatible infrastructure would have had to be created for this using a border router. Since appropriate devices such as a network router or BLE-capable end devices such as smartphones were available for the examination of Wi-Fi and BLE, the cost factor could be significantly reduced.

References

Bernal, A. J. P., Parra, O. J. S. & López, A. A. (2018) Vulnerabilities and Attacks on WiFi Networks. *International Journal of Applied Engineering Research 13*(15): 12052-12054. Available from: http://www.ripublication.com/ijaer18/ijaerv13n15_49.pdf [Accessed 11 May 2023].

CSA (2022a) Matter Security and Privacy Fundamentals. Available from: CSA_Matter_Security_WP.docx (csa-iot.org) [Accessed 06 April 2023].

CSA (N.D.a) The Foundation for Connected Thing. Available from: https://csa-iot.org/all-solutions/matter/ [Accessed 16 March 2023].

CVE (N.D.a) Thread Project. Available from: https://www.cvedetails.com/vulnerability-list/vendor_id-18345/product_id-46709/Thread-Project-Thread.html [Accessed 11 May 2023].

CVE (N.D.b) Bluetooth. Available from: https://www.cvedetails.com/vulnerability-list/vendor_id-11436/Bluetooth.html [Accessed 11 May 2023].

DSTIKE (N.D.) DSTIKE WiFI Deauther MiNi V3. Available from: https://dstike.com/products/dstike-wifi-deauther-mini [Accessed 13 July 2023].

Espressif Systems (2023) ESP32-S3 – ESP-IDF Programming Guide. Available from: https://docs.espressif.com/projects/esp-idf/en/latest/esp32s3/esp-idf-en-v5.2-dev-1805-g9a1cc59338-esp32s3.pdf [Accessed 23 July 2023].

Kajor, M., Siu, I., Turon, M., Litvin, A., Zbarsky, B., Lunde, G. S., & Smith, M. (2023) Working with the CHIP Tool. Available from: https://github.com/project-chip/connectedhomeip/blob/master/docs/guides/chip_tool_guide.md [Accessed 13 July 2023].

Nordic (2022) nRF Sniffer for Bluetooth LE v4.1.x. Available from: https://infocenter.nordicsemi.com/pdf/nRF_Sniffer_BLE_UG_v4.1.x.pdf [Accessed 17 July 2023].

Patil, S., Litvin, A., Jadhav, R., Zbarsky, B., Chen, S., Qixiang, W. & Wood, J. (2023) Matter ESP32 Lighting Example. Available from: https://github.com/project-chip/connectedhomeip/tree/master/examples/lighting-app/esp32 [Accessed 13 July 2023].

Scapy (N.D.) What is Scapy? Available from: https://scapy.net/ [Accessed 13 July 2023].

Wireshark Foundation (N.D) The world's most popular network protocol analyzer. Available from: https://www.wireshark.org/ [Accessed 31 July 2023].