1 WPA2-Personal

1.1 Objective

The purpose of this section is to implement a dictionary attack over a WPA2-Personal wifi. To answer most of the following questions, I strongly recommend to use Python cryptography library.

1.2 Preliminaries

File tradio.pcapng is a capture test that contains a WPA2-Personal handshake and some ping packets after handshake for the following wifi session:

- SSID: Wifi_Test
- Password: Wifi_Test_Password

You can identify the 4 handshake messages by applying filter `eapol` in wireshark. Also, you can decrypt traffic (see: https://wiki.wireshark.org/HowToDecrypt802.11).
Question 1. For WPA2_personal, PMK is PSK. Prove that PMK is: `a22c...b603`
Question 2. Parse the capture file with `tshark` and dump the required handshake packets in hexadecimal. From the first handshake message, prove that nonce is `b6ea...d7d3b`. From the second handshake message, prove that nonce is `e6d8...b61c`.
Question 3. Prove that PTK is `0ffc...8aad`.
Question 4. Prove the authenticity of handshake messages 2, 3 and 4.

1.3 Decrypt unicast data

Now is time to decrypt a data packet. You can use packet number 517 which is a `ping request`. Encryption is done using AES128-CCMP.
Question 5. Prove that nonce is: `002269a9e50b3500000000000b`
Question 6. Prove that AAD is: `884184aa9cfd08202269a9e50b3584aa9cfd081f00000000`
Question 7. Prove that decrypted plaintext is: `aaaa...3637`

1.4 Decrypt multicast/broadcast data

In the same capture, there is also multicast/broadcast traffic, such as packet 527, that can not be decrypted with the same key.
Question 8. Obtain GTK and prove that is: `3014...dd00`
Question 9. Prove that nonce is: `0084aa9cfd08200000000008f0`
Question 10. Prove that AAD is: `0842ffffffffffff84aa9cfd082084aa9cfd081f0000`
Question 11. Decrypt packet 527

1.5 Dictionary attack

File tradio2.pcapng contains traffic of a wifi network with SSID: Wifi_Test but password is unknown. We only now that password consists of the SSID concatenated to a number, having 10 possible passwords.
Question 12. Write a dictionary attack based on checking the integrity of message 2 to derive the correct password.

2 WPA2-Enterprise

2.1 Objective

The purpose of this section is to decrypt a WPA2-Enterprise traffic capture assuming that the server RSA private key is known.

2.2 Wifi parameters

File tradio_pap_wpa_enterprise.pcapng is a capture test that contains a WPA2-Enterprise handshake for the following wifi session:

- SSID: TIC_Project
- Server private key file: server.p12 (password: whatever)
- 802.1X authentication: TTLS (TLS-v1.2)
- EAP inner authentication protocol: PAP

2.3 TTLS phase

Your first objective is to get the **premaster** key from the TLS handshake. In this phase, observe that some TLS packets (`Client_Key_Exchange`, `Server_Hello`,...) may be grouped into a unique TCP packet. So, you must disassemble them, once parsed and extracted with `tshark`.

Question 1. Decipher premaster key and prove that is: `0303...fd89b0ab` (48 bytes)

Question 2. Prove that Master Key is: `a5a6...b4a6`

2.4 Decryption of the inner authentication phase

Derive the Key Block

Question 3. Prove that Client Write Key (first 32 bytes of Key Block) is: `16de...dda6`

The PAP authentication phase consists of a single EAP message that can be filtered with tshark options: `tls.record.content_type==23`. In our capture that message is number 119. It can be decrypted using a AES256-GCM-SHA384 algorithm.

Question 4. Decrypt message 119. Which are the login and password credentials?

2.5 The 4-way handshake

The authentication process of the subsequent 4-way handshake messages is done as in WPA2-Personal, but PTK is derived differently.

Question 5. Prove that MSK is: `85e8...6e3b` (48 bytes) and PTK is: `b3c6...8ae4` (48 bytes)

Question 6. Prove the authenticity of handshake messages 2, 3 and 4.

2.6 Decrypt data

Consider data packet number 131. It is ciphered using AES-128-CCMP.

Question 7. Decrypt it. What kind of packet is it?