English

Norwegian University of Science and Technology
Department of Telematics

EXAM IN
TTM4137 – WIRELESS SECURITY

Contact persons: Stig F. Mjølsnes/Håkon Jacobsen. (Tel. 918 97 772)

Date of exam: December 11, 2014.

Time of exam: 9:00 – 13:00 (4 hours).

Date of grade assignment: January 12, 2014.

Credits: 7.5

Permitted aids: Approved calculator. No printed text or handwritten notes permitted. (D).

Attachments:

- 6 pages of questions
- 1 answer page for Part I

The 37 exam questions and problems are divided into three parts, where each part is assigned an evaluation weight percentage of the total. The sequence of questions is probably, but not necessarily in your order of difficulty, so time your work and make sure you find time for all questions. Try to make succinct answers. Your best effort in making a comprehensible handwriting will be much appreciated.

Part I. Wireless Security Facts (50%)

This part consists of 25 multiple choice questions. The assessment weight is equally distributed over all the questions in this part. Each question offers four possible answers, but only one is correct. Marking the correct answer results in 2 points, whereas double, wrong or missing mark result in zero. *Please use the attached sheet for marking your answers to this Part I.*

1. What is the length of the WEP initialization vector (IV)?
   a) 24 bits
   b) 32 bits
   c) 48 bits
   d) 64 bits
2. What is the main trick of the Beck & Tews chopchop-like attack on TKIP?
   a) An attacker can avoid the re-keying interval of the MIC failure report frame
   b) An attacker can get responses to packets sent with partly guessed content
   c) An attacker can cause packets to be silently dropped
   d) An attacker can decrypt the special packets received over QoS channels
3. What are the fields of the 128-bit start value for RSN CCMP encryption?
   a) 8-bit flag, 104-bit nonce, and a 16-bit counter; where the nonce field contains an 8-bit priority value, the 48-bit source address, and the 48-bit packet number
   b) 16-bit flag, 104-bit nonce, and a 8-bit counter; where the nonce field contains an 8-bit priority value, the 48-bit source address, and the 48-bit packet number
   c) The 16-bit packet number, and a 112-bit nonce value from a sequence counter
   d) 128-bit random nonce value
4. What is Extensible Authentication Protocol (EAP)?
   a) EAP is a set of encapsulation messages for mutual authentication methods
   b) EAP is a set of encapsulation messages for upper-layer authentication methods
   c) EAP is a set of encapsulation messages for RSN authentication methods
   d) EAP is a set of encapsulation messages for RADIUS server authentication methods
5. What are the inputs of the GSM authentication function A3?
   a) K_i and $RAND$ and $XRES$
   b) $RAND$ and $XRES$
   c) K_i and $XRES$
   d) K_i and $RAND$
6. What is the purpose of the sequence number (SQN) used in UMTS?
   a) Preventing man-in-the-middle attacks
   b) Preventing session hijacking
   c) Preventing replay attacks

d) Enabling re-synchronization

7. Is mutual authentication provided when a GSM SIM is used to access a UTRAN?
   a) Yes, between the MS and the RNC
   b) Yes, between the MS and the core network, but not the RNC
   c) No, the GSM SIM cannot authenticate the base station
   d) No, the GSM SIM cannot connect to a UTRAN
8. What is the content and use of the UMTS AUTS parameter?
   a) $SQN \oplus AK$, *MAC-S*. Resynchronization when the SQN check fails on the network side
   b) $SQN \oplus CK$, *MAC-S*. Resynchronization when the SQN check fails on the network side
   c) $SQN \oplus AK$, *MAC-S*. Resynchronization when the SQN check fails on the MS side
   d) $SQN \oplus CK$, *MAC-S*. Resynchronization when the SQN check fails on the MS side
9. How is forward key separation achieved during handovers over X2 connections in EPS?
   a) The target eNB receives a fresh key from MME immediately after handover
   b) The target eNB receives a fresh key from MME right before handover
   c) The source eNB sends a derived key to the target eNB by applying a one-way function to the current key
   d) Forward key separation cannot be achieved, only backward key separation
10. What is the specified length of the permanent subscriber key K in EPS/LTE?
    a) No standard length specified
    b) 128 bits
    c) 192 bits
    d) 256 bits
11. The end points of user data encryption in EPS are
    a) The UICC and the eNB
    b) The UE and the MME
    c) The UE and the eNB
    d) The UICC and the MME
12. The end points of signalling encryption in the EPS access stratum are
    a) The UICC and the eNB
    b) The UE and the eNB
    c) The eNB and the MME
    d) The UE and the MME
13. The end points of signalling integrity in the EPS non-stratum access are
    a) The UICC and the eNB
    b) The UE and the eNB

c) The eNB and the MME

d) The UE and the MME

14. Does EPS provide end-to-end data security?

a) No

b) Yes, but only authenticity

c) Yes, but only anonymity

d) Yes both confidentiality and authenticity

15. What is the telecom practice of lawful interception?

a) Dragnet surveillance secretly performed by an authorized intelligence agency

b) Legal deep packet inspection and filtering of mobile systems traffic

c) Eavesdropping of private communication performed by the police

d) Wiretapping of private communication requested by a law enforcement agency

16. Can UMTS USIMs work in an LTE UE device?

a) Yes, because the key hierarchy is designed for this

b) Yes, because the cryptographic keys are the same

c) No, because the cryptographic keys must remain in the USIM

d) No, because the LSIM and USIM are not compatible

17. Where does the key derivation function KDF of EPS reside?

a) In the UICC and the HSS

b) In the UICC and the UE

c) In the UE and the MME

d) In the UE and the AuC

18. What are the three functional requirements for UMTS authentication?

a) Confidentiality and privacy for the subscriber, and mutual authentication for the service provider

b) AV generation at AuC, key transport to the RNC, and the SQN synchronization

c) Mutual authentication between USIM and HSS, securing the radio channel communication, and end-to-end confidentiality

d) Mutual authentication between USIM and AuC, securing the radio channel communication, and user identity confidentiality

19. Why can the UICC be physically separated from the rest of the UE device?

a) The UE manufacturing and lifecycle can be managed independently from the personalization and subscription process

b) The UICC holds an expiration date and, like credit cards, must be replaced

c) The failure rate of the integrated circuit cards (UICCs) are high because the issuers (mobile operators) want to optimize cost against subscription duration

d) The manufacturer plugs a special key-card into the UICC interface slot for key distribution and software management

20. What is the difference between a checksum code and a cryptographic message authentication code?

    a) There is no difference, they are only different terms for the same primitive
    b) A message authentication code can be used to construct a checksum code, but not the other way around
    c) A checksum can be (re-)computed by an attacker, the authentication code cannot
    d) A keyed checksum provides stronger message integrity protection than a message authentication code

21. What cipher mode of operation is specified in the Bluetooth Low Energy standard?

    a) CCMP
    b) CBC
    c) E0
    d) BLE

22. What is ciphertext padding?

    a) Methods of adding false bits to a ciphertext packet
    b) Methods of making fixed length ciphertext packets
    c) Methods of cryptanalysis using weak crypto-keys
    d) Methods of cryptanalysis using paper pads

23. Are the GPS satellite signals protected cryptographically?

    a) No protection because GPS receivers are keyless
    b) Partly, the military spread-spectrum code is encrypted
    c) By the distinct satellite signal authentication codes
    d) By a public key satellite identity authentication code

24. Which attack is prevented if an RFID tag can authenticate the reader?

    a) Tracking of the tag locations
    b) Tag blocking
    c) Tag inventory registration
    d) Illicit reading of the tag information

25. What is an RFID tree-walking singulation protocol?

    a) A privacy-preserving identification protocol where a tag releases its identity number bit by bit
    b) A disruption protocol by a blocker tag simulating a range of identities
    c) A reader initiated anti-collision protocol run when multiple tags respond simultaneously
    d) A reader monitoring protocol for discovering a given tag identity

Part II. WLAN Security (40%)

26. What are the IEEE 802.1X authentication and access control concepts and roles? Describe by using a diagram. (4%)

27. Interpret and map the concepts and roles described in question 26 onto a wireless 802.11 infrastructure mode network. Make a diagram of an infrastructure with two BSS in one ESS, where each BSS contains three STAs. (3%)

28. What is a RADIUS server? (3%)

29. Let TWIG be the network structure described in question 27. List the stages of a possible wireless man-in-the-middle attack on TWIG, even if a RADIUS server is used, but where the wireless channels are run without any cryptographic protection. (3%)

30. List and explain which security properties an 802.11 wireless channel should have. (3%)

31. Let TWIG use RSN with its cryptographic key hierarchy, where a pairwise master key (PMK) is either derived from a master session key (MSK), or a cached PMK from a previous session, or simply a pre-shared key (PSK).

    a) Which entities of TWIG use a PMK? (2%)

    b) How many PMK instances are there in TWIG? (2%)

32. Security protocols use nonce values.

    a) Define what nonce values are? (2%)

    b) List four different practical mechanisms for nonce value generation. (2%)

33. The 4-way handshake subprotocol of the 802.11 security association protocol inputs a PMK and outputs a pairwise transient key (PTK). Draw a message sequence diagram of the 4-way handshake including the roles, the essential computations at the roles, and the protocol messages with variables. Then describe the 4-way handshake protocol by explaining the purpose and consequence of each message. (8%)

34. A PTK is 384 bits long in RSN. What are the uses of these PTK bits? (4%)

35. Multicast messages in TWIG can be secured by the RSN group key hierarchy of group master keys (GMK) and group temporal keys (GMTK). Explain how this works? (4%)

Part III. Wireless Ad-Hoc Network (10%)

An 802.11 based network in ad-hoc mode does not include an access point nor other coordinating infrastructure. All ad-hoc stations (STA) have equal rank, and no trusted third party is available.

We shall limit the possible STA-to-STA associations to those within direct radio-link range. Moreover, we assume a multiparty SSID beacon protocol is in operation. Therefore each STA in the independent basic service set (IBSS) will be able to discover, send messages directly to, and receive messages directly from, the other STAs in the set. For concreteness, let there be three STAs in our IBSS.

All this means that each STA must enforce its own authentication, key management, access control, and security policy. Assume that a secret password can be shared somehow and input to each STA, which then becomes the starting point for setting up a pre-shared key among the STAs, and then establish the security associations.

36. Try to find a useful mapping of the principles and roles of 802.1X onto this ad-hoc structure. Include an illustrative diagram in your description. (5%)

37. Construct and describe an authentication and key agreement protocol (AKA) suitable for the ad-hoc wireless network setting described, which can establish a security association between an initiator STA and a responder STA. You will decide the security association properties. (5%)

Hint: The intention here is to adapt or use parts of the security mechanisms and protocols that you already know from the 802.11 infrastructure mode, and you are free to apply other mechanisms too.

sfm