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 1, 2008.

Time of exam: 9:00 – 13:00 (4 hours).

Date of grade assignment: December 22, 2008.

Credits: 7.5

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

Attachments:

- 7 pages of questions and 1 page for multiple choice answers.

The 40 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 not necessarily in your order of difficulty, so time your work and make sure you find time for all questions. We hope you will find Part II and III both enlightening and entertaining. Please make your best effort to write comprehensible, and with brief, concise and good answers. 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. Which stream cipher is used for WEP encryption?

   a) AES

   b) DES

   c) RC4

   d) RC5

2. What is the length of the WEP initialization vector (IV)?

   a) 24 bits

   b) 32 bits

   c) 48 bits

   d) 64 bits

3. How many messages are exchanged in the WEP shared key authentication protocol?

   a) 2

   b) 3

   c) 4

   d) 5

4. Is the same key used for both authentication and encryption in WEP?

   a) Yes

   b) No

   c) Yes, if 802.1X authentication is not used

   d) The same key is never used twice

5. What is an RC4 weak key value?

   a) A key value where many bits of the first bytes of the plaintext are leaked when an IV collision occurs

   b) A key value where a few bits in the key determine many bits in the first few bytes of the key stream

   c) A key value where a few bits in the key determine many bits in the cipher text

   d) A key value where the bits in the key determine the bits in the first few bytes of the key stream

6. Which cryptographic algorithm is used in counter mode with cipher block chaining message authentication code protocol (CCMP)?

   a) AES

b) Michael
c) RC4
d) TLS

7. Which three roles participate in the 802.1X access control protocol?

a) Station, authenticator and autentication center
b) Client, server and RADIUS server
c) Supplicant, access point and RADIUS server
d) Supplicant, authenticator and authentication server

8. How many EAP-TLS messages are exchanged in an EAP-TLS handshake?

a) 2
b) 4
c) 9
d) It varies with the TLS parameters exchanged

9. What encapsulates EAP messages in RSN?

a) They are encapsulated in TCP/IP
b) They are encapsulated in EAPOL messages
c) They are encapsulated in RADIUS messages
d) They are encapsulated in EAPOL and RADIUS messages

10. Does EAP-SIM provide mutual authentication?

a) No, it uses the regular GSM authentication
b) Yes, by the regular GSM authentication and the authentication token from the AuC
c) Yes, by the regular GSM authentication and a nonce in the encrypted AP response
d) Yes, it uses the regular UMTS authentication

11. 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

12. How long is the IV used in TKIP?

a) 24 bits
b) 48 bits
c) 64 bits
d) 128 bits

13. What is the key size of AES as used in RSN?

    a) 128 bits
    b) 192 bits
    c) 256 bits
    d) 512 bits

14. What is the block size of AES as used in RSN?

    a) 64 bits
    b) 128 bits
    c) 256 bits
    d) 512 bits

15. Is the complete MAC PDU encrypted by the CCMP?

    a) Yes, the CCMP uses a shared key
    b) No, the MAC header is not encrypted
    c) No, the CCMP header is not encrypted
    d) No, the MAC header and the CCMP header are not encrypted

16. Which GSM entities store the secret user keys K_i?

    a) MS and HLR
    b) VLR and AuC
    c) SIM and AuC
    d) SIM, BS and VLR

17. What is the output of the GSM authentication function A3?

    a) MAC (32-bit message authentication code)
    b) MAC (64-bit message authentication code)
    c) SRES (32-bit signed response)
    d) SRES (64-bit signed response)

18. Which authentication data does the GSM VLR have to request?

    a) The authentication quintet (RAND, AUTN, XRES, CK, IK)
    b) The authentication quintet (RAND, AUTN, XRES, K_i, K_c)
    c) The authentication triplet (RAND, XRES, K_i)
    d) The authentication triplet (RAND, XRES, K_c)

19. What are the variables of the authentication token (AUTN) used in UMTS networks?

    a) $SQN \oplus AK$, XRES, MAC
    b) $SQN \oplus AK$, AMF, MAC
    c) SQN, AMF, MAC, RAND
    d) $SQN \oplus AK$, AMF, MAC, RAND

20. Which UTRAN layer provides integrity protection?

    a) MAC layer

    b) RLC layer

    c) RRC layer

    d) Physical layer

21. What happens if the result of the UTRAN algorithm negotiation is that the user equipment (UE) and network have no integrity protection algorithms in common?

    a) The network may establish the connection without integrity protection

    b) The connection is shut down immediately by the network

    c) The network may establish the connection with the default integrity protection algorithm

    d) UTRAN does not use integrity algorithm negotiation

22. How is the traffic between the terminal equipment and Proxy CSCF (P-CSCF) protected in IMS?

    a) Using the UMTS f8 encryption algorithm with the cipher key CK

    b) Using IPsec Authentication Header (AH)

    c) Using IPsec Encapsulated Security Payload (ESP)

    d) It is not protected at all, but the UTRAN radio link is protected by the UMTS security mechanisms

23. Which authentication method is used by IMS?

    a) Internet Key Exchange (IKE)

    b) IPsec Authentication Header (AH)

    c) IPsec Encapsulated Security Payload (ESP)

    d) UMTS Authentication and Key Agreement (AKA)

24. What is the length of the cipher key CK used in UMTS?

    a) 56 bits

    b) 64 bits

    c) 128 bits

    d) 256 bits

25. Which UMTS entities implement the functions f1-f5, f1* and f5*?

    a) USIM, UE and BS

    b) SGSN and AuC

    c) USIM and AuC

    d) USIM, BSC and AuC

Part II. Authentication Protocols (30%)

As the communication systems security engineer in Telematics Inc. you are responsible for the design of an authentication protocol between mobile equipment UE and a new radio access network PTRAN being developed. You start thinking about the problem by recalling the UMTS Authentication and Key Agreement protocol, denoted $\mathcal{U}$ here.

26. Draw a message sequence diagram of $\mathcal{U}$ that shows how the authentication and session key generation take place between the user equipment UE and the radio access network UTRAN. Show how the message variables are computed and communicated. (5%)

Having finished your recollection of UMTS, a new protocol proposal $\mathcal{P}$ arrive on your desk for your analysis. The cryptographic functions are the same as in UMTS. Here is $\mathcal{P}$:

$\boxed{\textbf{UE}}$		$\boxed{\textbf{PTRAN}}$
Const (IMSI,K) RAND1 $= f0()$		Table $\{$(IMSI, K)$\}$
	$\xrightarrow{\text{IMSI,RAND1}}$	
		RES1 $= f2_K$(RAND1) RAND2 $= f0()$
	$\xleftarrow{\text{RES1,RAND2}}$	
Verify RES1 RES2 $= f2_K$(RAND2)		
	$\xrightarrow{\text{RES2}}$	
		Verify RES2
CK $= f3_K$(RAND1 $\oplus$ RAND2) IK $= f4_K$(RAND1 $\oplus$ RAND2)		CK $= f3_K$(RAND2 $\oplus$ RAND1) IK $= f4_K$(RAND2 $\oplus$ RAND1)

27. Compared to $\mathcal{U}$, which new function do you find must be implemented in UE for $\mathcal{P}$? Propose how this function can be implemented.(5%)

28. All variables in $\mathcal{P}$ er 128 bits except IMSI. What is the difference between $\mathcal{U}$ and $\mathcal{P}$ with respect to the number of bits communicated?(5%)

29. Make an analysis of $\mathcal{P}$ and try to identify at least two security weaknesses not present in $\mathcal{U}$. What are the weaknesses?(5%)

30. What is the basis for your claim that the generation of (CK, IK) is better in $\mathcal{P}$ than in $\mathcal{U}$?(5%)

31. Propose how $\mathcal{P}$ can be modified in order to avoid the security problems you identified in Question 29.(5%)

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

You are conducting an experiment in wireless network security. Using the aircrack-ng tool suite, you try 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. Your lab journal table is reproduced below. It shows the number of minutes the ARP replay attack has been running and the total number of unique IVs observed with time. After 140 minutes, it seems like you are not able to obtain any more unique IVs from the AP.

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. What is the purpose of the IV in WEP? (2%)
33. Name at least two different methods of IV value generation.(2%)
34. What is the security problem with a fixed value for IV?(2%)
35. How is the size of the set of IV values in the WEP specification? (2%)
36. How does this relate to the observations in your experiment as shown in Table 1?(2%)

The observations in your experiment are not what you expected, so you repeat it several times but get similar results. You search for an explanation and decide on a hypothesis based on your observations. Since the increase in the number of unique IVs observed is close to the number of captured data frames in the first few minutes of the experiment, and then gradually decreases until it is close to zero after approximately two hours, you assume that the IVs are picked randomly. But the total number of different IVs observed is lower than expected.

37. Based on the description above, state your hypothesis about the number of possible IV values in use by this AP. Explain how you found the result.(2%)

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 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.

38. 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 100, 120 and 140 minutes. The second new column should show the expected number of unique IVs observed using WEP with random IV selection at 100, 120 and 140 minutes.(3%)

39. Create a plot of the experimental data and the two new columns described above at 100, 120 and 140 minutes.(2%)

As a final step, you decide to have a look at the actual IVs from your capture file. Table 2 shows 25 IVs from your experiment, one IV per line and in binary format.

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

40. 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?(3%)