

## 6. Discussion

Based on the tests carried out, some conclusions can be drawn regarding the security of the Matter communication standard, which are reflected in the following.

### 6.1 Bluetooth sniffing

Tests based on the Bluetooth standard determined that Matter devices do not have static MAC addresses. After switching the Matter device on again, a randomised MAC address was assigned to the device. While the implementation of randomised MAC addresses is stated in the Matter specifications, it is not clear here that this design of the MAC addresses is an explicit security feature (CSA, 2022b). However, it can be assumed that this feature was used for security reasons. The randomisation of the MAC address strengthens some security aspects that can be considered problematic under Bluetooth. A random MAC address makes it difficult for an attacker to commission to a Matter device before the legitimate user. In the case of a static address, this could be carried out in a targeted and automated manner, making it impossible for the legitimate user to integrate the device into the network (Kalantar et al., 2018). Furthermore, the investigation using bettercap did not lead to any recognisable vulnerabilities. By reading the handles, only the name of the device and the discriminator was found out.

The final BLE test of sniffing the exchanged data packets during the commissioning process via Wireshark and the nRF52840 dongle led to inconsistent results. In some implementations of the Matter device's sniffing attack, the complete process of commissioning could be recorded, but in most cases the eavesdropping attack stopped before commissioning was complete. Furthermore, it was not possible to find the exchange of the encryption in any of the tests carried out, so that it was not possible to determine the content of the exchanged packets. Thus, the greatest threat, determining the access data to the Wi-Fi network, could not be confirmed during the tests. However, the possibility of sniffing the commissioning process via Bluetooth does not exclude this threat.

Another interesting observation that could be made during the commissioning of Matter devices is the different security functions that emanate from the hub device. While the iPad as a hub allows the integration of devices not certified by Matter as a risk, the non-certified Matter device was rejected by the Google Nest Hub. This shows that the device developers

are given some freedom with regard to security aspects. Furthermore, this observation shows that in some cases a trade-off between security and usability has to be made. In the case of the iPad, this decision was made in favour of usability, allowing potentially malicious devices to infect the network. The Google Nest Hub, on the other hand, relies on security, which, however, prevents the creation and the use of non-certified Matter devices, thus limiting interoperability.

These two aspects contradict each other to a certain extent by the claims that Matter makes of itself, since on the one hand interoperability has been stated as a central goal of Matter and on the other hand CSA claims that 'Customers buying Matter devices will not have to think about security: it is just there' (CSA, 2022a). These two approaches of prioritising Matter functions by the manufacturers mean that Matter vulnerabilities can be device-specific in the future, which means that, contrary to CSA's claims, users have to be aware of the security of Matter.

## 6.2 De-authentication attack

A summary of the test results of the de-authentication attacks carried out is listed in Table 2.

**Table 2: Compilation of de-authentication attacks results**

<b>Network</b>	<b>Attacked target</b>	<b>Deauthentication attack</b>
Computer - Test AP	Device	successful
Computer - Test AP	AP	successful
Matter device - Matter AP	Device	successful
Matter device - Matter AP	AP	successful
Computer - Matter AP	Device	unsuccessful
Computer - Matter AP	AP	unsuccessful

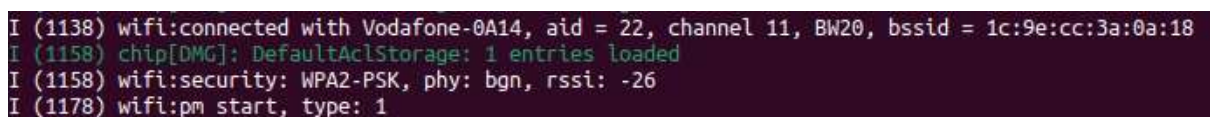
During the tests, it was found that neither the test network, consisting of a smartphone as an AP, nor the Matter network is protected against de-authentication attacks. However, the execution of a de-authentication attack on the computer used in the test network, connected to the AP used for the Matter network, was unsuccessful.

Furthermore, it was determined that when a device was attacked, it lost the connection to the network, but not other devices that were connected to the AP. In the event of an attack on the

AP, all or just some devices in the network were affected, depending on the AP. This finding suggests that the properties of the AP or the device are not the only prerequisites for preventing de-authentication attacks. Rather, it is the compatibility of both participating network components that determines the vulnerability with regard to de-authentication attacks. A search for an explanation of the results obtained in this test leads to the assumption that the IEEE 802.11w supplement to the Wi-Fi standard is the cause of the observed results (IEEE 802 LAN/MAN Standards Committee, 2009).

The IEEE 802.11w standard ensures that management and control information transmitted in an 802.11 WLAN is encrypted (Qureshi & Asghar). This is intended to prevent attackers without a valid key from disrupting communication in the WLAN or from being able to penetrate the network. Encrypted management information, known as Protected Management Frames (PMF), ensures the integrity of network management traffic and increases the WLAN's resilience to attacks. However, to use the security function, both the AP and the WLAN client must support PMF.

In order to encrypt the management frames, it is also necessary for the WLAN environment to support WPA2 (Chen & Punya, 2020). However, it should be noted that only a few Wi-Fi devices under WPA2 have integrated the IEEE 802.11w supplement (Lounis et al., 2021). For the latest WPA3 standard, PMFs are an integral part. The monitoring of an integrated Matter ESP32-S3 controller has shown that the security standard WPA2 is used in the tested Matter network, which can be seen in Figure 24.

A terminal window with a dark background and light-colored text. The text shows system logs for a Wi-Fi connection. The first line indicates a successful connection to a Vodafone network. The second line shows that the chip's default ACL storage has been loaded. The third line specifies the security protocol as WPA2-PSK, the PHY mode as bgn, and the RSSI as -26. The fourth line shows the PM (Protected Management) start type as 1.

```
I (1138) wifi:connected with Vodafone-0A14, aid = 22, channel 11, BW20, bssid = 1c:9e:cc:3a:0a:18
I (1158) chip[DMG]: DefaultAclStorage: 1 entries loaded
I (1158) wifi:security: WPA2-PSK, phy: bgn, rssi: -26
I (1178) wifi:pm start, type: 1
```

**Figure 24: WPA2 encryption of the Matter device**

However, an examination of the Matter specifications showed that Matter does support WPA3 (CSA, 2022c). Research into the security standards of the ESP32-S3 controller used also revealed that the device supports WPA3 as a security feature (Espressif Systems, 2023). It therefore had to be assumed that the router used for the Matter network only has the WPA2 security standard, which could be confirmed by looking at the router settings.

Finally, it was found that Matter is protected against de-authentication attacks within the framework of a WPA3 environment, but this requires that all devices in the network are WPA3 compatible. In the test scenario carried out, however, the AP was only compatible with WPA2, so the security standard was downgraded to WPA2. Under this security standard, the

Matter device was not protected against de-authentication attacks, since the IEEE 802.11w supplement to the Wi-Fi communication standard was not implemented. A search in the Matter specifications did not contain any information on IEEE 802.11w (CSA, 2022c). It can therefore be concluded that under WPA2 Matter devices are not adequately protected against de-authentication attacks. This increases the potential threat of downgrade attacks in which older WPA security standards are specifically exploited (Lamers et al., 2021).

### **6.3 Replay attack**

As part of the intended test of a replay attack on a Matter device, a Python script was created with the scapy tool, which can resend data packets intercepted via Wireshark. In order to be able to confirm the functionality of the script, the message exchange between a client-server structure of two Ubuntu 22.04 TLS computers was intercepted, the content of a UDP packet was manipulated and sent again.

However, the execution of replay attacks on Matter devices with the lighting-app application showed that no vulnerabilities of Matter with regard to replay attacks could be detected in the scenario used. Based on the monitoring of a Matter controller during a replay attack, which can be seen in Figure 23 in Chapter 5.2.2.1, it can be confirmed that the packets resent by the Python script were received by the Matter device. In addition to the observation that the LED was not switched on by these packets, the error message 'OnMessageReceived failed, err = 70' could also be determined. The Matter specification does not provide any information regarding this error message (CSA, 2022c). However, it was possible to find out, that the error message 70 stands for "CHIP\_ERROR\_UNSOLICITED\_MESSAGE\_NO\_ORIGINATOR" (Shripad621git, 2023). This error message occurs when a message was detected that was sent from an unauthorised source or does not conform to session integrity. Since the replay attacks were carried out by the same computer from which the packets recorded for the test were sent, it is likely that the message counter recognised the packets that were sent again as invalid. The message counter is used by Matter to ensure packet integrity and is randomly initialised at the beginning of each session and then incremented with each outgoing message (CSA, 2022c). It can therefore be concluded that the replay attack could be warded off as a result of inconsistency of the session integrity, recognised by the message counter.

With regard to the replay attacks carried out, it should be emphasised that all tests were executed with packets that were recorded directly on the sender's computer. As part of the

experiments, it had to be determined that recording the Wi-Fi communication turned out to be difficult and various approaches to reading out the data traffic via Wireshark failed.

On the one hand, an attempt was made to remotely record the data traffic of the network in which the Wi-Fi dongle tp-link TL-WN722N and BrosTrend AC1200, which are supposed to support the monitor mode required for remotely capturing Wi-Fi packets (WikiDevi, 2021; SecWiki, N.D.). However, it was found that the chipset of the TL-WN722N has changed and the chip that is now in use no longer supports monitor mode. With the BrosTrend AC1200 Wi-Fi adapter, a basic recording of the data traffic of packets could be made, but the packets sent from the client-server structure and between the Matter components could not be found. It must be noted here that wireless acquisition is difficult due to various factors such as physical characteristics of the devices and supported operating system drivers, and if successful, the amount of data easily exceeds the capacities of the hardware and software due to the unfiltered data acquisition (Kismet, N.D.).

Attempts to scan the traffic packets of the Matter network via the iPad used as a hub device also failed. An attempt was made to establish a remote virtual interface between an Apple computer and the iPad in order to record the communication via this connection using Wireshark. However, it had to be determined that the available devices (iPad generation 1-3 and MacBook os El Capitan v. 10.11.16) are not compatible with each other or the versions of the iPad are too old to be compatible with Matter. Furthermore, an attempt was made to create an AP for the Matter network with the operating systems Ubuntu 22.04 TLS and OpenWRT 22.03.5. However, the result was that the iPad could not be connected to the Ubuntu 22.04 TLS as an AP and the commissioning of the Matter device with the hub was not successful under OpenWRT. These results offers the realisation that the acquisition of Wi-Fi data packets using Wireshark is made more difficult due to various factors such as hardware, compatibility of operating systems and interoperability between different versions.

## **6.4 Verification and validation**

With regard to Bluetooth sniffing, it can be stated that the experiments were carried out successfully and that comparable results from Matter and test networks were recorded. However, since the test with bettercap with the iPad as a comparison device led to similar results as with the Matter device, these tests could only determine that this method enables possible vulnerabilities to be spied out in insufficiently implemented BLE devices. Choosing

a device with known vulnerabilities would therefore have led to more meaningful results at this point. Nevertheless, it can be stated that no vulnerabilities of the Matter device could be identified in the course of this experiment.

Furthermore, the Bluetooth package capturing of the commissioning process also led to valuable results, which, however, have deficiencies in terms of consistency. In 10 consecutive tests, the complete process could be recorded in 2 cases and only parts of it in 8 cases. An examination of the last collected packets of the respective tests revealed that there was no recognisable regular place for the termination of the sniffing attack. The last recorded write requests each referred to different handles, so the abort appears random. However, incorrect execution of the tests, for example due to the selection of an incorrect MAC address, can be ruled out because, contrary to the inconsistent completion of the tests, the beginning of each recording took place with the exchange of the same packets and these can be found in every test run. Figure 25 shows the initial exchange of packages during the commissioning process.

3147 4525.7.. Master_0x5065451e	LE IM	LE LL	6 17267µs	0	0	False	0	Control Opcode: LL_VERSION_IND
3148 4525.7.. Slave_0x5065451e	LE IM	LE LL	9 151µs	0	1	True	0	Control Opcode: LL_SLAVE_FEATURE_REQ
3149 4525.7.. Master_0x5065451e	LE IM	LE LL	0 150µs	1	1	False	0	Empty PDU
3150 4525.7.. Slave_0x5065451e	LE IM	LE LL	0 151µs	1	0	False	0	Empty PDU
3151 4525.7.. Master_0x5065451e	LE IM	LE LL	9 21609µs	0	0	False	1	Control Opcode: LL_FEATURE_RSP
3152 4525.7.. Slave_0x5065451e	LE IM	LE LL	6 150µs	0	1	True	1	Control Opcode: LL_VERSION_IND
3153 4525.7.. Master_0x5065451e	LE IM	LE LL	0 151µs	1	1	False	1	Empty PDU
3154 4525.7.. Slave_0x5065451e	LE IM	LE LL	0 150µs	1	0	False	1	Empty PDU
3155 4525.8.. Master_0x5065451e	LE IM	LE LL	3 21609µs	0	0	False	2	Control Opcode: LL_PHY_REQ
3156 4525.8.. Slave_0x5065451e	LE IM	LE LL	0 151µs	0	1	False	2	Empty PDU
3157 4525.8.. Master_0x5065451e	LE IM	LE LL	0 22166µs	1	1	False	3	Empty PDU
3158 4525.8.. Slave_0x5065451e	LE IM	LE LL	3 151µs	1	0	True	3	Control Opcode: LL_PHY_RSP
3159 4525.8.. Master_0x5065451e	LE IM	LE LL	0 150µs	0	0	False	3	Empty PDU
3160 4525.8.. Slave_0x5065451e	LE IM	LE LL	0 151µs	0	1	False	3	Empty PDU
3161 4525.8.. Master_0x5065451e	LE IM	LE LL	5 21704µs	1	1	False	4	Control Opcode: LL_PHY_UPDATE_IND

**Figure 25: Sniffed initial Bluetooth packages**

These results suggests that the different results of the sniffing attacks cannot be explained by channel hopping and the associated randomly recorded sections of the process, since otherwise the first detected packets would not have been recorded in all test runs. However, it can be assumed that the nRF52840 dongle has a significant impact on the test and thus the results. The sniffing device used in the tests is a Bluetooth sniffing dongle, which is located at the lower end of the price segment. Better and therefore more expensive devices have a better quality of packet recording, so it can be assumed that a better sniffing device could have led to more consistent results (Scheible, 2020). It therefore had to be determined that the capturing of Bluetooth packets is not as consistent as assumed.

With regard to de-authentication attacks, it can be stated that verification of the executions can be confirmed. Since each of the test scenarios was performed 10 times and the results were the same according to the devices involved, it can be assumed that the experiments could be carried out consistently and in a target-oriented manner. Due to the reproducibility of the results, sources of interference that lead to the test results are considered unlikely.

A verification of the experiments of the replay attack can also be confirmed. Since the simulation of a replay attack could be carried out successfully, it can be concluded that the created Python script is able to carry out a replay attack. Since these experiments led to the same, consistent results when repeated 10 times, it can be assumed that the possible vulnerability to be tested was successfully investigated and the test design was created appropriately.

A final validation of the results can be carried out with regard to the respective experiments as well as in the context of the overall project question. The results in relation to Bluetooth suggest that Matter has no vulnerabilities. However, it should be noted that this assessment can only be made on the basis of the test results obtained. It is not possible to rule out threats relating to Matter's Bluetooth components based on the experiments. The conclusion must therefore be drawn that a sufficient assessment with regard to the research question regarding Bluetooth cannot be made.

In contrast to this, a clear validation can be carried out in the context of the de-authentication attack. The results indicate that Matter has identified vulnerabilities in the Wi-Fi component relative to older WPA security protocols supported by Matter. It therefore follows that in this context Matter is not able to fix all security problems of Wi-Fi. The test of replay attacks also leads to a clear finding. It can be seen that Matter was actively mitigating threats of replay attacks.

**Table 3: Summary of the test results**

Hacking experiment	Outcome
Bluetooth sniffing	No vulnerabilities found.
De-authentication attack	Attack was under WPA2 successful. Matter does not support 802.11w.
Replay attack	Replay attack was not successful on Matter. Attack was prevented by the Message Counter.

It can thus be summarised that, with regard to some aspects, Matter can contribute to a more secure smart home network, but not all vulnerabilities have been sufficiently taken into account. In view of the research question, it can therefore be finally assessed that Matter is not able to solve all security problems of the communication standards used under Matter. Matter thus does not overcome the security problems of implemented communication standards.

## 6.5 Lessons learned

A variety of devices and tools were used within the project to investigate security aspects. In this way, first experiences with the handling of microcontrollers could be made and learned how they can be built, flashed and utilised as part of a development framework. Furthermore, the in-depth handling of various operating systems such as Ubuntu 22.04 TLS, OpenWRT and macOS was learned, which were only used superficially in the past. Interesting in this context was the experience that the interoperability of different macOS and iOS versions can pose a much bigger problem than initially assumed. The question arises to what extent the lack of interoperability with older devices can be justified with security aspects and what significance the economic interests of the companies have behind this decision.

Regarding Matter, it became clear that the large promises regarding the security of the standard could not be confirmed. No particularly new and outstanding security functions are invented, so it is questionable whether Matter can rule out all risks for smart home networks for users and society. Companies should be aware of this problem and take care about the security of their products independently.

A particularly large increase in knowledge can be found in the context of communication standards, since a theoretical analysis of various standards took place as part of the project and the experiments, but practical tests were also carried out on the Wi-Fi and Bluetooth standards. Through these tests, a reflected understanding of possible threats from attacks could be developed and the vulnerabilities of the corresponding standards were clarified. Thus, the theoretical knowledge about threats based on the Bluetooth standard could be transferred into a practical context, so that application-specific skills could be trained. Furthermore the knowledge could be gained how easy it is to capture the packets of the Bluetooth standard compared to Wi-Fi.

In contrast, the implementation of the Wi-Fi tests was accompanied by some challenges, so that solutions had to be found that promoted personal problem-solving skills. These challenges primarily included capturing Wi-Fi packets and interoperability between devices and Wi-Fi AP. It was interesting to note that capturing packets, especially remotely, is far more complicated than originally expected, but further processing of these packets turned out to be easy. The finding led to the realisation that the primary security of a Wi-Fi network is located in the prevention of intrusion by malicious users.



Competence gains in relation to project planning and time management can also be confirmed, since the project that was carried out was confronted with some challenges, which can be attributed to the relatively new communication standard Matter, but were also due to planning that could be improved.

It should be stated that the planned experiments have exceeded the scope of the project. Due to regulations such as the word limit, it had to be realised that the respective experiments could not be analysed and discussed comprehensively enough. Choosing fewer aspects to be examined would have made it possible to evaluate the results more intensively. For future projects, the realisation was gained that narrower and more focused objectives should be pursued.

## References

- CSA (2022a) Matter Security and Privacy Fundamentals. Available from: [CSA Matter Security WP.docx \(csa-iot.org\)](#) [Accessed 06 April 2023].
- CSA (2022b) Matter Security and Privacy: A Deep Dive with the Experts – Connectivity Standards Alliance. Available from: <https://www.youtube.com/watch?v=Q4jhK-IBKuI> [Accessed 04 April 2023].
- CSA (2022c) Matter Specification Version 1.0. Available from: [https://csa-iot.org/wp-content/uploads/2022/11/22-27349-001\\_Matter-1.0-Core-Specification.pdf](https://csa-iot.org/wp-content/uploads/2022/11/22-27349-001_Matter-1.0-Core-Specification.pdf) [Accessed 25 April 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].
- IEEE 802 LAN/MAN Standards Committee (2009) IEEE Standard for Information technology-Telecommunication and information exchange between systems-Local and metropolitan area networks-Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 1: Radio Resource Measurement of Wireless LANs. Available from: <https://ieeexplore.ieee.org/document/5278657> [Accessed 22 July 2023].
- Kalantar, G., Mohammadi, A. & Sadrieh, S. N. (2018) ‘Analyzing the effect of Bluetooth low energy (BLE) with randomized MAC addresses in IoT applications’, *IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*. Halifax, Canada, 30 July - 03 August. IEEE. 27-34. Available from: <https://ieeexplore.ieee.org/abstract/document/8726525> [Accessed 20 July 2023].
- Kismet (N.D.) Passive Capture. Available from: [https://www.kismetwireless.net/docs/readme/intro/passive\\_capture/](https://www.kismetwireless.net/docs/readme/intro/passive_capture/) [Accessed 24 July 2023].
- Lamers, E., Dijksman, R., van der Vegt, A., Sarode, M. & de Laat, C. (2021) ‘Securing home Wi-Fi with WPA3 personal’, *IEEE 18th Annual Consumer Communications & Networking Conference*. Las Vegas, USA, 09-12 January. IEEE. 1-8. Available from: <https://ieeexplore.ieee.org/abstract/document/9369629> [Accessed 23 July 2023].
- Lounis, K., Ding, S. H. & Zulkernine, M. (2021) ‘Cut It: Deauthentication attacks on protected management frames in WPA2 and WPA3’, in: Aïmeur, E., Laurent, M., Yaïch, R., Dupont, B., Garcia-Alfaro, J. (eds) *Foundations and Practice of Security*. Springer. 235-252. Available from: [https://link.springer.com/chapter/10.1007/978-3-031-08147-7\\_16](https://link.springer.com/chapter/10.1007/978-3-031-08147-7_16) [Accessed 22 July 2023].

Qureshi, I. A. & Asghar, S. (2023) A Systematic Review of the IEEE-802.11 Standard's Enhancements and Limitations. *Wireless Personal Communications* 131: 1-34. Available from: <https://link.springer.com/article/10.1007/s11277-023-10553-7> [Accessed 22 July 2023].

Scheible, T. (2020) Spionage von Bluetooth-Verbindungen. Available from: <https://scheible.it/bluetooth-spionage/> [Access 21 July 2023].

SecWiki (N.D.) Npcap/WiFi adapters. Available from: [https://secwiki.org/w/Npcap/WiFi\\_adapters](https://secwiki.org/w/Npcap/WiFi_adapters) [Accessed 24 July 2023].

Shripad621git (2023) OnMessageReceived failed, err = 70 (CON-571) #468. Available from: <https://github.com/espressif/esp-matter/issues/468> [Accessed 24 July 2023].

WikiDevi (2021) List of Wireless Adapters That Support Monitor Mode and Packet Injection. Available from: [https://deviwiki.com/wiki/List\\_of\\_Wireless\\_Adapters\\_That\\_Support\\_Monitor\\_Mode\\_and\\_Packet\\_Injection](https://deviwiki.com/wiki/List_of_Wireless_Adapters_That_Support_Monitor_Mode_and_Packet_Injection) [Accessed 24 July 2023].