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, 2011.

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:

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

The 35 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 major weakness in WEP, exploited by the PTW attack used in the lab?
   a) The initialization vector is too short
   b) No protection against message replay
   c) The integrity check value is too short
   d) The IV is part of key stream
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 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
4. Which cryptographic algorithm is used in counter mode with cipher block chaining message authentication code protocol in CCMP?
   a) AES
   b) Michael
   c) RC4
   d) KASUMI
5. What is the purpose of the EAPOL 4-way handshake?
   a) To compute a fresh pairwise temporal key (PTK) from the pairwise message 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
6. 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) $C = E(i) \oplus M$

7. Is the complete MAC PDU encrypted by the CCMP?
   a) Yes, the CCMP uses a shared key
   b) Yes, the CCMP header is encrypted
   c) No, the MAC header is not encrypted
   d) No, the MAC header and the CCMP header are not encrypted
8. Which block cipher mode of operation is used for AES in RSN?
   a) Counter Mode with Cipher Block Chaining Message Authentication Code
   b) Counter Mode with Galois Message Authentication Code
   c) Cipher Block Chaining with Counter Mode Message Authentication Code
   d) Cipher Block Chaining with Hashed Message Authentication Code
9. How is the 128 bits start value of the counter for CCMP encryption initialized in RSN?
   a) By a random IV
   b) By the concatenation of IV and the extended IV
   c) By flag/priority bits, packetnumber, source-address, and a constant
   d) By source address, destination address and the MIC value of the MPDU
10. Which 802.11 frame type is cryptographically protected by the 802.11w standard?
    a) Data frames
    b) Control frames
    c) Management frames
    d) Beacon frames
11. How is the subscriber identity protected from radio channel eavesdropping in UMTS?
    a) By the network providing temporary subscriber identities to the USIMs
    b) By keeping the subscriber identity in the USIM only
    c) By storing the 128-bit secret key (K_{IMSI}) in the USIM, and distribute only to trusted VLRs
    d) By using the IMEI instead of the IMSI
12. Which information is sent from the HSS to the MME during the LTE/EPS authentication protocol?
    a) IMSI, RAND, AUTN, XRES
    b) RAND, AUTN, XRES, K_{ASME}
    c) RAND, AUTN, XRES, CK, IK
    d) RAND, AUTN, XRES, K_c
13. Which UTRAN protocol 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

14. What happens if the result of the UTRAN cryptoalgorithm 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 download
    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

15. 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

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

    a) No assumptions were made
    b) The kernel function must be a secure block cipher
    c) AES must be used as the kernel function
    d) The kernel function must be a one-way function

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

    a) The UE manufacturing and lifecycle can be managed independently from the personalization and subscription process
    b) The failure rate of the integrated circuit cards (UICCs) are high because the issuers (mobile operators) want to reduce cost for short subscription duration
    c) End-to-end UMTS key-card may be plugged into the USIM slot for key distribution and management
    d) The USIM holds an expiration date and, like credit cards, must be replaced

18. What is the bit length of the permanent subscriber key in UMTS?

    a) 56
    b) 64
    c) 128
    d) 256

19. The end points of the 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

20. The end points of signal-message 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

21. The end points of signal-message integrity protection 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

22. Does LTE/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

23. Can a 3G USIM work in an LTE UE handset?

    a) No, because the cryptokeys must be kept in the USIM
    b) No, because the cryptokeys are not compatible
    c) Yes, because the cryptokeys are the same in the two systems
    d) Yes, because the USIM cryptokey output is the same in the two systems

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

    a) In the USIM and the AuC
    b) In the USIM and the UE
    c) In the UE and the MME
    d) In the UE and the HSS

25. What is lawful interception in mobile communication networks?

    a) Eavesdropping approved by judicial court
    b) Eavesdropping performed by or on behalf of the police authorities
    c) Signal jamming ordered by the police authorities
    d) Law enforcement command to the mobile operators to turn off the communication encryption in order to enable eavesdropping

Part II. Cryptographic Mechanisms (35%)

26. What is the difference between a block cipher and a stream cipher? (3%)

27. What is a one-way function? Give an example of a one-way function construction and its usage. (4%)

28. Define the cipher-block-chaining mode with an algebraical formulation for the block cipher $c = e_k(m)$. (3%)

29. What is a message authentication code (MAC)? Give an example of a MAC function construction. (5%)

30. Can you think of a reason why MD5 hash values are used instead of message authentication codes (MAC) to identify known files in digital forensic procedures? (3%)

31. What is the purpose of an initialization vector (IV) in cipher systems? How large must the set of IV values be, and how can the values be chosen? (7%)

32. Analyze the RC4 algorithm pseudocode below and find what the size of the key space of the RC4 cipher can be? Explain. (4%)

Variables:

```
int keylength
byte i, j, S[256], keyinput[int]
boolean Continue
```

RC4 key schedule:

```
for i from 0 to 255
   { S[i] := i }
j := 0
for i from 0 to 255
  { j := (j + S[i] + keyinput[i mod keylength]) mod 256
   swap(S[i], S[j]) }
```

RC4 generator:

```
i := 0 ;  j := 0 ; Continue := True
while Continue  {
    i := (i + 1) mod 256
    j := (j + S[i]) mod 256
    swap(S[i], S[j])
    output S[(S[i] + S[j]) mod 256] }
```

33. A pseudorandom generator can be modeled as a finite state machine. What is the number of possible states for the RC4 generator? What can you tell from the *relation* between the number of possible states and the key space of the RC4 cipher? (As an aside, the number of atoms in the observable universe is estimated to about 10^{80}, a quite minuscule number in this context!) (6%)

Part III. Protocols (15%)

34. Name and characterize the main categories of protocol attackers, and rank them according to their capabilities. (5%)

35. Construct a cryptoprotocol for two parties that want to select and use one out of several MAC algorithms, over an open insecure network. Explain the model and assumptions, the protocol attacker category(-ies), the interactions, the local computations, and express in an itemized way your security claims for the protocol. (10%)

_____sfm_____