Network Security (ROL) - Exam: June 2024

EXAM - General instructions

1. The first page of the exam file must contain your name, group, and a list of unsolved exercises (e.g.,: *Unsolved exercises: 1(a), 1(c), 3(b).* or -).
2. Partial scores are awarded. For wrong answers at the written exam you will NOT be subtracted any extra points.
3. To pass the exam, **it is mandatory to obtain minimum 22.5 points in the final exam and minimum 45 points as the final grade**.

Good luck!

EXAM - Exercises

1. **True of False**

   Respond with true or false. If the claim is false, make it true by enforcing a minimal change (keep the same context, but do not simply negate).

   Example: RC4 is used as a building block in CCMP.
   Expected answer: False. AES is used as a building block in CCMP.

   (a) A Sequence Number (SEQ) normally offers integrity protection. **(2p)**

   (b) In general, it is easier to mount an eavesdropping attack in a wireless network rather than in a wired network. **(2p)**

   (c) WPA Enterprise performs authentication using a single password for all the devices in a network. **(2p)**

   (d) The NAS security context is established between the UE and the NodeB. **(2p)**

   (e) SUCI is the concealed form of the SUPI. **(2p)**

   (f) AI/ML threats become an important security concern in 6G. **(2p)**

   (g) The consensus protocol in Bitcoin assumes that all nodes have to agree to publish a block. **(2p)**

   (h) Cryptographically Generated Address (CGA) are IPv6 addresses. **(2p)**

   (i) Identifiable Random MAC (IRM) addresses aim to prevent the identification of the station by all parties.**(2p)**

   (j) The handshake protocol in TLS always uses ECDH to setup the cryptographic keys. **(2p)**

2. **WPA2 Keys**

   In WPA2 CCMP, the Pairwise Transient Key (PTK) is derived from the Pairwise Master Key (PMK) as

   $$PTK = f(PMK, NonceA, NonceB, AddressA, AddressB),$$

   where $NonceA$ and $NonceB$ are two nonces chosen by the communication parties A and B.

(a) Explain what do *AddressA* and *AddressB* refer to. **(5p)**

(b) Explicitly mention one security property f must have. **(5p)**

(c) Let PTK = A303D7FFD553F2967CE6EA3B00D0EEF3 453226B6FCCDC5DD96DF79910B667C0F DAB235449468A8F9D7D8DC3BE64F08A6. What is the value of the key used in CCMP? **(5p)**

(d) Give one strong reason for which deriving PTK from PMK is favourable (instead of, for example, using PMK directly). **(5p)**

3. **Authentication similitudes in Bluetooth and Mobile Networks**

Reason about similtudes in the authentication procedure in Bluetooth and Mobile networks, more precisely **Bluetooth Classic Secure Authentication** and **EPS AKA**, respectively. For this, refer to Figures 1 and 2.

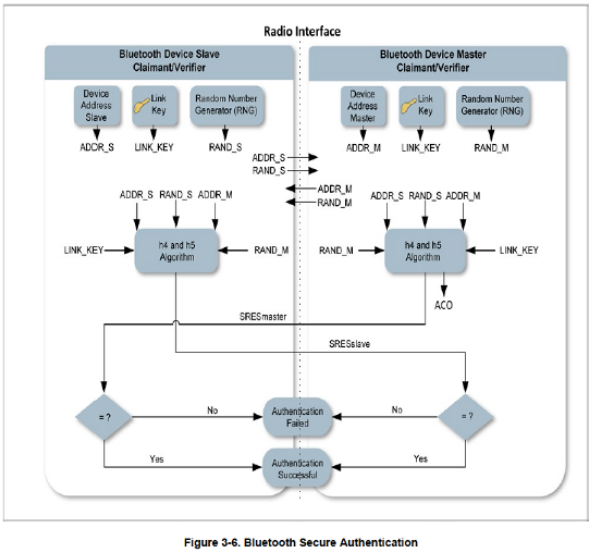

Figure 1: Bluetooth Classic Secure Auth [1]

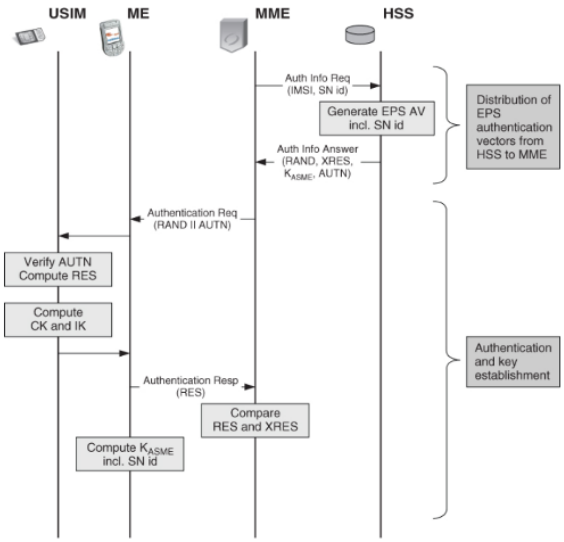

Figure 2: EPS AKA [2]

(a) Both procedures use a challenge-response mechanism. Name the challenge values in each procedure (refer to the names as they appear in the figures). **(5p)**

(b) Explicitly name one type of attack the challenge-response mechanism mitigates/stand against and explain why is this (max.1 paragraph). **(5p)**

(c) Both procedures make use of a secret key shared between the two corresponding parties. Name the two keys, one for each of the two procedures. **(5p)**

(d) State if both procedures accept mutual authentication. Briefly motivate your answer (max.1 paragraph). **(5p)**

[1] Padgette, J., Bahr, J., Batra, M., Holtmann, M., Smithbey, R., Chen, L., Scarfone, K. (2022). Guide to Bluetooth Security (No. NIST Special Publication (SP) 800-121 Rev. 2). National Institute of Standards and Technology.

[2] Forsberg, D., Horn, G., Moeller, W. D., Niemi, V. (2012). LTE security. John Wiley and Sons.

TOTAL available: 60p