TTM4137 2014 Exam Solution Outline

19:12:14, 19.12.2014

Stig F. Mjølsnes

Part I. Wireless Security Facts

1a, 2b, 3a, 4b, 5d, 6c, 7c, 8c, 9a, 10a, 11c, 12b, 13d, 14a, 15d, 16a **or** 16b, 17a, 18d, 19a, 20c, 21a, 22b, 23b, 24d, 25c.

Part II. WLAN Security

26. See Real 802.11 Security, Figure 8.5 page 127. The three roles Supplicant—Authenticator—Authentication Server. The Supplicant makes the access request, the Authenticator performs the access control assisted by the Authentication Server, which authorize the access according to its security policy. The notion of access is in the form of a switch on each physical port at the Authenticator.
27. STAs communicates through one AP in infrastructure mode. For 802.1X, STAs take on the role of Supplicants, the AP takes on the role of Authenticator. The Authentication Server role is either integrated into the AP, or available to the AP by the backbone Distribution System. The physical connection STAs to AP are many-to-one, so the AP must implement the Authenticator ports logically to enforce one STA to one logical port. Moreover, the radio link messages must be bound to the logical port by authentication codes.
28. RADIUS is short for *Remote Authentication Dial-In User Service*. RADIUS specifies both a service functionality and a protocol to access this functionality. A part of the RADIUS functionality is the Authentication Server role.
29. See slide 12 of lecture 6.

1. STA → MiM →AS: Authentication
2. AP → AS: Open port
3. STA → MiM: Disassociate
4. MiM → AP: Network access

30. Authenticity, Replay-protected, Confidentiality, Availability.
31. a) STA and AP use the PMK, whereas the AS generates and transports the PMK to the Authenticator. b) 6.
32. A nonce is a variable that is not assigned the same value twice or more.
33. See Figure 6 in the lab description, or slide 18 in lecture note 6.
34. The PTK 384 bits constitute three 128 bits keys:
1. EAPOLMICKey used for message integrity in the 4-way handshake
2. EAPOLEncrKey used for confidentiality of the GTK
3. DataEncr/MICKey used for confidentiality, integrity and replay-protection by the CCMP
35. Each AP will generate its GMK and derive GTKs from this. The AP distributes a GTK to its set of STAs by the group key handshake protocol, where the GTK is encrypted using the EAPOLEncrKey.

Part III. Wireless Ad-Hoc Network

The problem is open, as stated in the text. Here is a sketch of one possible solution:
36. An initiator STA will take on the role of Authenticator, whereas the responder STA will take on the role of Supplicant, then it is possible to carry out a key exchange protocol very similar to the 4-way handshake protocol used in infrastructure mode. It is very important to observe that neither party can base the AKA on identities or MACaddresses because no access control list will exist ad-hoc. The only basis we have is the knowledge of the shared password. One illustration can be Figure 13.2 page 287 in Real 802.11 Security book.
37. Both parties will be able to derive a PTK from the shared password by using an adapted 4-way handshake protocol. The Initiator STA will start out with message 1 including its nonce. The Responder STA is now able to compute a PTK derived from the password, the received nonce, and its locally generated nonce. And so on. The 4-way handshake will verify mutually the knowledge of the password and establishes a shared PTK that can be used to protect the data by using CCMP encapsulation. The security claims for these one-to-one channels will be message authenticity, replay-protection, and confidentiality. Each STA will have to establish distinct security association with each of the other STAs in the IBSS. Each STA will generate and distribute its own group key for multicasting, hence there will be three GTK in our IBSS.

—