Homework lecture 6
WiFi security

Harald Vranken
harald.vranken@ou.nl
March 16, 2020

Question 1
Is WPA (as well as WPA2 and WPA3) Personal vulnerable to an evil twin attack?

Answer
In an evil twin attack, an attacker sets up a rogue access point using the SSID of a preferred network of the user. This can be done in all cases, independently whether WEP/WPA/WPA2/WPA3 is used. The more interesting question is what the attacker could do next, after the client has connected to the rogue access point. In case of Personal, the authentication relies on a pre-shared secret (either a password or a key) between client and access point. Since the rogue access point does not have this, the attack stops there. However, an attacker could set up a phishing attack, for instance such that the client enters a captive portal after connecting to the rogue access point in which the client is asked to type the shared secret. An unaware client could be tricked into actually typing the secret.

Question 2
How can an attacker obtain PSK and PTK in WPA(2) Personal?
(See slide 18 of the lecture.)

Answer
The attacker can eavesdrop upon the 4-way handshake and learn ANonce and SNonce (plaintext) as well as the MIC associated with SNonce, and the MAC-addresses of the supplicant (S) and authenticator (A). Since PTK is obtained from a pseudo-random function with PSK, ANonce, SNonce, and the MAC addresses of A and S as inputs, and since PSK is generated using a key derivation function with the password and SSID (known by attacker) as inputs, the attacker can learn PSK by a brute-force, dictionary, or rainbow-table attack. Part of PTK (KCK) is used to generate the MIC. By trying a password and using the according KCK to generate a MIC, this MIC should match the observed MIC in case of a successful attack.
(*See the following paper for a demo of this attack:*
Vulnerabilities of Wireless Security protocols (WEP and WPA2),
Vishal Kumkar, Akhil Tiwari, Pawan Tiwari, Ashish Gupta, and Seema Shrawne,
International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), 1(2): 34-38, April 2012.)

Question 3
Let's assume that eduroam is configured correctly, using IEEE 802.1x authentication with EAPOL, PEAP, and MS-CHAPv2. What steps would an attacker have to take in order to learn your username and password?

Answer

First, the attacker has to be able to decrypt the TLS-protected network traffic. This is nearly impossible if strong encryption is applied.
Second, the attacker has to be able to crack MS-CHAPv2. This is possibly by exploiting weaknesses in the cryptography applied in MS-CHAPv2, eg. by using the tool ChapCrack (see https://www.ncsc.nl/dienstverlening/response-op-dreigingen-en-incidenten/beveiligingsadviezen/NCSC-2012-0499+1.00+Kwetsbaarheid+in+MS-CHAPv2+wachtwoorduitwisseling.html).