NTNU – Trondheim
Norwegian University of
Science and Technology

Department of Telematics

Examination paper for TTM4137 Wireless Security

Academic contact during examination: Stig F. Mjølsnes
Phone: 413 05 114
Examination date: December 17, 2015
Examination time (from-to): 9:00 – 13:00 (4 hours)
Permitted examination support material: Approved calculator. No printed text or handwritten notes permitted. (D).

Other information: The 33 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.

Language: English
Number of pages (front page excluded): 5 pages of questions, 1 answer page
Number of pages enclosed:

Informasjon om trykking av eksamensoppgave
Originalen er:
1-sidig ☐ **2-sidig** ☐
sort/hvit ☐ **farger** ☐

Checked by:

_____

Date Signature

TTM4137 Final Exam, Dec. 17, 2015

Part I. Wireless 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 purpose of the EAPOL 4-way handshake?
   a) Authenticated key agreement for session keys
   b) User authentication
   c) Negotiation of radio parameters
   d) Distribution of long term keys
2. How does WEP provide replay protection?
   a) By using a sequence counter
   b) By using an integrity check value
   c) By using a frame specific encryption key
   d) WEP does not provide replay protection
3. How many messages are exchanged in a group key handshake?
   a) 1
   b) 2
   c) 3
   d) 4
4. What are the five input values to the CCMP Decryption block?
   a) Key, Data, Nonce, PN, AAD
   b) Key, Data, Nonce, MAC1, MAC2
   c) Key, Data, Nonce, MIC, AAD
   d) Key, Data, Nonce1, Nonce2, IV
5. What is a mutable field in CCMP?
   a) A header field that is not integrity protected because it can be modified in transit
   b) A header field that is integrity protected because it will not be modified in transit
   c) A header field indicating if the frame has been modified in transit
   d) A header field that specifies whether or not a frame can be modified in transit
6. What is the major weakness in WEP, exploited by the PTW attack used in the lab?
   a) Weak IVs
   b) IV reuse
   c) Short encryption key
   d) Correlation between keystream and RC4 key
7. How are EAP messages transported between the authenticator and the authentication server in RSN?
   a) Encapsulated in EAPOL
   b) Encapsulated in RADIUS
   c) Encapsulated in 802.1X
   d) Encapsulated in TLS
8. Which frame types are cryptographically protected by 802.11i?
   a) Data frames only
   b) Data and Management frames
   c) Data and Control frames
   d) Data, Management and Control frames

9. Which standard actually enabled practical DoS attacks on 802.11i TKIP?
   a) 802.11e Quality of Service Enhancements
   b) 802.11h Spectrum and Transmit Power Management Extensions
   c) 802.11i MAC Security Enhancements
   d) 802.11k Radio Resource Measurement
10. Does Windows 10 Wi-Fi Sense allow sharing of 802.11i keys?
   a) No, Wi-Fi Sense only shares SSIDs
   b) No, Wi-Fi Sense only shares location information for open hotspots
   c) Yes, the PSK
   d) Yes, the PTK
11. Does Windows 10 Wi-Fi Sense enforce access control to wireless networks?
   a) Yes, by using 802.1X
   b) Yes, by using the Windows Filtering Platform on the client
   c) Yes, by transmitting an Access Control List to the AP
   d) No, Wi-Fi Sense does not enforce access control
12. Does GSM provide mutual authentication?
   a) Yes, but only between the SIM and the home network
   b) Yes, but only between the SIM and the visited network
   c) No, the SIM does not authenticate the network
   d) No, the network does not authenticate the SIM
13. How is backward key separation achieved during handovers over X2 connections in EPS?
   a) X2 handovers in EPS do not support backward key separation
   b) The target eNB receives a fresh key from the MME
   c) The source eNB securely deletes the key after transmitting it to the target eNB
   d) The source eNB applies a one-way function to the key before transmitting it to the target eNB
14. How is the EPS key derivation function constructed?
   a) AES-CBC
   b) AES-CCM
   c) HMAC-SHA256
   d) HMAC-MD5
15. How long are the cipher key (CK) and integrity key (IK) used in UTRAN, and how are they obtained if a GSM SIM is used to access a UTRAN?
   a) CK 128 bits, IK 128 bits, obtained using a conversion function
   b) CK 256 bits, IK 256 bits, obtained using a conversion function
   c) CK 128 bits, IK 128 bits, distributed from the AuC to the SIM
   d) CK 256 bits, IK 256 bits, distributed from the AuC to the SIM
16. What is cryptographic network separation (in EPS)?
   a) All network entities have separate cryptographic keys
   b) Communication between different core networks is protected by IPSec
   c) The cryptographic network is separated from the core network
   d) The derived keys are specific to the serving network
17. Which values are sent from the AuC to the VLR/SGSN during 3G/UMTS authentication?
   a) RAND, XRES, Kc, AUTN
   b) RAND, XRES, CK, IK, AUTN
   c) RAND, XRES, CK, IK, AK
   d) RAND, XRES, CK, IK, SQN

18. Which UMTS entities implement the functions f1-f5, f1* and f5*?
    a) UE and VLR
    b) UE and AuC
    c) USIM and VLR
    d) USIM and AuC
19. Why does EPS provide a more complex key hierarchy than UMTS and GSM?
    a) To support more cryptographic algorithms
    b) For backward compatibility with UMTS and GSM
    c) To support cryptographic key separation and enable more frequent key renewal
    d) To support other types of access networks
20. Will 3G USIMs work with EPS UE handsets?
    a) Yes, but only after a firmware update
    b) Yes, because the ME computes the EPS keys
    c) No, because USIMs do not support generation of EPS keys
    d) No, because EPS uses different AKA functions
21. Does EPID have a mechanism for key revocation?
    a) Yes, using a revocation list
    b) Yes, using the Online Certificate Status Protocol
    c) No, EPID does not need a mechanism for key revocation
    d) No, because the designers of EPID considered key compromise a low risk
22. What is the purpose of the EPID **join** procedure?
    a) To prove membership of a group
    b) To join a network
    c) To join two network messages into one
    d) To assign a private key to a device
23. Which three entities participate in the WPS configuration process?
    a) Supplicant, Authenticator, Authentication Server
    b) Enrollee, Access Point, Registrar
    c) Client, Access Point, Verifier
    d) Station, Authenticator, Registrar
24. How many messages are exchanged in the WPS in-band registration protocol?
    a) 2
    b) 4
    c) 6
    d) 8
25. Which protocol state will an 802.11 STA be in after having received a deauthentication notification message?
    a) State 1
    b) State 2
    c) State 3
    d) State 4

Part II. Mobile Network Security (35%)

26. Draw a message sequence diagram showing the UMTS AKA procedure. The diagram should show the protocol participants, the relevant parameters of each message, and the computations performed by the participants. Explain how the UMTS AKA procedure improves on the security of the GSM authentication procedure. (10%)
27. Describe how a false base station ("IMSI Catcher") can be used to compromise GSM security. (7%)
28. Is a UMTS network that also supports GSM vulnerable to the attack described in question 27? Explain your assumptions and reasoning. (7%)
29. Explain how the EPS/LTE AKA procedure improves on the security of the UMTS AKA procedure. (4%)

Recent research has shown that the TAU procedure in LTE is vulnerable to attacks. The TAU Request message sent from the UE to the network is integrity protected, but not encrypted. Certain types of TAU Reject messages sent from the network to the UE are not protected at all. One such unprotected message is the TAU Reject message "LTE service not allowed", which will tell the UE that LTE services in this area are not available.

30. Explain the security implications of unprotected TAU Reject messages in LTE. (7%)

Part III. Wireless Network Attacks (15%)

You have been hired by the company SecureCorp as a penetration tester. Your mission is to gain unauthorized access to their wireless network. SecureCorp uses an 802.11 network with CCMP and 802.1X authentication with PEAP. They have a single AP that all employees connect to. Employees of SecureCorp use their personal password to access the wireless network. According to the contract with SecureCorp, you are only allowed to launch attacks against their wireless network. Attacks against wired networks, social engineering through phone calls or e-mails and any other attack not directed at the wireless network are prohibited.

After an initial round of reconnaissance you conclude that SecureCorp has a strict software update policy. There are no software vulnerabilities in the employee's computers or network devices that you are able to exploit. Furthermore, you do not have access to a valid PEAP password. You have two laptops running Kali Linux, installed with the tools you have selected for the task.

31. How would you try to obtain a valid password to gain access to the wireless network? Explain the technical details of the attack, and explain your assumptions and reasoning. (5%)

Having successfully obtained a password, you are now able to access SecureCorp's wireless network. You decide that your next goal is to be able to eavesdrop on all the traffic between SecureCorps's wireless network and the wired network that the AP is connected to. Unfortunately, you were only able to obtain a single password, so you are not able to access the network as more than one user. You conclude that you have to exploit one or more protocol weaknesses to achieve your goal.

32. What kind of attack would you use to eavesdrop on all the network traffic? Explain the technical details of the attack, and explain your assumptions and reasoning. (5%)

You manage to eavesdrop on all the traffic and include evidence in the final report to SecureCorp. In your report, you also give recommendations for how to improve their wireless network security.

33. Given your successful attacks in 31. And 32., which technical recommendations would you give? (5%)

Dec. 17, 2015

EXAM TTM4137 – Answer sheet for Part I

MARK ONLY ONE ANSWER PER QUESTION

READ THE RULES BEFORE YOU START

Student Number →.....

In case of inkblots, request a new sheet.

Question	A	B	C	D		Question	A	B	C	D
1						14				
2						15				
3						16				
4						17				
5						18				
6						19				
7						20				
8						21				
9						22				
10						23				
11						24				
12						25				
13										