English

Norwegian University of Science and Technology
Department of Telematics

EXAM IN
TTM4137 – WIRELESS SECURITY

Contact person: Professor Stig F. Mjølsnes. (Tel. 918 97 772).

Date of exam: December 12, 2012.

Time of exam: 9:00 – 13:00 (4 hours).

Date of grade assignment: January 12, 2012.

Credits: 7.5

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

Attachments:

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

The 36 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. 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 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. How does the integrity check value (ICV) in WEP protect against message modification attack?
   a) The ICV in WEP protects against message modification due to the integrity key
   b) The ICV in WEP protects against message modification by the error-detection property
   c) The ICV in WEP does not protect against message modification by an attacker
   d) The ICV in WEP protects against message modification by the challenge value
3. What is "Michael" in RSN?
   a) Michael is the 32 bits sequence counter scheme used in TKIP
   b) Michael is the 64 bits block encryption scheme used in TKIP
   c) Michael is the 20 bits replay protection scheme used in TKIP
   d) Michael is the 64 bits message authentication code used in TKIP
4. What are the consequences 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 decrypt traffic and send packets with custom content
   c) An attacker can cause packets to be silently dropped
   d) An attacker can send packets with custom content over QoS channels
5. What is the 128-bit start value for RSN CCMP encryption?
   a) 8-bit flag, 104-bit nonce, 16-bit counter; where the nonce created 8-bit priority, 48-bit source address, 48-bit packet number
   b) 128-bit fresh nonce
   c) 16-bit flag, 104-bit nonce, 8-bit counter; where the nonce created 8-bit priority, 48-bit source address and 48-bit packet number
   d) 16-bit packet number, 112-bit nonce
6. What is a mutable field in RSN CCMP?
   a) A header field that is modified in transmission to ease decryption operation
   b) A header field that may be modified in transmission
   c) An integrity protected header field that may be modified prior to transmission

d) An encrypted header field that may be updated prior to transmission

7. 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

8. The TKIP Pairwise Transient Key is a collection of several keys.

   a) Pairwise Master Encryption Key (256 bits), Pairwise Master Data Integrity Key (128 bits), EAPOL-Key Encryption Key (64 bits), EAPOL-Key Integrity Key (64 bits)
   b) Pairwise Master Encryption Key (256 bits), Pairwise Master Data Integrity Key (256 bits), EAPOL-Key Encryption Key (64 bits), EAPOL-Key Integrity Key (64 bits)
   c) Data Encryption Key (128 bits), Data Integrity Key (128 bits), EAPOL Pairwise Master Encryption Key (256 bits), EAPOL Pairwise Master Integrity Key (256 bits)
   d) Data Encryption Key (128 bits), Data Integrity Key (128 bits), EAPOL-Key Encryption Key (128 bits), EAPOL-Key Integrity Key (128 bits)

9. 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*

10. How is the subscriber identity protected from radio channel eavesdropping in GSM?

    a) By a temporary subscriber identity
    b) By the subscriber key encryption
    c) By the tamper-resistant SIM card
    d) The subscriber identity is not protected in GSM, only in UMTS and LTE

11. What is the purpose of the sequence number (SQN) used in UMTS?

    a) Preventing replay attacks
    b) Preventing man-in-the-middle attacks
    c) Preventing session hijacking
    d) Enabling re-synchronization

12. 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

13. 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

14. What are the purposes of the UMTS MILENAGE functions?

    a) Message encryption and authentication

    b) Message encryption and session key generation

    c) Message and user authentication/confirmation, and session key generation

    d) Message authentication and session key generation

15. What is the output of the UMTS $f9$ algorithm?

    a) It is a 32-bit MAC

    b) It is an indefinite length keystream

    c) It is a 64-bit block ciphertext

    d) It is a 32-bit authenticated ciphertext

16. What are the consequences of the Zhang & Fang redirection attack against UMTS authentication?

    a) Because serving networks are not authenticated in UMTS, an attacker can redirect the traffic via servers abroad, causing roaming fees

    b) Because serving networks are not authenticated in UMTS, an attacker can learn the session keys

    c) Because core networks are not authenticated in UMTS, an attacker can redirect the traffic to an authentication center abroad, causing roaming fees

    d) Because core networks are not authenticated in UMTS, an attacker can learn the session keys

17. Is the UMTS/LTE network domain security specifications for the core network sufficient to protect the authentication and key agreement messages against parallel session attacks?

    a) No, the network domain security does not necessarily protect the session identifier, but this cannot be exploited by an attacker

    b) No, the network domain security does not necessarily protect the session identifier and may allow session-mixup attacks

    c) Yes, the network domain specification demands the use of IPsec or MAPsec, and therefore the core network communication is protected

    d) Yes, but the core network communication is always assumed to be secure, independent of the network domain security specifications

18. How is forward key separation achieved during handovers over X2 connections in EPS?
    a) The target eNB gets a fresh key from MME immediately after handover
    b) The target eNB gets a fresh key from MME right before handover
    c) The source eNB provides a key KeNB to the target eNB by applying a one-way function to the old key
    d) Forward key separation is not achieved, only backward key separation
19. Which attacks are prevented if an RFID reader authenticates to a tag?
    a) For instance, tracking of the tag
    b) For instance, distance measuring and tag blocking
    c) For instance, tag inventory registration
    d) For instance, illicit reading, cloning, and reprogramming of the tag
20. How does the anti-counterfeiting measure "track and trace" for low cost RFID tags work?
    a) By reading tags regularly with centralized storage for date and location, then a tag is "genuine" if it has a valid item history
    b) By using a challenge & response protocol, where the tag must answer a random challenge by the reader
    c) By using a privacy-preserving identification protocol
    d) By observing the unique radio communication fingerprint of a tag
21. What are the general steps performed by intrusion detection systems for mobile ad-hoc networks?
    a) Data Collection and Retaliation
    b) Data Collection, Detection, and Response
    c) Node Detection, Obstruction, and Response
    d) Node Detection, Rendering, and Alarm
22. What is the vulnerability of captive pages?
    a) The weak encryption can easily be broken
    b) There is encryption but no integrity protection
    c) There is integrity protection but no encryption
    d) Sessions can be hijacked
23. What is the problem with MAC Sequence Number Analysis in Intrusion Detection Systems?
    a) The MAC Sequence Number Analysis does not work at all because the sequence numbers are not integrity protected
    b) The MAC Sequence Numbers only protect against message replay attacks, but not against session hijacking
    c) Each class in QoS (WMM) has its own sequence number. Also an attacker can still hijack a session when the victim goes offline
    d) Implementations very often use a constant value as MAC Sequence Number, and, therefore, this does not even protect against replay attacks

24. 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

25. Why is it not sufficient to construct a one-way function $y = f(x)$ based on an NP-hard problem?

    a) The one-way property requires that the problem is NP-complete and not just NP-hard

    b) NP-hardness guarantees only that there exists a y for which x is hard to compute

    c) A one-way function must satisfy the property of collision-resistance too

    d) Computing a preimage must be hard in the worst case

Part II. Password Based Authentication (20%)

The company Cyberphobia uses a networked file server to store sensitive customer information. Each of the 100 employees has a user account on the server. Most users access the server by a WiFi network. Only 10 users have write permission to the server files, the rest can only read the files. Security engineer Terje decides to use simple password based user authentication for the server access, however, one of the immediate precautions he has taken is to create a computer program that generates random passwords of length 10 characters. All employees are obliged to generate their passwords using this program.

26. What kind of attack did Terje prevent by this solution? (2%)

The server access list is stored in a text file which ordinary users cannot access. Nevetheless, Terje decides to store hash values of the passwords, i.e., the entries in the text file `passwords.txt` are of the form $(id, h(pwd_{id}))$. For simplicity, assume that he uses an ideal cryptographic hash function (with uniformly distributed output) $h : \{0,1\}^* \to \{0,1\}^k$, where $k = 32$.

One dishonest user, Malin, plans a scam, for which she needs write permissions to some files. Anne is one of the users with write permissions, and she connects to the file server every day.

27. Explain a technical attack Malin can perform to acquire the write permissions she wants? (2%)

Now you propose to use a slightly different authentication protocol, where the user must send $(id, h(pwd_{id}))$ to the file server login process. Explain under which circumstances this protocol is:

28. As secure as the currently implemented protocol, (2%)

29. Better than the currently implemented protocol. (2%)

Malin somehow comes across a fresh printout of `passwords.txt`, where she sees that Terje forgot to delete the user entry for ex-employee Berit, with write permissions.

30. What is the minimum number of random passwords Malin has to try in order to have a success probability greater than 0.01? (5%)

A math student friend of yours recently raved about a curious combinatorial problem, called *The Birthday Paradox*. "The solution is not really a paradox," she said, "but quite surprising".

> Suppose we bring together 23 people at random, like students in a classroom, then "the paradox" tells us that it is pretty likely (probability more than 0.5) that we will find two people in this small group with birthdays on the same date.

The probability of two people having different birthdays is $1 - \frac{1}{365}$. (we will just assume that 29th of February is nobody's birthday.) With $n = 23$ people, there are $\frac{n \cdot (n-1)}{2} = \frac{23 \cdot 22}{2}$ pairs. So, the probability that there are no two people that share a birthday is $(1 - \frac{1}{365})^{\frac{23 \cdot 22}{2}}$, and thus, the probability that there are two people with the same birthday is

$$p = 1 - (1 - \frac{1}{365})^{\frac{23 \cdot 22}{2}}.$$

If we use the approximation $e^x \approx 1 + x$, when x is close to 0, then we have that

$$p \approx 1 - e^{-\frac{1}{365} \cdot \frac{23 \cdot 22}{2}} = 0.5005.$$

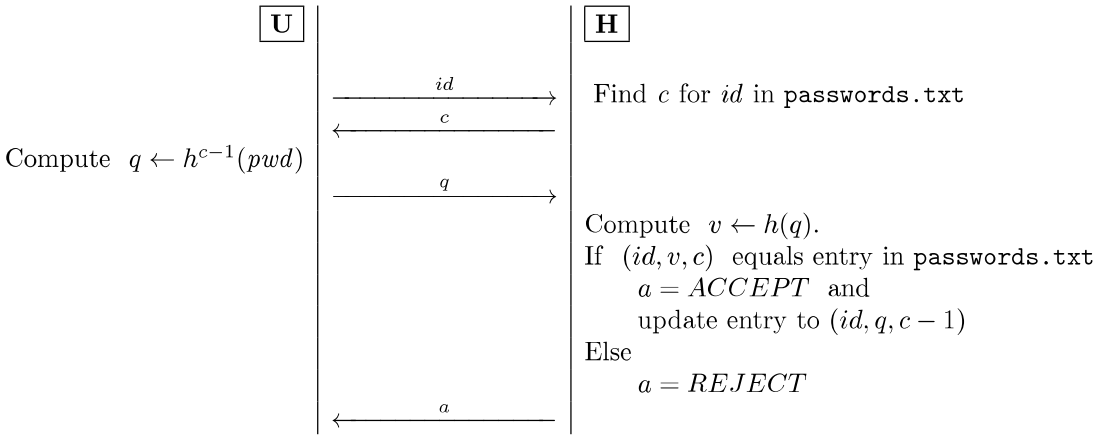
Part III. Protocols (30%)

Recall the password authentication protocols of Part II. Terje now realizes that his protocol is not sufficiently secure for the purpose, so he decides to consult you, a network security expert, in order to propose a better solution. You come up with the following SKEY protocol:

SETUP:

The user U and host H set up U's initial entry $(id, h^{100}(pwd), 100)$, where h is a cryptographic hash function. The protocol will modify the entry to $(id, h^{c}(pwd), c)$, where $1 \leq c \leq 100$.

PROTOCOL:



Now you go on to analyze the security and efficiency properties of this SKEY protocol.

32. State the intended security and correctness properties of the SKEY protocol. (5%)

33. Describe a possible man-in-the-middle attack for the SKEY protocol. Justify your answer. (6%)

34. Adapt the SKEY protocol to a mobile network system with mobile stations, visited networks, and home networks. Describe your protocol construction. (6%)

35. Compare your protocol to the GSM authentication and key agreement protocol and its security properties. (6%)

36. Make a comparison of your protocol with the GSM authentication protocol in terms of computational efficiency. Assume that the computing cost of the A3 function is the same as the computing cost of the function h. Discuss the possible time-memory trade-offs in all of the entities in the protocol. (7%)

sfm