English

Norwegian University of Science and Technology
Department of Telematics

EXAM IN
TTM4137 – WIRELESS SECURITY

Contact person: Professor Danilo Gligoroski. (Tel. 95089319).

Date of exam: December 04, 2013.

Time of exam: 9:00 – 13:00 (4 hours).

Date of grade assignment: January 06, 2014.

Credits: 7.5

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

Attachments:

- 7 pages of questions,

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.

Multiple choice answers Candidate nr ___________________

USE CAPITAL LETTERS!

PLEASE FILL IN AND DELIVER THIS PAGE

Nr.	Answer
1	
2	
3	
4	
5	
6	
7	
8	
9	
10	
11	
12	
13	

Nr.	Answer
14	
15	
16	
17	
18	
19	
20	
21	
22	
23	
24	
25	

1. Which one of the following security goals were present for the WEP design:
   A. To be equivalent to the Kerberos access policy.
   B. To be equivalent to wired access point security.
   C. To be equivalent to wide ethernet protocol.
   D. To be equivalent to wireless entity policy.

2. Which key distribution protocol is specified in WEP?
   A. Diffie-Hellman key distribution.
   B. RC4 key distribution.
   C. RSA key distribution.
   D. There is no specified key distribution protocol in WEP.

3. What is the major weakness in WEP, exploited by the PTW attack used in the lab?
   A. RC4 is broken even with 104 bit keys
   B. The initialization vector is too short
   C. No protection against message replay
   D. The integrity check value is too short

4. WPA and WPA2 share the following security component:
   A. CCMP
   B. TKIP
   C. AES
   D. RC4

5. How many message integrity failures have to be logged in order the Temporal Key Integrity Protocol to start the Denial Of Service mechanism:
   A. Two failures within 60 seconds
   B. Two failures within 30 seconds
   C. Two failures within 10 seconds
   D. Two failures within 1 second

6. In RSN, the encryption and message authentication are realized via
   A. AES-GCM
   B. AES-CBC
   C. AES-HMAC
   D. AES-CCMP

7. How big is the message integrity code in RSN
   A. 32 bits
   B. 48 bits
   C. 64 bits
   D. 128 bits

8. What is Extensible Authentication Protocol (EAP)?
   A. EAP is a set of encapsulation messages for upper-layer authentication methods
   B. EAP is a set of encapsulation messages for physical layer authentication methods
   C. EAP is a set of encapsulation messages for PKI authentication methods
   D. EAP is a set of encapsulation messages for RADIUS server authentication methods

9. In GSM, what is the role of the Visitor Location Register:
   A. When mobile equipment register to the network, to retrieve the information for that equipment from HLR.
   B. To protect the anonymity of the owner of the mobile equipment.
   C. To obtain a session key from HLR.
   D. To communicate the user's Authentication Center (AuC).

10. Which security mechanism is NOT present in GSM:
   A. Authentication
   B. Confidentiality
   C. Anonymity
   D. Authorization

11. In GSM, what is the role of A8 algorithm:
   A. For production of random numbers
   B. For encryption key generation
   C. For user authentication
   D. For Data encryption

12. The function f6( ) in the MAPsec protocol of UMTS is:
   A. AES in counter mode
   B. AES in CBC mode
   C. KASUMI in counter mode
   D. KASUMI in CBC mode

13. How many modes of protection offers MAPsec?
   A. 1
   B. 2
   C. 3
   D. 4

14. What is the crucial protocol in IP Multimedia Subsystem
   A. Internet Key Exchange (IKE)
   B. MAPsec
   C. Session Initiation Protocol (SIP)
   D. IPsec

15. A simple description of MILENAGE functions can be done as:
    A. $f_{i,K}(x) = E_K(E_K(x \text{ xor } c_i))$; where i = 1,2,3,4,5, and c_i are distinct constants
    B. $f_{i,K}(x) = E_K(E_K(x) \text{ xor } c_i)$; where i = 1,2,3,4,5, and c_i are distinct constants
    C. $f_{i,K}(x) = E_K(E_K(c_i) \text{ xor } x)$; where i = 1,2,3,4,5, and c_i are distinct constants
    D. $f_{i,K}(x) = E_K(E_K(x)) \text{ xor } c_i$; where i = 1,2,3,4,5, and c_i are distinct constants

16. Which two ciphers are used in UEA1 and UEA2
    A. AES and KASUMI
    B. AES and RC4
    C. AES and SNOW 3G
    D. KASUMI and SNOW 3G

17. In UMTS, the function f9( ) is used for:
    A. Integrity key generation
    B. Integrity protection
    C. Encryption key generation
    D. Encryption

18. Where is encryption located in the UMTS stack of protocols?
    A. In Physical Layer and Media Access Control Layer
    B. In Media Access Control Layer and Radio Link Control Layer
    C. In Radio Link Control Layer and Radio Resource Control Protocol
    D. In Radio Resource Control Protocol and Higher Layers

19. In UMTS, the security mechanisms employed between the Mobile Station and the Radio Network Controller are responsible for:
    A. Sequence Number Management
    B. Encryption and Integrity Protection
    C. User Authentication
    D. Network Authentication

20. In LTE, the Home Subscriber Server has the following information:
    A. policy control and decision-making rules,
    B. IP address allocation for the UE,
    C. buffer of downlink data while the MME paging,
    D. information about the PDNs.

21. In LTE, E-UTRAN is the part of the whole system infrastructure responsible for the:
    A. radio access network
    B. circuit switch core network
    C. packet switch core network
    D. evolved packet core network

22. How many security levels has LTE?
    A. 5
    B. 4
    C. 3
    D. 2

23. The following component IS NOT a part of the RFID technology
    A. Transceiver – Tag Reader
    B. Transponder – RFID tag
    C. Antenna
    D. Infra Red Analog/Digital Converter

24. The EPCGen2 tag is
    A. A passive tag that allows just low-speed reading and sortation
    B. An Active tag that allows high-speed reading and sortation
    C. A passive tag that allows high-speed reading and sortation
    D. An Active tag that allows just low-speed reading and sortation

25. In RFID, the usual budget for implementation of the cryptographic primitives is:
    A. 100 – 200 gates
    B. 200 – 500 gates
    C. 500 – 1000 gates
    D. 200 – 2000 gates

Part II. Cryptographic Mechanisms (35%)

Candidate nr ___________________

PLEASE FILL IN AND DELIVER THIS PAGE

26. Which cipher is used in WEP? (3%)

____

27. How big can be the key in WEP? (4%)

____

28. What is the integrity check algorithm used in TKIP? (3%)

____

29. What is the input data for the integrity check algorithm used in TKIP? (6%)

____

30. Which cipher is used in RSN? (3%)

____

31. What is achieved by AES-CCMP? (6%)

____

32. The key derivation function used in LTE is HMAC. What is the definition of HMAC? (7%)

____

33. Which hash function is used in the key derivation function of LTE? (3%)

____

Part III. Protocols (15%)

Candidate nr ___________________

PLEASE FILL IN AND DELIVER THIS PAGE

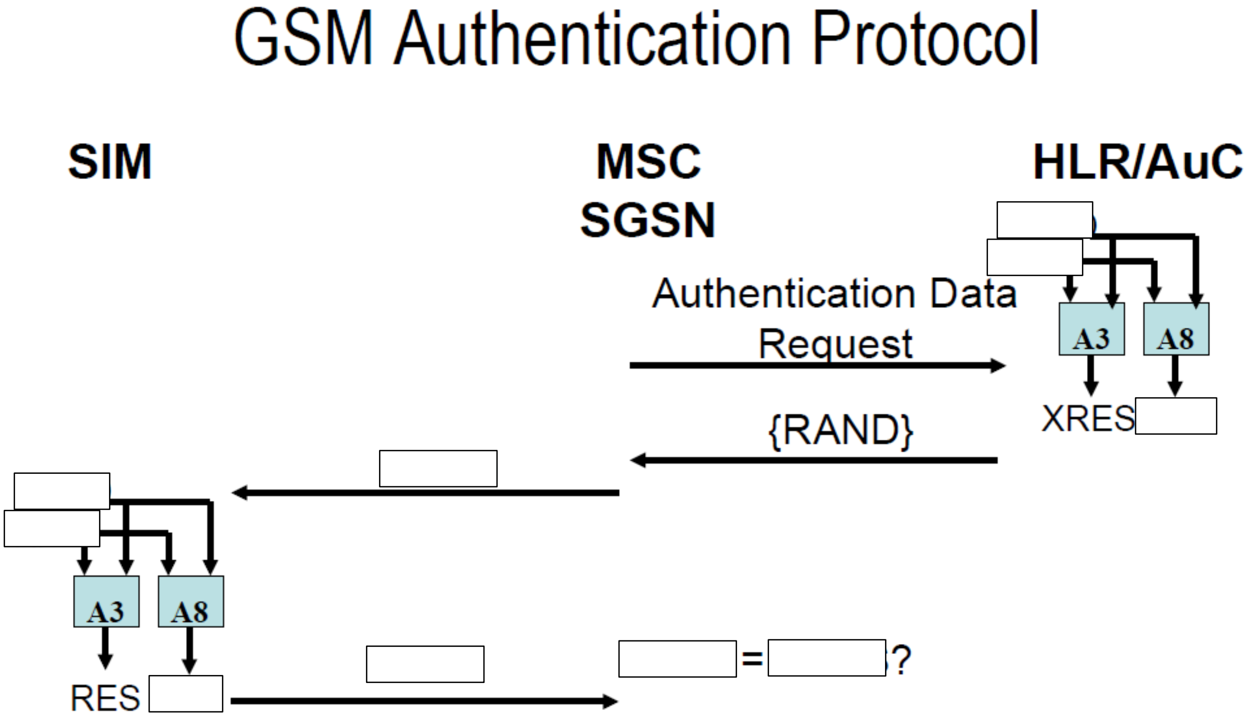
34. Name and characterize the main categories of protocol attacks, and rank them according to their capabilities. (5%)

    ____

    ____

    ____

35. Below is a figure of the GSM Authentication protocol where some crucial variables are missing in the blank boxes (one variable per box). Fill in the blank boxes with the correct variables in order the GSM Authentication protocol to be fully defined. (10%)



TTM4137 Exam Dec. 04, 2013 Solution Outline

Danilo Gligoroski

Part I. Wireless Networks Security Facts

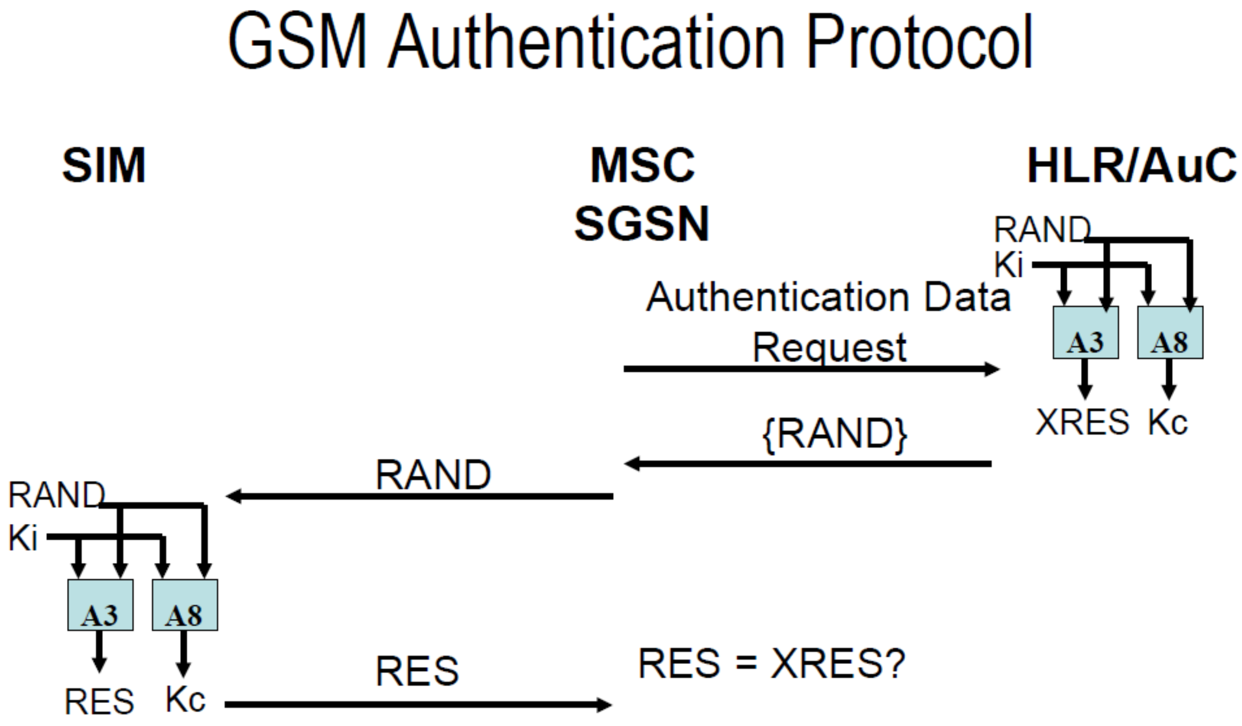
1b, 2d, 3c, 4b, 5a, 6d, 7c, 8a, 9a, 10d, 11b, 12a, 13c, 14c, 15b, 16d, 17b, 18b, 19b, 20d, 21a, 22a, 23d, 24c, 25d

Part II. Cryptographic Mechanisms (35%)

26. RC4,
27. 40 bits or 104 bits,
28. Michael
29. MIC Key, Transmitter address, Receiver address
30. AES
31. Data encryption with AES in Counter mode and Message Authentication with AES CBC-MAC Protocol.
32. $HMAC(K,m) = H((K \oplus opad) || H((K \oplus ipad) || m))$
33. SHA-256

Part III. Protocols (15%)

34. The attacker categories and the granularity of these may vary. For instance, in increasing capability order: Passive (readonly), Active (Modify message, Initiator, Responder, Man-in-the-middle with several sessions, ...), Insider games, Insider collusions.
35.


GSM Authentication Protocol
SIM
MSC
SGSN
HLR/AuC
RAND
Ki
A3
A8
Authentication Data Request
XRES
Kc
{RAND}
RAND
RAND
Ki
A3
A8
RES
Kc
RES
RES = XRES?