English

Norwegian University of Science and Technology
Department of Telematics

EXAM IN
TTM4137 – WIRELESS SECURITY

Contact person: Professor Stig F. Mjølsnes. (Tel. 413 05 114).

Date of exam: December 3, 2010.

Time of exam: 9:00 – 13:00 (4 hours).

Date of grade assignment: January 4, 2011.

Credits: 7.5

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

Attachments:

- 8 pages of questions,
- 1 page for multiple choice answers 1-25,
- 1 page for answer to 26.

The 38 exam questions and problems are divided into three parts, where each part is assigned an evaluation weight percentage of the total. I hope you will find Part II and III enlightening and maybe even entertaining as you work through these. 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. A comprehensible handwriting will be much appreciated. Good luck!

Part I. Wireless Networks 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 gives 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. Is the same key used for both authentication and encryption in WEP?

   a) Yes, if 802.1X authentication is not used

   b) The same key is never used twice

   c) No

   d) Yes

2. What is the major weakness in WEP, exploited by the PTW attack used in the lab?

   a) Too short IV

   b) No protection against message replay

   c) The integrity check value

   d) The IV is part of key stream

3. What is EAP

   a) Extensible Authentication Protocol is a set of encapsulation messages for mutual authentication methods

   b) Extensible Authentication Protocol is a set of encapsulation messages for smartcard-based authentication methods

   c) Extensible Authentication Protocol is a set of encapsulation messages for upper-layer authentication methods

   d) Extensible Authentication Protocol is a set of authentication server methods

4. How are EAP messages transported between the authenticator and the authentication server in RSN?

   a) EAP messages are encapsulated in TCP/IP

   b) EAP messages are encapsulated in EAP-TLS

   c) EAP messages are encapsulated in VPN

   d) EAP messages are encapsulated in 802.1x

5. Which security method is used in the first phase of PEAP?

   a) TLS

   b) EAPOL

   c) 802.1x

   d) LEAP

6. The Pairwise Transient Key (PTK) is a collection of several keys. List these keys and their length when CCMP is used.

   a) EAPOL MIC Key (128), EAPOL Encr Key (128), Data Encr Key (128), Data MIC Key (128)

   b) EAPOL MIC Key (128), EAPOL Encr Key (128), Data Encr/MIC Key (128)

   c) EAPOL MIC Key (128), EAPOL Encr Key (256), Data Encr Key (128), Data MIC Key (128)

   d) EAPOL MIC Key (128), EAPOL Encr Key (128), Data Encr/MIC Key (256)

7. What is *Michael* in WPA/RSN?

   a) The encryption algorithm in TKIP

   b) The key mixing algorithm of RC4

   c) The message integrity code of TKIP

   d) The replay protection algorithm of TKIP

8. What is the purpose of the EAPOL 4-way handshake?

   a) To compute a fresh pairwise temporal key (PTK) from the pairwise master key (PMK)

   b) To compute a fresh pairwise master key (PMK) from the pairwise transient key (PTK)

   c) To compute a fresh pairwise transient key (PTK) from the pairwise master key (PMK) after both parties have verified the PMK

   d) To compute a fresh pairwise message key (PMK) from the pairwise trusted key (PTK) generated in the 4-way key agreement

9. How does the counter mode operation of a block cipher $E()$ work?

   a) $C = E(i) \oplus i$

   b) $C = E(i) \oplus M \oplus i$

   c) $C_i = E(i) \oplus M_i$

   d) $C = E(i) \oplus M$

10. How is the IEEE 802.11 CCMP nonce input constructed?

    a) The values of the Pairwise Transient Key, the NonceA, and the NonceB

    b) The values of the Pairwise Temporal Key, the Source Address, and the Destination Address

    c) The values of the fields Packet Number, Address1, Flag of the MPDU

    d) The values of the fields Packet Number, Address2, Priority of the MPDU

11. Does GSM provide mutual authentication?

    a) No

    b) Yes

    c) Operator dependent

    d) In cooperation with UMTS

12. How is the subscriber identity protected from radio channel eavesdropping in GSM?
    a) By the network providing temporary subscriber identities to the SIMs
    b) By storing the subscriber identity in the SIM only
    c) By storing the 128-bit secret key (K_{IMSI}) in the SIM and distributed only to trusted VLRs
    d) By using the IMEI instead of the IMSI

13. Which information is sent from the AuC to the VLR/SGSN during 3G/UMTS authentication?
    a) IMSI
    b) RAND, AUTN, XRES, CK, IK
    c) RAND, AUTN
    d) RAND, AUTN, XRES, Kc

14. Which UTRAN layers provide encryption?
    a) MAC layer and RRC layer
    b) RLC layer and RRC layer
    c) PHY layer and MAC layer
    d) MAC layer and RLC layer

15. What happens if the result of the UTRAN algorithm negotiation is that the user equipment (UE) and the network do not have a common encryption algorithm?
    a) UTRAN provides a new encryption algorithm as an app
    b) The connection is shut down immediately by UTRAN
    c) UTRAN may establish the connection without encryption
    d) UTRAN does not use encryption algorithm negotiation

16. Can the security header in MAPsec be encrypted? Why/why not?
    a) No, because the header consists of {SPI || Original Component ID || TVP}
    b) Yes, because the header consists of {SPI || Original Component ID || TVP}
    c) No, because the MAPsec header must be processed at the receiving end
    d) Yes, because an IPsec tunnel is set up

17. Which CSCF handles SIP registration requests and informs the Home Subscription Server (HSS)?
    a) All
    b) P-CSCF
    c) I-CSCF
    d) S-CSCF

18. Which three modes does the confidentiality algorithm in UMTS support?

    a) RLC-Transparent, RLC-Unacknowledged, RLC-Acknowledged

    b) RRC-Transparent, RRC-Unacknowledged, RRC-Acknowledged

    c) RLC-Transparent, RRC-Unacknowledged, RLC-Acknowledged

    d) RRC-Transparent, RLC-Unacknowledged, RRC-Acknowledged

19. In which mode of operation is KASUMI used for constructing the 3GPP f8 key stream generator?

    a) Combining Counter-mode and ECB-mode

    b) Combining Counter-mode and CCM-mode

    c) Combining Counter-mode and OFB-mode

    d) Combining Counter-mode and CBC-mode

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

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

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

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

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

21. What was the underlying assumption for the MILENAGE security analysis?

    a) No assumptions were made

    b) The kernel function must be a robust block cipher

    c) AES must be used as the kernel function

    d) The kernel function must be a oneway function

22. Which part of the IEEE 802.16 MAC PDU is encrypted?

    a) Both the header and the payload part

    b) The payload part and some fields of the header

    c) The payload part

    d) The header part

23. Which WiMAX entity is generating the Traffic Encryption Key (TEK)?

    a) The Base Station

    b) The AAA Server

    c) The Access Service Network

    d) The Network Service Provider

24. Why can the USIM be removed from the rest of the UE?

    a) The USIM holds an expiration date and, like credit cards, must be replaced

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

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

    d) End-to-end UMTS key-card plugs into the USIM slot for key distribution and management

25. What is Internet Key Exchange (IKE)?

    a) The security association set up protocol in the IPsec protocol suite

    b) The key exchange subprotocol of the Transport Layer Security protocol

    c) The key transformation protocol for the inter-operation of GSM and UMTS

    d) The security association center in the IMS system

Part II. Authentication Protocols (30%)

As Master of communication security in Securemore Inc. you are responsible for contributing to a NextGSM recommendation proposal for enhancing the authentication protocol in the GSM system. You start thinking about the problem by recapitulating the GSM Authentication and Key Agreement protocol. Next you construct a new and promising enhancement to this cryptoprotocol that needs to be analyzed.

26. Recall the standard entity authentication and key transport protocol of the GSM mobile network, which includes the entities SIM&MS, BS, VLR, HLR & AuC. Draw the protocol, using the supplied MSD form, and include all security messages with variables and computations starting from "Identity Request" to "Cipher Mode Command". (3%)

27. Formulate compactly the security assumptions and the logic for the security claims regarding the authentication of a SIM resulting from the protocol interactions and computations of Question 26. (6%)

28. Consider the scenario where Malice is able to set up a rogue GSM base station that can accept both incoming MS connections and establish connections to genuine GSM network operators. Make a message sequence diagram that shows how Malice is able to "catch IMSIs" and eavesdrop on the communications of calling MS. (6%)

29. Now construct your enhancement to the GSM authentication protocol, while preserving the existing GSM authentication protocol. The protocol must enable the SIM to distinguish between rogue and authentic access network connections, and assure the SIM that the link encryption key is fresh, and available at the BS. Draw your protocol diagram, and formulate the assumptions and the logic for your security claims of the new protocol construction. (7%)

30. Compare the number of bits in the message exchange and the computations of your protocol with the original GSM protocol. What is the increase in communication and computational load? (2%)

31. A successful man-in-the-middle attack can be defined as an attack that engages two independent protocol participants to communicate with the attacker in such a way that a security goal/claim of the protocol is broken. Analyze your enhanced GSM authentication protocol with respect to a man-in-the-middle attack threat, and describe your reasoning and conclusion. (6%)

Part III. Analysis of Cipher Initialization Implementation (20%)

Alice is conducting an experiment in wireless network security. Using the aircrack-ng tool suite, she tries several different attacks on a Cisco access point (AP) configured with Wired Equivalent Privacy (WEP). While running an ARP replay attack with 682 captured data frames per second, the total number of unique initialization vectors (IVs) observed seems to reach a maximum value of approximately 1 040 000 after about two hours. The Table 1 is reproducing the measurements from her lab journal. It shows the number of minutes the ARP replay attack has been running and the total number of unique IVs observed with time. The number of fresh IVs observed is close to the number of captured data frames in the first few minutes of the experiment, and then the growth gradually decreases until it is close to zero after approximately two hours.

Minutes	Unique IVs observed
2	76 874
23	629 428
30	727 198
40	824 629
50	896 612
60	945 423
80	1001 550
100	1026 429
120	1038 326
140	1043 822

Table 1: The accumulated number of different IVs observed with time.

32. State at least three different methods of IV value generation. (2%)
33. What is the size of the set of IV values in the WEP specification? (3%)
34. How do your answers to the questions above relate to the data in Alices experiment as shown in Table 1? (3%)

The lab journal of Alice shows that she did not expect this IV generator behaviour, and she has repeated the experiment several times but each time she ends up with very similar results.

35. Look into the data of Table 1 and search for an explanation why Alice did not expect this result, then settle for a plausible hypothesis of the generation of the IV values based on your observations and assumptions. State your hypothesis about the IV generation used by this AP, and explain how you found the result. (3%)

Fortunately, a mathematical friend of yours is familiar with a problem from probability theory that applies to this experiment, the general birthday problem. This problem states that when n values are selected with a uniform distribution, with replacement, from a total population of m values, the expected number of *unique* values observed is

$$E(m, n) = m(1 - (1 - 1/m)^n).$$

In the experiment, m represents the total number of possible IV values, and n represents the number of data frames captured, hence $E(m, n)$ represents the expected number of unique IV values observed.

36. Add two new columns for Table 1 and make the following computations. The first new column should show the expected number of unique IVs observed under your hypothesis at 60, 120 and 140 minutes. The second new column should show the expected number of unique IVs observed using WEP with random IV selection at 60, 120 and 140 minutes. (3%)

37. Draw interpolation plots for the experimental data and the two new columns described above at 60, 120 and 140 minutes. (2%)

As a final step, you decide to have a look at the actual IVs in the capture file. Table 2 shows 25 IV values from one of the experiments of Alice.

011100100101011011010110
011101110010100010101000
011011100100110001011100
011011010010001110001100
001111000000100101110100
001111000010000100011010
011100000000000111100000
011001100100010101110010
011101110000111011101110
011010100001110011100110
011111010100100110100110
001011110110010101101010
011101110010101010000000
011010100101111111101010
011001110010000001011110
001000010001111011100010
001011110001011100000100
001111100110011000110010
001100100001110110101010
001000000011010101011000
011110110100100011100100
011010010111100100010000
001001100100100000001100
011100110111011010100110
011010100111000101011100

Table 2: A sample of captured IVs in binary representation.

38. Does the data in Table 2 support your hypothesis? Explain why/why not. What new information can you find by looking at the actual IVs in Table 2? (4%)