Bluetooth sniffing

Matter's Bluetooth sniffing tests included various tools designed to reveal information about the Matter device.

<u>Hcitool:</u>

First, the tool hcitool was used to probe the MAC addresses that could be found in the area. The commands hcitool scan or hcitool lescan can be used to differentiate between Bluetooth and Bluetooth Low Energy devices (Miller & Estrella, 2018).

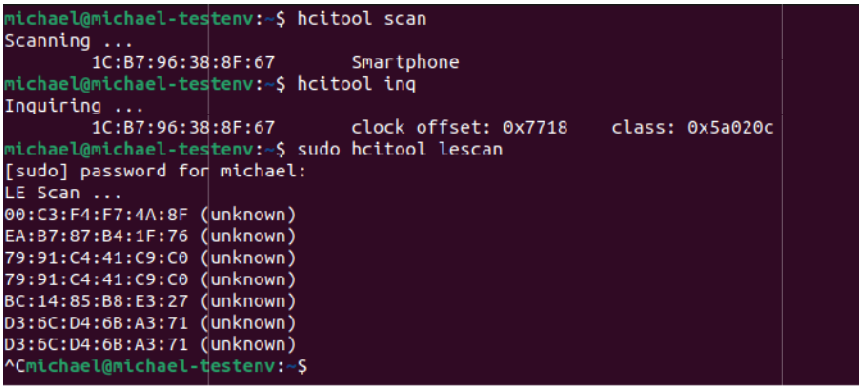

Figure 1: hcitool Bluetooth and BLE device scan

The distinction makes sense because the tools used later do not differentiate between Bluetooth and BLE. The test can also be carried out quickly and easily repeated, so that it was found that the Matter device, when unpaired, is assigned a new randomised MAC address every time it is switched on.

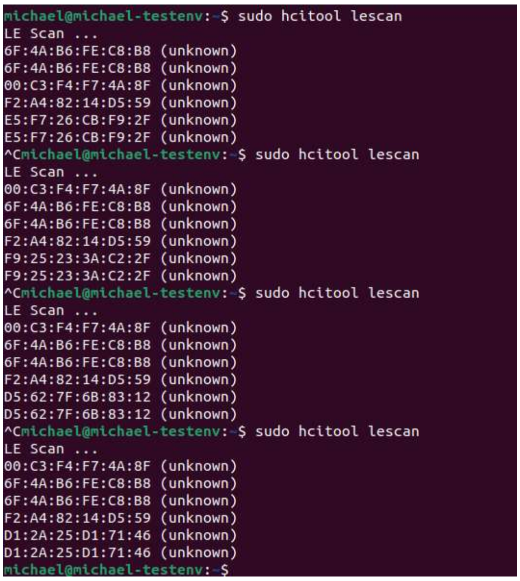

Figure 2: Changing Matter MAC address

Sdptool:

A further examination of Bluetooth devices was carried out using the sdptool, which can determine information about the device and its functions (Krasnyansky, N.D.). For this, however, it is necessary that the MAC address of the device to be examined is known, so that the MAC addresses had to be probed beforehand using the hcitool. The application can be executed using the command ‘sdptool browse [MAC address]’.

An excerpt of the functions found for a smartphone as a test object can be seen in the following figure.

The tool can therefore be used to determine the various functions of the device, with the information from which you can not only gain knowledge about the corresponding device, such as what device it is (e.g. camera, smartphone, smart TV, etc.). This information can also be used to carry out further hacking attacks tailored to the device. It should be noted that during the test it was not possible to examine BLE devices for their functions using this tool.

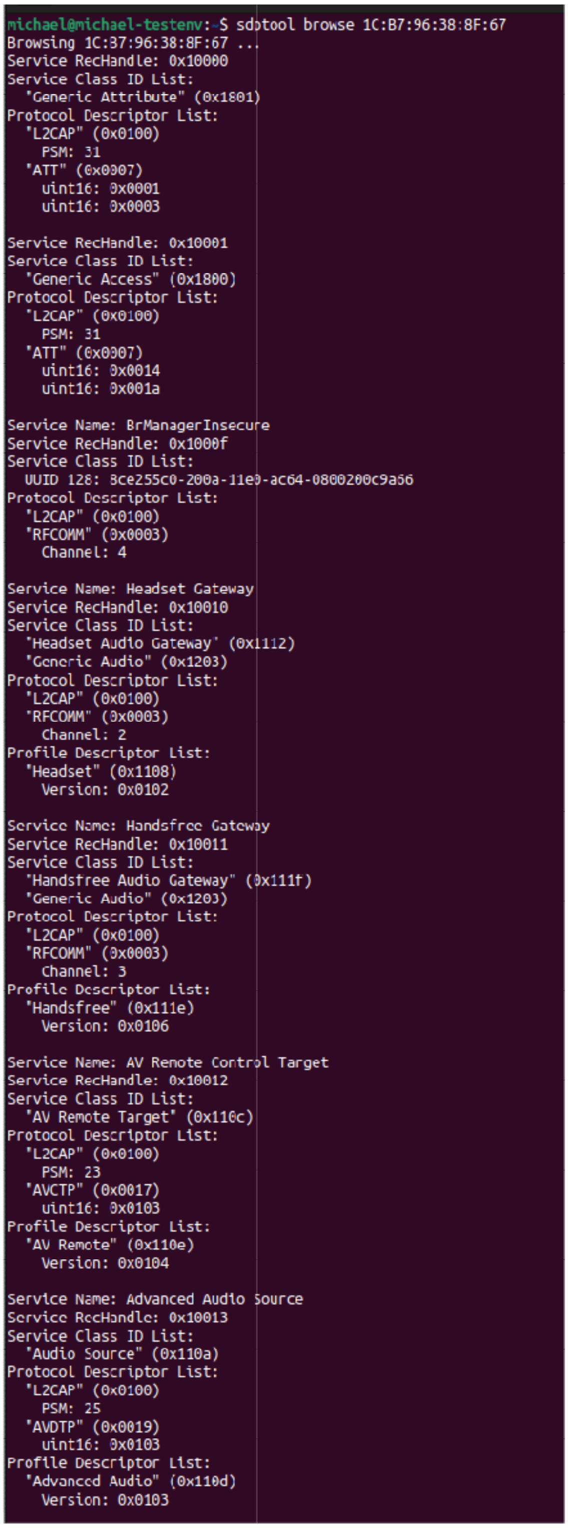

Figure 3: Device information via sdptool (excerpt)

Bettercap

Another approach to determine information and potential vulnerabilities of BLE devices was pursued using the bettercap tool. The tool bettercap offers a variety of functions to sniff Wi-Fi and BLE networks (Margatelli et al., 2021).

As part of the tests carried out with bettercap, it was found that the most stable use of bettercap for BLE sniffing could be achieved with a Docker image. The image was then downloaded from the bettercap website and started with the command 'docker run -it -privileged -net=host bettercap/bettercap'. After bettercap was started, the tool automatically searched for discoverable BLE devices.

Figure 4: iPad sniffing with bettercap

In the upper section of the figure it can be seen that the devices found are listed with the respective MAC address and, if identifiable, also the vendor. In addition, the dBm provides information about how strong the signal is. The signal strength can be used to estimate how far away the device is. However, further investigations into the signal strength have shown that this can only be assessed as an indication of the distance. Some devices inherently have a stronger or weaker signal strength. In addition, it can also be severely affected by sources of interference (electromagnetic devices, walls, water pipes, etc.). Using the 'ble.show' command, the devices found can be displayed in a table, whereby information can also be provided as to whether the respective device is connected to another device and whether it is a end-device (slave) or controller (master).

To get detailed information about a specific device, the command 'ble.enum [MAC]' can be used. The results of this research can be seen in the bottom table of the figure. Handles found, the functions of the device, as well as further information such as characteristics, properties and authorisations and other details are listed here. This is where things get particularly interesting, because possible vulnerabilities and attack vectors can be identified using the information about the handles' permissions. In addition, it can be determined whether a characteristic of the corresponding handle is encrypted or not. Finally, depending on the device, it is also possible to find out exactly which device it is in detail. The test with bettercap using the iPad as the test device revealed that it is such a device and also that it is the 8th or 9th generation of an iPad.

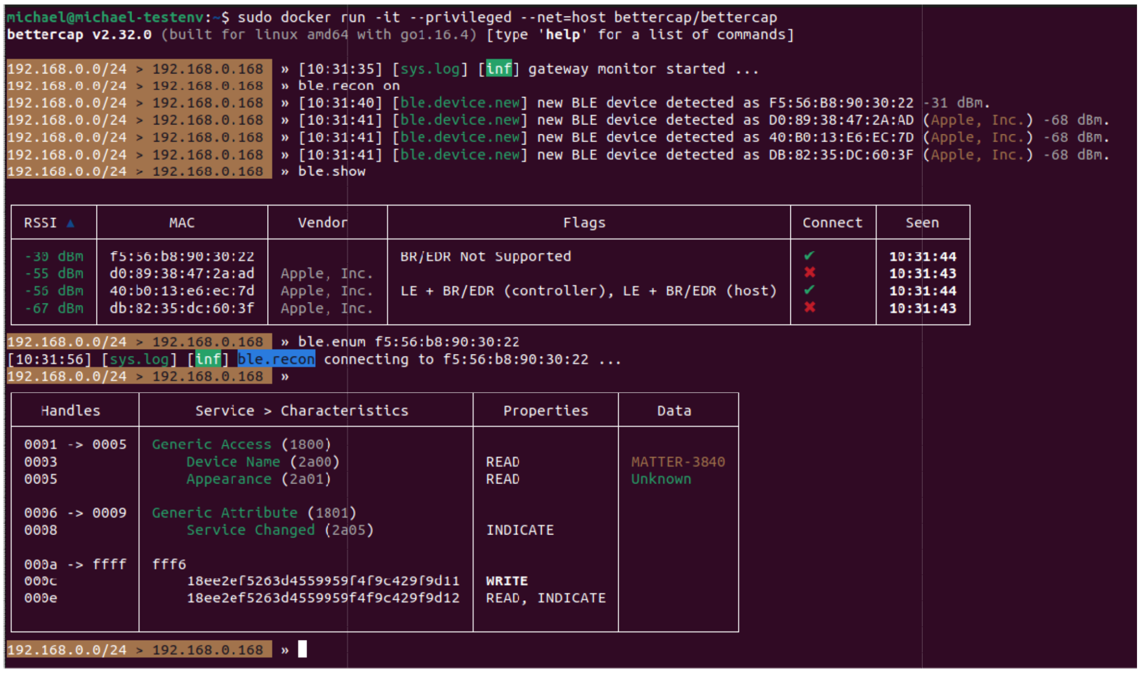

Figure 5: Matter device sniffing with bettercap

A similar test using the Matter device as a target revealed basically the same possible information available. Since the Matter device used is a device that was self flashed using a test application, the information received regarding the device name is rather cryptic. However, it can be clearly stated that the device is a Matter device (see name). Furthermore, the number 3840 can be found behind the name of the device, which is the discriminator of the device, which was assigned to the device during the flash process. While all tests carried out with bettercap did not lead to any detectable vulnerabilities, it can still be noted that possible vulnerabilities can be easily identified with bettercap, so that a responsible and thoughtful implementation of handles/functions of Bluetooth devices is of central importance.

Wireshark:

With Matter devices, the Bluetooth communication standard is used exclusively for commissioning and switches off automatically after the device has been successfully implemented into a Matter network. However, when putting a Matter device into operation, extremely sensitive information such as the access point (router) name and its password is exchanged. Therefore, a final attempt was made to record the packets exchanged when the Matter device was put into operation. The wireshark tool was used for this, which can listen to a variety of other standards in addition to Bluetooth (Wireshark Foundation, N.D.). In order to record Bluetooth packets with Wireshark, a Bluetooth sniffing device is required. As part of the project, the nRF52840 dongle from Nordic was used (Nordic, 2022). After the dongle was flashed with software also provided by Nordic and the necessary addons for Wireshark were added, Bluetooth packets sent in the area could be recorded.

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

Figure 6: Sniffed initial Bluetooth packages

The figure shows the first exchanged packages when putting a Matter device into operation. The respective transmitter (master or slave) can be seen here, as well as the communication standard used for the packets, the time of transmission, the sequence number, the next sequence number to be expected, whether further information is available, the event counter and finally further information about the packets. A complete record of the captured packets when a Matter device is put into operation can be found separately. However, Wireshark or another program that can read .pcap files is required to read them. By selecting individual packages, their contents and other information can be read.

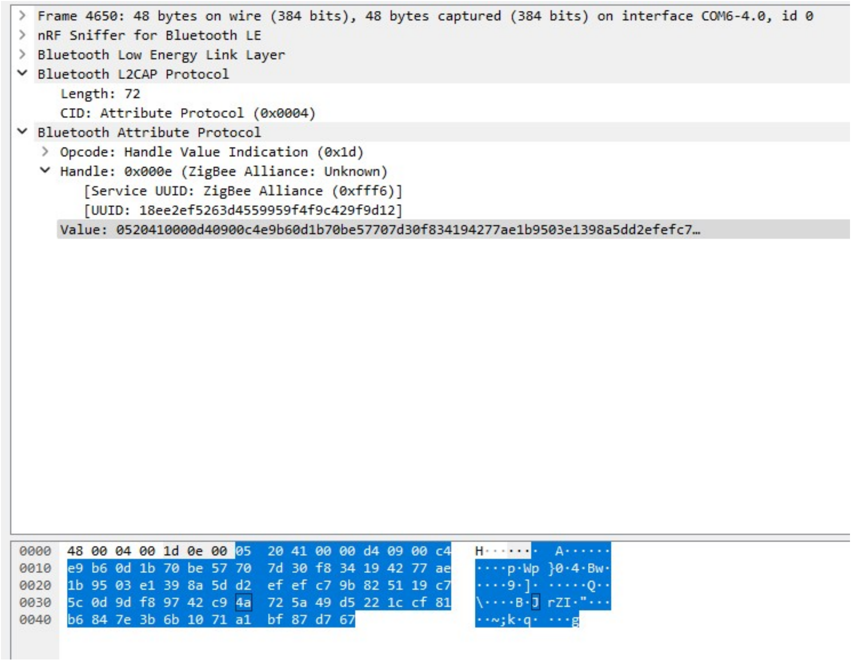

Figure 7: Sniffed Matter commissioning package

These include the packet size, the protocol used and the handle involved. The UUID of the sender and receiver is also specified. Finally, the contents of the package can also be seen. In all packets examined, the content was encrypted, so that the greatest risk of the router's password being captured did not apply. However, the ease with which these packages could be recorded shows how delicate the commissioning process is for Matter devices.

References

Krasnyansky, M. (N.D.) sdptool (1) – Linux man page. Available from: https://linux.die.net/man/1/sdptool [Accessed 14 July 2023].

Margaritelli, S., Braga, G., Trotta, G. & Gruber, K. (2021) bettercap. Available from: https://github.com/bettercap/bettercap [Accessed 14 July 2023].

Miller, A. C. & Estrella, M. (2018) hcitool. Available from: https://github.com/MillerTechnologyPeru/hcitool [Accessed 14 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].

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