EXAM questions for the course TTM4137 - Wireless Security 29th November 2007 0900-1300 H

Part 1

This part consists of 20 questions. For every question 5 alternative answers are given, of which ONLY ONE is correct. If you chose the correct answer you will earn 2 points, otherwise you will loose 0.5 points (i.e. the penalty is -0.5 points). If you not choose any answer - then you will not get any points (i.e. the earned points are 0). The maximum number of points in this part of the exam is 40. Time for work on this test: 90 minutes.

1. Which wireless technology has only limited reliability according to the speed of the movement of the mobile equipment:
   a. GSM
   b. GPRS
   c. UMTS
   d. Bluetooth
   e. WiFi

2. Which wireless technology offers the highest transmission rates:
   a. GSM
   b. GPRS
   c. UMTS
   d. Bluetooth
   e. WiFi

3. What type of the attack is the attack guided by the following motivation: “The attacker wants to steal information, damage your system because of a grievance, or alter your system to acquire a tangible reward”:
   a. Profit or revenge
   b. Profit
   c. Revenge
   d. Gaming
   e. Ego

EXAM questions for the course TTM4137 - Wireless Security 29th November 2007 0900-1300 H

4. Which one of the following attacks is **NOT** classified as a wireless attack:
   a. Snooping
   b. Meet in the middle
   c. Modification
   d. Masquerading
   e. Denial of Service

5. What is **"one-time password"**?
   a. You use one unique password for all your logons and connections.
   b. Each and every time you logon or connect, you use a new password.
   c. You use passwords with a time stamp in them.
   d. A password that you use for generating the master key.
   e. A password that you use for generating the session key.

6. In the wireless communication terminology what the abbreviation MAC stands for?
   a. Message Authentication Code
   b. Media Access Control
   c. Mobile Authentication Code
   d. Medium Accessibility Coding
   e. Military Air Command

7. According to the IEEE 802 standard, what is the right ordering of the layers:
   a. MAC Layer, IP Layer, TCP Layer, LLC Layer, Application Layer
   b. MAC Layer, LLC Layer, IP Layer, TCP Layer, Application Layer
   c. LLC Layer, MAC Layer, IP Layer, TCP Layer, Application Layer
   d. LLC Layer, MAC Layer, TCP Layer, IP Layer, Application Layer
   e. MAC Layer, LLC Layer, TCP Layer, IP Layer, Application Layer

8. If a station moves only within BSS, then this type of mobility is known as:
   a. No transition mobility
   b. BSS transition
   c. Limited BSS transition
   d. ESS transition
   e. Limited ESS transition

9. If station or AP sends a notice for association termination, then that service is known as:
   a. Association
   b. Reassociation
   c. Disassociation
   d. Deassociation
   e. Quitassociation

10. The original 802.11 standard operated on the following frequencies:
   a. 2.4 GHz
   b. 2.4 – 5.0 GHz
   c. 900 MHz
   d. 1.2 GHz
   e. 900 MHz – 1.3 GHz

11. The maximal data rate per channel in the original 802.11 standard was:
   a. 54 Mbps
   b. 16 Mbps
   c. 11 Mbps
   d. 4 Mbps
   e. 2 Mbps

12. How many IVs are available in WEP?
   a. 2^{24}
   b. 2^{64}
   c. 2^{128}
   d. 0
   e. 24

13. What is true for WEP?
   a. Mobile station and the access point get a session key from the LAN
   b. Mobile station have a master key and produces a session key for the access point
   c. Mobile station sends a key to the access point
   d. Mobile station have a different key than the access point
   e. Mobile station shares key with access point

14. In Wi-Fi what is the **“gold standard”**?
    a. That was the first certification standard that came from Motorola.
    b. That was the second security standard that came from an alliance of hardware producers.
    c. The pin connection in the mobile equipment has to be made by gold.
    d. The pin connection in the mobile equipment has to be made by gold or silver.
    e. To obtain the Wi-Fi certification – the product has to be compatible with the set of “gold standard” products.

15. What encryption algorithm is used in WPA?
    a. RC4 with 40 bits key
    b. RC4 with 104 bits key
    c. AES with 128 bits key
    d. RC4 with 128 bits key
    e. AES with 256 bits key

16. What is the length of the user’s secret key in GSM technology?
    a. There is no such a security in GSM
    b. 56 bits
    c. 64 bits
    d. 96 bits
    e. 128 bits

17. In GSM, when a mobile is switched on, it registers its current location in a
    a. Authentication Centre
    b. Roaming Data Center
    c. Visitor Location Register
    d. Home Location Register
    e. Nearest Base Station

EXAM questions for the course TTM4137 - Wireless Security
29th November 2007 0900-1300 H

18. “Protect against someone tracking the location of the user or identifying calls made to or from the user by eavesdropping on the radio path” is the following GSM security feature:
    a. Encryption
    b. Handover
    c. Authentication
    d. Confidentiality
    e. Anonymity

19. In UMTS what kind of protection provides the “Protection mode 2” of MPSec?
    a. Both integrity protection and encryption.
    b. Just integrity protection.
    c. Just encryption.
    d. Just message authentication.
    e. No protection

20. What is the crucial protocol in IMS?
    a. DH key-exchange
    b. AuC protocol
    c. Session Initiation Protocol
    d. The Proxy CSCF
    e. The Interrogating CSCF

EXAM questions for the course TTM4137 - Wireless Security 29th November 2007 0900-1300 H

Part 2

This part consists of 8 questions all from one common topic. The maximum number of points for every correctly answered question is 5. Maximal number of points in this part of the exam is 40. Time for work on this test: 90 minutes.

TOPIC: UMTS

1. List all the cryptographic functions f0-f9 involved in UMTS and explain briefly what they are used for.
2. Explain with the help of a figure the authentication and key agreement protocol in UMTS.
3. What is the purpose of the sequence number SQN in the UMTS AKA protocol? The SQN for a certain user contains two concatenated parts: SQN=SEQ||IND. Describe three different ways of generating and maintaining the SEQ at the authentication centre (AuC).
4. What is the purpose of the operator-variant algorithm configuration field OP, used in the UMTS authentication and key generation algorithms? What is the purpose of OP_C? How is OP_C derived from OP?
5. What are the three modes of operation for the UMTS confidentiality algorithm? At what layer is the encryption performed with respect to these modes of operation?
6. How is the problem of re-usage of initialization values solved in the UMTS encryption algorithm?
7. How is the UMTS RRC (Radio Resource Control) layer signaling integrity protected? Why is integrity protection done at this layer?
8. Explain by the help of a figure how the UMTS integrity function is designed.

EXAM questions for the course TTM4137 - Wireless Security
29th November 2007 0900-1300 H

Part 3

This part consists of 4 questions all from one common topic. The maximum number of points for every correctly answered question is 5. Maximal number of points in this part of the exam is 20. Estimated time for work on this test: 60 minutes.

TOPIC: AD HOC ROUTING

1. What is the purpose of packet leashes? Explain, with the help of an example, the concept of geographical packet leashes.
2. What is an ActiveVCattacker, and why is this a particularly powerful attacker?
3. The ad hoc routing protocol ARAN (Authenticated Routing for Ad hoc Networks) uses certificates to authenticate routing messages, what are the advantages and disadvantages of using public key cryptography for this?
4. Explain, with the help of a figure, an example of route discovery in ARAN.