[redacted]

21.01.2022

410

Exam

Unsolved:

1) a) TRUE
b) TRUE
c) FALSE: We have to use the transmitter address, the receiver address, the plaintext and the MIC Key.
d) FALSE: The CCMP, CTR mode is used for data confidentiality.
e) TRUE
f) FALSE: K_{eNB} should only be used for the derivation of keys (3 others → K_{RRCint} for integrity ~~confidentiality~~ for signalling plane
→ K_{RRCenc} for encryption
→ K_{UPenc} " — " " — " of UP traffic
g) TRUE
h) FALSE: The home network makes the final decision.
i) TRUE
j) FALSE: SUCI (Subscription Concealed Identifier) is obtained from the encryption of SUPI.

2) a) WPA2-E (Enterprise) is better than WPA2-P (Personal) from a security point of view. First of all, as the name suggests, it's better equipped to deal with the requirements of a bussiness.
- In WPA2-P, we have 1 password for all users and devices, making it very unsafe. If one equippment is compromised, then all are and everyone can access the password. (If you want to change the password, then you must change it for all devices). Now, imagine we have a company and one employee leaves or is fired. That employee knows the password and is now a threat (not to mention we might have at any point a switch in the company) so we must change the password ⇒ TROUBLESOME.
- In WPA2-E, each user gets a unique login credential (so if an employee leaves, we only need to delete his credentials). Also users can't eavesdrop on other's sessions (each user session is encrypted with a different key).

b) - Message 1 (AP → Device): This is not encrypted. It contains ANonce. Tampering with the value will result in handshake failure
- Mess. 2 (Devices → AP): Not encrypted because the SNonce is sent and needs to be extracted, but it includes MIC to prevent tampering.
- Mess 3 (AP → Device): Also includes MIC check in order to verify that the AP has a matching PTK. for the device
Also unencrypted. AP does not yet install the temporal keys, until mess. 4 in case of failure (it needs to resend 3).
- Mess. 4 (DEVICE – AP): Also unencrypted (OK → start encryption)

c) WPA → TKIP (RC4 → stream cipher)
WPA2 → CCMP (AES → block cipher)
For example, in TKIP Group Key Hierarchy we have 256 bits ~~GTK~~ GTK vs. 128 bits GTK for AES (stream vs. block).

d) Wi-fi Enhanced is a new security standard for public networks based on OWE (opportunistic wireless encryption). It provides unauthenticated data encryption to users:
- it doesn't require password on free Wi-fi from cafes (for ex.)
- provides data and management frame protection for end users
- simplicity of deployment because there are no network credentials to maintain or share.

3) a) We need both of them for the calculation of Master Key and in order to prevent replay attacks. If 2 systems (A, B) run the protocol and B proves its identity with "x", then we must change "x" constantly so that the attacker C can't impersonate B. So "x" must be used only onced. A must be sure that "x" is a new value, so now A must chose a value. Also, this is a symmetrical situation, so we need both nonces for verification.

b) Principle of minimal trust: Authentication and trust are ensured only between 2 entities and only after multiple stages using certificates, key exchanges, hash functions...

c) Client sends "Hello$_C$", N_C and the list of suggested cipher suits.

Server sends "Hello$_S$", N_B, certificate$_{PK}$ and requests client's certificate.

Client responds with certificate (lets the server know that it owns the certificate) and the session key information (encrypted with PK). Also sends message to activate the negociated options for future messages.

Server sends mess. to activate "——" "——".

d) It hides the real length of the message being sent, by allowing extra padding.