De-authentication attack

A de-authentication attack aims to interrupt a client's connection to an AP and therefore falls into the category of a denial of service attack. De-authentication frames are packets based on the IEEE 802.11 (Wi-Fi) standard, which are sent to terminate an existing connection. After the target has received these packets, all further packets from the affected devices are rejected until re-establishing of the connection occurs via a handshake.

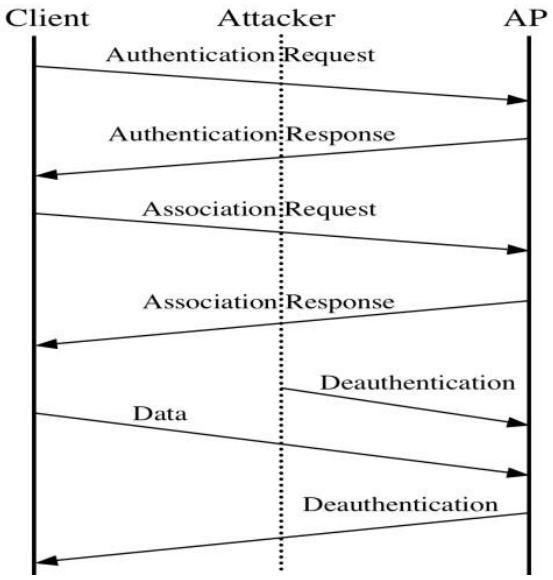

Figure 1: De-authentication attack schematic (Noman, et al., 2015)

In order to carry out the de-authentication attack, a device is required that sends the de-authentication frames. As part of the project, the DSTIKE Deauther MiNi V3 was used. The device can search for possible APs as well as end devices and send targeted de-authentication packets (DSTIKE, N.D.). The device has a built-in screen, so that only a power source, such as a smartphone, is required to operate the device. However, the Deauther can also be connected to a computer via a Wi-Fi connection in order to carry out the attacks. In order to enable better visualisation of the tests, this approach was followed and the video was created to illustrate the test execution of the de-authentication attack. The following refers to the video 'De-authentication-ESP-32-Device'.

On the left you can see a terminal with which the Matter device is monitored. The command 'idf.py monitor' initialises the monitoring and the device is restarted by this command. It will take a moment for the Matter device to boot up and be ready for use.

On the right, the de-authenticator is open in a browser. You can see that after refreshing the page, it displays the access points found and the end devices below. In addition to the signal strength of the AP, the MAC addresses of all devices and, if available, their real names are also displayed.

After the Matter device has fully booted up, it was ensured that it was functional by switching the device on and off several times. This can be seen in the video by the many commands that the device receives, as displayed in the terminal. The green text of the commands confirms that all commands are processed successfully.

Now the Matter device is selected as the target and the de-authentication attack is initialised via the 'Attack' tab. Immediately after the attack begins, the Matter device reports that the connection to the access point is lost. It is stated that a reconnection to the AP will be initialised in 100ms, but since de-authentication frames are continuously received, a connection to the AP cannot be established.

After the de-authentication attack has ended, it only takes a few seconds until the Matter device can reconnect to the AP and commands to the device are successfully processed again. It should be noted that this attack can also be carried out against the AP. As a result, if the attack is successful, all devices lose connection to the AP.

References

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

Noman, H. A., Abdullah, S. M. & Mohammed, H. I. (2015) An automated approach to detect deauthentication and disassociation dos attacks on wireless 802.11 networks. *International Journal of Computer Science Issues* 12(4): 107-112. Available from: https://www.researchgate.net/profile/Haydar-Mohammed/publication/283354063_An_Automated_Approach_to_Detect_Deauthentication_and_Disassociation_Dos_Attacks_on_Wireless_80211_Networks/links/563729f508ae758841151f49/An-Automated-Approach-to-Detect-Deauthentication-and-Disassociation-Dos-Attacks-on-Wireless-80211-Networks.pdf [Accessed 13 June 2023].