Part I. WLAN (40%)

1. Is the cipher RC4 a stream or a block cipher?
2. Cipher systems often use an initialization value or vector (IV). Why is IV used in WEP, and how is IV used in WEP?
3. The 802.11 MAC-frame with WEP is [Header | IV | KeyID | Data | ICV | CRC] Explain the receive process of this packet.
4. The intention of including the ICV was to enable message modification detection. Explain how this mechanism fails to detect a modification attack.

The IEEE 802.11i standard includes both the robust security network (RSN) and the transitional security network (TSN) specifications.

5. What are the components of the TSN architecture?
6. What is WPA and how does this relate to RSN?
7. Describe the pair-wise key hierarchy of RSN, how the keys are generated and where they are used.
8. How is the concept of access control modelled in the IEEE 802.1X standard?
9. Initially, the IEEE 802.1X was designed for controlling access from individual physical LAN ports, how is this translated into the wireless environment where a single physical access point may support multiple stations?
10. CCM mode of encryption was designed especially for use in RSN with AES, but is generally applicable as well. Describe the CCM mode.

Part II. UMTS (40%)

11. What is the quintuplet (denoted “quintet” in the book) of values sent from the HLR/AuC to the VLR/SGSN in the UMTS authentication protocol?
12. How is this quintuplet used between the VLR/SGSN and UE in the mutual authentication protocol? Illustrate this with a figure.
13. What happens when there is a failure in the synchronization of SQNs in the UMTS authentication process?
14. Explain by the help of a figure how the *f8* stream cipher based on KASUMI blocks is designed.
15. What is the purpose of the pre-whitening value *W* used in *f8*?
16. What is IMS and what are the three main components of the IMS security architecture?
17. What was the biggest problem when the 3GPP AKA was to be implemented in SIP, and how was this problem solved by the developers?

18. What are the three phases of a man-in-the-middle attack scenario on UMTS and GSM co-operation?

Part III. Bluetooth (10%)

19. What is pairing of two BT devices?
20. What is the maximal length of a pass-key in a BT system?
21. What is a fixed pass-key?
22. What are the two types of link keys in a BT system?
23. Which block cipher is used in the BT specifications?

Part IV. Wireless Ad Hoc Routing (10%)

24. Give three examples of routing-disruption attacks on ad hoc networks.
25. Explain the concept of “packet leashes”.
26. Sketch three general approaches for how one can set up symmetric keys in an ad hoc network, and list their advantages and disadvantages.

TTM4137 Wireless Security

Solutions to written exam December 11, 2006

Friday, December 22, 2006

1. Stream cipher.
2. IV is used in WEP to hide identical plaintext packets by selecting a new IV for each packet sent. The IV in WEP is a 24-bit public part of the RC4 cipher key of 64 or 128 bits.
3. The receiver verifies the CRC, notes that the WEP bit is set and therefore reads the IV value, the reads the keyID bits to select the correct key, append the IV, and initialize the RC4 with the resulting key, generate the RC4 pseudorandom sequence, decrypts by bitwise XOR. Finally, the ICV is computed on the cleartext and compared with the received ICV.
4. The ICV is a linear function of the data; hence flipped bits in the data ciphertext determine exactly which bits to flip in the ICV ciphertext.
5. IEEE 802.11i defines a transitional security network (TSN) in which both RSN and WEP systems can operate in parallel.
6. WiFi Protected Access (WPA) denotes the major Wi-Fi manufacturers intermediate security upgrade from WEP solution based on the capabilities of existing hardware. This led to the definition of the Temporal Key Integrity Protocol (TKIP). It is a optional subset of RSN.
7. See Figure 10.5 page 213 in Edney Arbaugh.
8. A supplicant connects to the network through a port. Each port is controlled by an authenticator, which again is associated with an authentication server.
9. The physical connection of a switched LAN hub is replaced with a logical connection formed by the wireless communications.
10. Figure 12.7 page 273 in Edney Arbaugh.
11. Q=(RAND, XRES, CK, IK, AUTN) where AUTN=SQN($\oplus$ AK)||AMF||MAC-A
12. See Figure 2.2 p. 32 in Niemi
13. The USIM generates a resynchronization token AUTS=SQN_USIM||MAC-S, where f1*(K,SQN_USIM, RAND,AMF*)→MAC-S and sends it to AuC. AuC checks if the next authentication quintet is ok for the USIM, if YES it generates fresh quintet and sends it to VLR/SGSN, if NOit calculates f1*(K,SQN_USIM, RAND,AMF*)→XMAC-S and checks if MAC-S=XMAC-S, if YES SQN_AuC is reset to SQN_USIM and a fresh quintet is generated and sent, if NO SQN_AuC is not reset, but a new quintet is sent anyway.
14. See Figure 6.3 p. 150 in Niemi
15. Protection against chosen plaintext attacks and collision attacks.
16. IMS is IP Multimedia CN Subsystem, a complete application layer system built on top of the UMTS PS domain, independent of underlying access technology. The three main components are:
    1. The IMS subscriber identity module (ISIM) that gives a permanent security context between the UE and the HSS
    2. IPsec ESP SAs that gives a temporary security context between the UE and the P-CSCF on the network side and authenticates each SIP message

3. Network domain security (NDS) that protects traffic between different network nodes

17. The problem was that 3GPP AKA is not password-based authentication, but HTTP Digest used in SIP is. The solution was to use RAND with AUTN as the nonce, and RES calculated from RAND as the password.
18. 1) Select the target's IMSI/TMSI. 2) Get a valid AUTN/RAND pair in active communication with the HLR/AuC. 3) Act as a base station towards the target and ask to turn of security.
19. Pairing is the initial authentication and key agreement procedure.
20. 128 bits.
21. The passkey is preset by the manufacturer.
22. Unit key and combination key.
23. SAFER+.
24. Black hole, grey hole, gratuitous detour, wormhole
25. Solution to the wormhole attack. A receiver can determine if a packet has traveled an unrealistic distance by a precise timestamp or location information combined with a loose timestamp
26. 1. Share them with each pair before deployment
    2. Resurrecting duckling
    3. If public keys already have been established, use a key-exchange protocol.

    -sfm

TTM4137 – Informasjonssikkerhet i mobilnett.
Eksamen 2007-08-07

Hjelpemidler: Ingen
Varighet: 0900 – 1300 (4 timer)

Del 1

Denne delen av eksamen består av 8 spørsmål fra ett felles tema. Maksimalt oppnåelig antall poeng for et korrekt svar er gitt for hvert enkelt spørsmål. Totalt antall poeng oppnåelig for denne delen er 40, og anslått nødvendig tidsforbruk for å besvare denne delen er 90 minutter.

Tema: WLAN

1. (6 poeng) Hvilke sikkerhetsmessige ulemper mener du eksisterer ved bruken av WEP (Wired Equivalent Privacy)?

2. (3 poeng) Forklar begrepet *nøkkelentropi*.

3. (3 poeng) Hva vil en angriper vanligvis oppnå ved å benytte et *ordboksangrep (dictionary attack)*?

4. (4 poeng) Forklar hovedtrekkene i RADIUS protokollen.

5. (7 poeng) Beskriv hvordan parvise nøkler for AES (Advanced Encryption Standard) i tellermodus (AES-CCMP) kan organiseres i et *nøkkelhierarki*.

6. (3 poeng) Hvordan kan en mobil enhet verifisere legitimiteten til et aksesspunkt?

7. (7 poeng) Beskriv fordeler og ulemper med bruken av Kerberos i et RSN (Robust Security Network)

8. (7 poeng) Hvordan benyttes TLS (Transport Layer Security) i forbindelse med EAP (Extensible Authentication protocol)?

TTM4137 – Informasjonssikkerhet i mobilnett.
Eksamen 2007-08-07

Del 2

Denne delen av eksamen består av 6 spørsmål fra ett felles tema. Maksimalt oppnåelig antall poeng for et korrekt svar er gitt for hvert enkelt spørsmål. Totalt antall poeng oppnåelig for denne delen er 40, og anslått nødvendig tidsforbruk for å besvare denne delen er 90 minutter.

Tema: UMTS-sikkerhet.

1. (7 poeng) Beskriv hovedtrekkene i UTRAN[1] kryptering.

2. (5 poeng) Hvilke(n) svakhet(er) introduseres dersom parameteren MASK gjenbrukes? Illustrer gjerne et eksempel.

3. (7 poeng) Hvilke trusler mot signaleringen i UTRAN mener du det er viktig å ta hensyn til?

4. (9 poeng) Forskjellige sikkerhetskrav imøtekommes av forskjellige kryptografiske algoritmer for autentisering og nøkkelforhandling (AKA) i UMTS. Lag en liste over de du mener er aktuelle, og gi en kort beskrivelse/forklaring av hver av dem.

5. (5 poeng) Hvorfor ble blokkchifferet Rijndael (AES) valgt som den anbefalte kjernen (kernel) i autentiseringsalgoritmene for UMTS?

6. (7 poeng) Lag en liste over angrep mot en MAC (Message Authentication Code) – algoritme, og drøft betingelsene og sannsynligheten for suksess for hvert enkelt angrep.

[1] UMTS Terrestrial Radio Access Network

TTM4137 – Informasjonssikkerhet i mobilnett.
Eksamen 2007-08-07

Del 3

Denne delen av eksamen består av 4 spørsmål. Maksimalt antall poeng oppnåelig for denne delen er 20, og anslått nødvendig tidsforbruk for å besvare denne delen er 60 minutter.

Tema: Sikkerhet i ad hoc nettverk

1. (5 poeng) Beskriv problemene med offentlig nøkkel revokasjon (public key revocation) i et trådløst ad hoc nettverk.
2. (7 poeng) Forklar virkemåten til en enveis hakkekjede (one-way hash chain).
3. (3 poeng) Navngi tre eksempler på ad hoc rutingprotokoller som benytter enveis hakkekjeder.
4. (5 poeng) Forklar virkemåten til et omdømmebasert system (reputation-based system) for ad hoc ruting.

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

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

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

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

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

KEY for Part 1

1. d
2. e
3. a
4. b
5. b
6. b Ambiguous question, more than one possible answer
7. b
8. a
9. c
10. a
11. e
12. a
13. e
14. e
15. d
16. e
17. d Ambiguous question, more than one possible answer
18. e
19. a
20. c

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

KEY for Part 2

TOPIC:

1. *f0: random challenge generation, f1: network message authentication, f1*: resynchronization message authentication, f2: user authentication, f3: cipher key derivation, f4: integrity key derivation, f5: anonymity key derivation, f5*: anonymity key derivation for resynchronization, f8: confidentiality, f9: integrity*
2. *See fig 2.1 and 2.2 in textbook*
3. *The purpose of SQN is to provide the user with proof that the authentication vector is fresh. The three ways of generating SEQ: 1. SEQ is an individual counter and its current value is maintained in a database independently for each user. 2. SEQ is based on a global counter, and for each user a deviation from the global counter, called DIF, is maintained in a database. 3. SEQ has two parts SEQ=SEQ1||SEQ2 where SEQ1 is an individual counter and SEQ2 is based on a global counter. The value of SEQ is maintained in a database for each user.*
4. *OP is there to provide separation between the functionality of the algorithms when used by different operators. OP_C is a subscriber-dependent value of OP, it is XORed to the input and output of the kernel functions, thus providing additional protection against attacks. $OP_C=OP \oplus E_K(OP)$*
5. *RLC transparent mode (MAC layer encryption), Unacknowledged mode (UM) (RLC layer encryption), Acknowledged mode (AM) (RLC layer encryption)*
6. *Part of the IV consists of a time-dependent counter COUNT-C. COUNT-C consists of a combination of the counter HFN (Hyper Frame Number) and a shorter counter that changes for each PDU (Connection Frame Number for MAC and RLC sequence number for RLC). HFN is set to zero whenever a new key is generated during AKA to avoid wrap-around.*
7. *MAC-I is computed with the f9 function at the sending side and appended to each RRC message. MAC-I is also computed at the receiving side and the result is checked against the bit string appended to the message. The signaling messages at the RRC layer are considered the most sensitive and important and are thus integrity protected, i.e. the encryption on/off message.*
8. *See fig 6.6 on p. 164 in textbook*

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.

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

KEY for Part 3

1. *Packet leashes are used to defend against wormhole attacks. Main idea: a receiver can determine if the packet has traveled an unrealistic distance. Geographical packet leashes: the receiver computes an upper bound on the distance between the sender and itself based on the timestamp t_s in the packet, the local receive time t_r, the maximum relative error in location information δ, and the locations of the receiver p_r and the sender p_s. $d_{sr} \leq ||p_s - p_f|| + 2v \cdot (t_r - t_s + \Delta) + \delta$. We assume sender and receiver's clocks are synchronized to within $\pm\Delta$ and that the maximum velocity of a node is v.*
2. *An attacker that owns all nodes on a vertex cut through the network, that partitions the good nodes into multiple sets. This is a powerful attacker because it controls all traffic between nodes of the disjoint partitions.*
3. *Advantages: no need to set up symmetric keys in network nodes, adding new nodes to the network is easy. Disadvantages: larger routing message size because of the need of adding certificates, computing overhead in verifying signatures, vulnerability to DoS attacks, the need of CA, certificate revocation problem*
4. *See figure 2 on p. 34 in the paper.*

English

Norwegian University of Science and Technology
Department of Telematics

EXAM IN
TTM4137 – WIRELESS SECURITY

Contact person: Professor Stig F. Mjølsnes. (Tel. 413 05 114).

Date of exam: December 1, 2008.

Time of exam: 9:00 – 13:00 (4 hours).

Date of grade assignment: December 22, 2008.

Credits: 7.5

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

Attachments:

- 7 pages of questions and 1 page for multiple choice answers.

The 40 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 not necessarily in your order of difficulty, so time your work and make sure you find time for all questions. We hope you will find Part II and III both enlightening and entertaining. Please make your best effort to write comprehensible, and with brief, concise and good answers. 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 gives 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. Which stream cipher is used for WEP encryption?
   a) AES
   b) DES
   c) RC4
   d) RC5
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 many messages are exchanged in the WEP shared key authentication protocol?
   a) 2
   b) 3
   c) 4
   d) 5
4. Is the same key used for both authentication and encryption in WEP?
   a) Yes
   b) No
   c) Yes, if 802.1X authentication is not used
   d) The same key is never used twice
5. What is an RC4 weak key value?
   a) A key value where many bits of the first bytes of the plaintext are leaked when an IV collision occurs
   b) A key value where a few bits in the key determine many bits in the first few bytes of the key stream
   c) A key value where a few bits in the key determine many bits in the cipher text
   d) A key value where the bits in the key determine the bits in the first few bytes of the key stream
6. Which cryptographic algorithm is used in counter mode with cipher block chaining message authentication code protocol (CCMP)?
   a) AES

b) Michael
c) RC4
d) TLS

7. Which three roles participate in the 802.1X access control protocol?

a) Station, authenticator and autentication center
b) Client, server and RADIUS server
c) Supplicant, access point and RADIUS server
d) Supplicant, authenticator and authentication server

8. How many EAP-TLS messages are exchanged in an EAP-TLS handshake?

a) 2
b) 4
c) 9
d) It varies with the TLS parameters exchanged

9. What encapsulates EAP messages in RSN?

a) They are encapsulated in TCP/IP
b) They are encapsulated in EAPOL messages
c) They are encapsulated in RADIUS messages
d) They are encapsulated in EAPOL and RADIUS messages

10. Does EAP-SIM provide mutual authentication?

a) No, it uses the regular GSM authentication
b) Yes, by the regular GSM authentication and the authentication token from the AuC
c) Yes, by the regular GSM authentication and a nonce in the encrypted AP response
d) Yes, it uses the regular UMTS authentication

11. What is the purpose of the EAPOL 4-way handshake?

a) To compute a fresh pairwise temporal key (PTK) from the pairwise master 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

12. How long is the IV used in TKIP?

a) 24 bits
b) 48 bits
c) 64 bits
d) 128 bits

13. What is the key size of AES as used in RSN?
    a) 128 bits
    b) 192 bits
    c) 256 bits
    d) 512 bits
14. What is the block size of AES as used in RSN?
    a) 64 bits
    b) 128 bits
    c) 256 bits
    d) 512 bits
15. Is the complete MAC PDU encrypted by the CCMP?
    a) Yes, the CCMP uses a shared key
    b) No, the MAC header is not encrypted
    c) No, the CCMP header is not encrypted
    d) No, the MAC header and the CCMP header are not encrypted
16. Which GSM entities store the secret user keys K_i?
    a) MS and HLR
    b) VLR and AuC
    c) SIM and AuC
    d) SIM, BS and VLR
17. What is the output of the GSM authentication function A3?
    a) MAC (32-bit message authentication code)
    b) MAC (64-bit message authentication code)
    c) SRES (32-bit signed response)
    d) SRES (64-bit signed response)
18. Which authentication data does the GSM VLR have to request?
    a) The authentication quintet (RAND, AUTN, XRES, CK, IK)
    b) The authentication quintet (RAND, AUTN, XRES, K_i, K_c)
    c) The authentication triplet (RAND, XRES, K_i)
    d) The authentication triplet (RAND, XRES, K_c)
19. What are the variables of the authentication token (AUTN) used in UMTS networks?
    a) $SQN \oplus AK$, XRES, MAC
    b) $SQN \oplus AK$, AMF, MAC
    c) SQN, AMF, MAC, RAND
    d) $SQN \oplus AK$, AMF, MAC, RAND

20. Which UTRAN layer provides integrity protection?

    a) MAC layer
    b) RLC layer
    c) RRC layer
    d) Physical layer

21. What happens if the result of the UTRAN algorithm negotiation is that the user equipment (UE) and network have no integrity protection algorithms in common?

    a) The network may establish the connection without integrity protection
    b) The connection is shut down immediately by the network
    c) The network may establish the connection with the default integrity protection algorithm
    d) UTRAN does not use integrity algorithm negotiation

22. How is the traffic between the terminal equipment and Proxy CSCF (P-CSCF) protected in IMS?

    a) Using the UMTS f8 encryption algorithm with the cipher key CK
    b) Using IPsec Authentication Header (AH)
    c) Using IPsec Encapsulated Security Payload (ESP)
    d) It is not protected at all, but the UTRAN radio link is protected by the UMTS security mechanisms

23. Which authentication method is used by IMS?

    a) Internet Key Exchange (IKE)
    b) IPsec Authentication Header (AH)
    c) IPsec Encapsulated Security Payload (ESP)
    d) UMTS Authentication and Key Agreement (AKA)

24. What is the length of the cipher key CK used in UMTS?

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

25. Which UMTS entities implement the functions f1-f5, f1* and f5*?

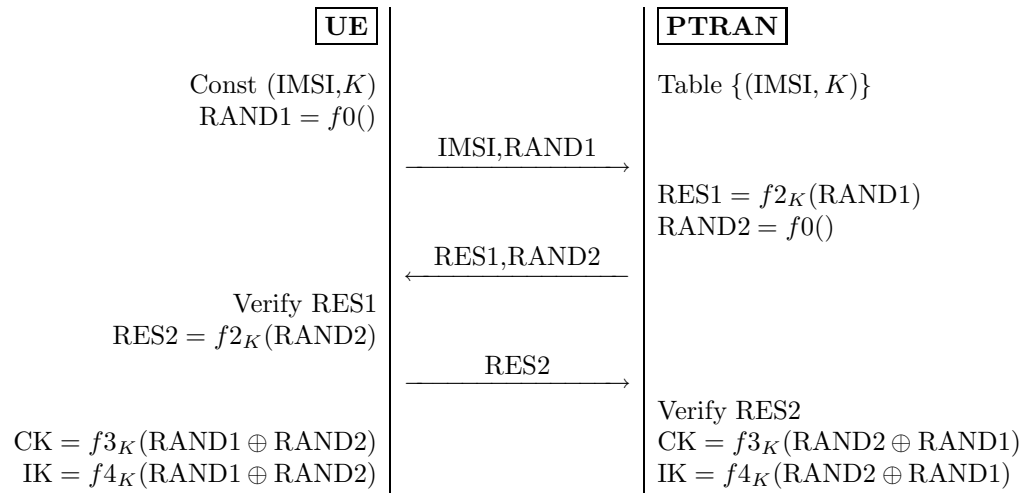
    a) USIM, UE and BS
    b) SGSN and AuC
    c) USIM and AuC
    d) USIM, BSC and AuC

Part II. Authentication Protocols (30%)

As the communication systems security engineer in Telematics Inc. you are responsible for the design of an authentication protocol between mobile equipment UE and a new radio access network PTRAN being developed. You start thinking about the problem by recalling the UMTS Authentication and Key Agreement protocol, denoted $\mathcal{U}$ here.

26. Draw a message sequence diagram of $\mathcal{U}$ that shows how the authentication and session key generation take place between the user equipment UE and the radio access network UTRAN. Show how the message variables are computed and communicated. (5%)

Having finished your recollection of UMTS, a new protocol proposal $\mathcal{P}$ arrive on your desk for your analysis. The cryptographic functions are the same as in UMTS. Here is $\mathcal{P}$:



27. Compared to $\mathcal{U}$, which new function do you find must be implemented in UE for $\mathcal{P}$? Propose how this function can be implemented.(5%)

28. All variables in $\mathcal{P}$ er 128 bits except IMSI. What is the difference between $\mathcal{U}$ and $\mathcal{P}$ with respect to the number of bits communicated?(5%)

29. Make an analysis of $\mathcal{P}$ and try to identify at least two security weaknesses not present in $\mathcal{U}$. What are the weaknesses?(5%)

30. What is the basis for your claim that the generation of (CK, IK) is better in $\mathcal{P}$ than in $\mathcal{U}$?(5%)

31. Propose how $\mathcal{P}$ can be modified in order to avoid the security problems you identified in Question 29.(5%)

Part III. Analysis of Cipher Initialization Implementation (20%)

You are conducting an experiment in wireless network security. Using the aircrack-ng tool suite, you try several different attacks on a Cisco access point (AP) configured with Wired Equivalent Privacy (WEP). While running an ARP replay attack with 682 captured data frames per second, the total number of unique initialization vectors (IVs) observed seems to reach a maximum value of approximately 1 040 000 after about two hours. Your lab journal table is reproduced below. It shows the number of minutes the ARP replay attack has been running and the total number of unique IVs observed with time. After 140 minutes, it seems like you are not able to obtain any more unique IVs from the AP.

Minutes	Unique IVs observed
2	76 874
23	629 428
30	727 198
40	824 629
50	896 612
60	945 423
80	1001 550
100	1026 429
120	1038 326
140	1043 822

Table 1: The accumulated number of different IVs observed with time.

32. What is the purpose of the IV in WEP? (2%)
33. Name at least two different methods of IV value generation.(2%)
34. What is the security problem with a fixed value for IV?(2%)
35. How is the size of the set of IV values in the WEP specification? (2%)
36. How does this relate to the observations in your experiment as shown in Table 1?(2%)

The observations in your experiment are not what you expected, so you repeat it several times but get similar results. You search for an explanation and decide on a hypothesis based on your observations. Since the increase in the number of unique IVs observed is close to the number of captured data frames in the first few minutes of the experiment, and then gradually decreases until it is close to zero after approximately two hours, you assume that the IVs are picked randomly. But the total number of different IVs observed is lower than expected.

37. Based on the description above, state your hypothesis about the number of possible IV values in use by this AP. Explain how you found the result.(2%)

Fortunately, a mathematical friend of yours is familiar with a problem from probability theory that applies to this experiment, the general birthday problem. This problem states that when n values are selected, with replacement, from a total population of m values, the expected number of *unique* values observed is

$$E(m, n) = m(1 - (1 - 1/m)^n).$$

In the experiment, m represents the total number of possible IV values, and n represents the number of data frames captured, hence $E(m, n)$ represents the expected number of unique IV values observed.

38. Add two new columns for Table 1 and make the following computations. The first new column should show the expected number of unique IVs observed under your hypothesis at 100, 120 and 140 minutes. The second new column should show the expected number of unique IVs observed using WEP with random IV selection at 100, 120 and 140 minutes.(3%)

39. Create a plot of the experimental data and the two new columns described above at 100, 120 and 140 minutes.(2%)

As a final step, you decide to have a look at the actual IVs from your capture file. Table 2 shows 25 IVs from your experiment, one IV per line and in binary format.

011100100101011011010110
011101110010100010101000
011011100100110001011100
011011010010001110001100
001111000000100101110100
001111000010000100011010
011100000000000111100000
011001100100010101110010
011101110000111011101110
011010100001110011100110
011111010100100110100110
001011110110010101101010
011101110010101010000000
011010100101111111101010
011001110010000001011110
001000010001111011100010
001011110001011100000100
001111100110011000110010
001100100001110110101010
001000000011010101011000
011110110100100011100100
011010010111100100010000
001001100100100000001100
011100110111011010100110
011010100111000101011100

Table 2: A sample of captured IVs

40. Does the data in Table 2 support your hypothesis? Explain why/why not. What new information can you find by looking at the actual IVs in Table 2?(3%)

TTM4137 Exam Dec. 1, 2008
Solution Outline
Dec. 20, 2008

Part I. Wireless Networks Security Facts

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

Part II. Authentication Protocols

26. See Figure 2.1, 2.2, 2.3 and 2.4 in the UMTS book page 31-35.
27. A random generator $f0()$ assigning value to RAND1. $f0()$ can be a pseudo-random generator seeded by the key and a time value.
28. We assume all variables are 128 bits long, the lenght of IMSI cancels out in computing the difference. P's first message includes the RAND1 extra, so P communicates 128 bits more than U.
29. This and question 31 are the hard "A" questions of this exam.
1) Chosen plaintext attack by RAND1 on $f2_K()$ cannot be done in U.
2) There is no cryptographic binding between RES1 and RAND2, this makes it possible to use the first "half" transcript from one session and the other "half" of the exchange from another session.
3) Traceability of sessions to the same subscriber because no use of temporary identity (TMSI) is indicated.
4) The access network (TRAN) can control the values of CK and IK. For instance, selecting RAND2 = RAND1 result in $f_K(0)$. A better solution is some nonlinear combination of RAND1 and RAND2.
30. The session keys CK and IK are now generated with input from both parties. For instance, if RAND1 is kept constant, randomization of RAND2 will ensure proper randomization of the key generation.
31. This question depends on the answer to question 29 and is open to creative ingenuity. Of course, one method is the U protocol. Another method is along the ISO 9798-2 "three-liner" presented in the lecture Sep 5, but this requires decryption at UE, and verification at AuC.

UE $\rightarrow$ TRAN: IMSI, RAND1
UE $\leftarrow$ TRAN: E_K(RAND1,RAND2, "AuC")
UE $\rightarrow$ TRAN: E_K(RAND2, RAND1)

Part III. Analysis of IV implementation

32. The requirements are:
1) The main key is fixed and used directly in WEP.
2) MAC-frames should be cryptographically self-contained at the receiver side.
3) The RC4 key must vary with each frame because the keystream must never be used twice.
Solution: An IV variable generated for and carried by each frame.
33. Truly random, pseudorandom, counter, fixed, or a combination.
34. See Item 3 in 32. Fixed IV $\Rightarrow$ fixed cipherkey $\Rightarrow$ all frames will be encrypted with the same key stream. Known plaintext attack will reveal the key stream. If an attacker obtains this key stream, all traffic can be decrypted without knowing the key value.
35. $2^{24} = 16,777,216$ values.
36. Only 1 million out of 16 million values have been observed, still the remaining unobserved values are becoming scarce.
37. Hypothesis: There is $\log_2(1043822) = 19.99344428$ approximately 20 bits

of entropy in the IV.
38. See Table 1
39. See Figure 1
40. Yes, this information supports the hypothesis. Four of the bits (position 1, 3, 9 and 24 counting from the left) are constant, the remaining 20 are variable bits in the IV.

Elapsed Time (minutes)	# Data	$E(X)$ 2^{20} IVs	$E(X)$ 2^{24} IVs
2	76 874	78 728	81 641
23	629 428	621 216	915 248
30	727 198	723 371	1 183 763
40	824 629	828 447	1 559 491
50	896 612	899 573	1 926 165
60	945 423	947 717	2 284 003
80	1 001 550	1 002 364	2 974 022
100	1 026 429	1 027 403	3 631 189
120	1 038 326	1 038 875	4 257 069
140	1 043 822	1 044 131	4 853 150

Table 1: Observed number of unique IVs and expected number of unique IVs

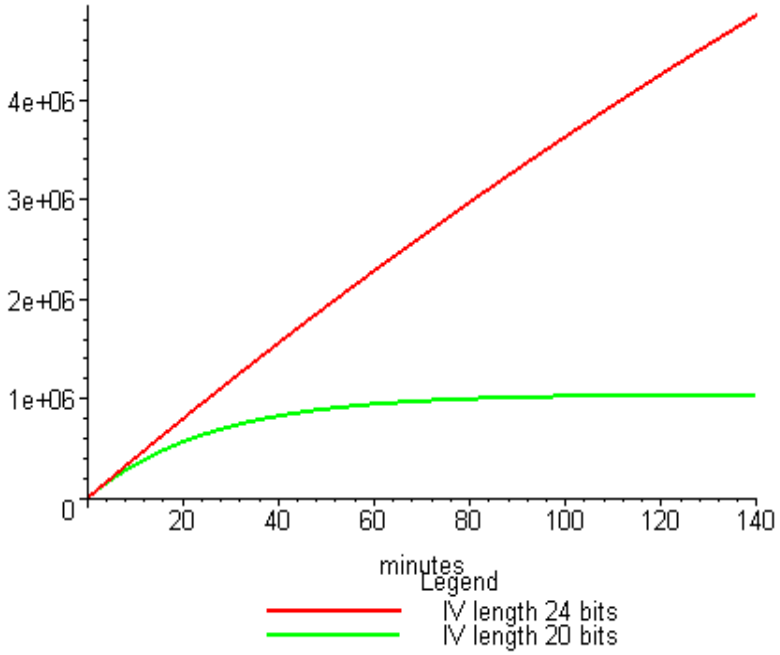


Figure 1: The expected number of new IVs as a function of elapsed time in minutes.

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 gives 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. Is the same key used for both authentication and encryption in WEP?
   a) Yes
   b) No
   c) Yes, if 802.1X authentication is not used
   d) The same key is never used twice
2. How does WEP detect replay?
   a) There is no replay detection
   b) By the intialization vector (IV)
   c) By the integrity check value (ICV)
   d) By the random nonce value (RNV)
3. How long is the IV used in TKIP?
   a) 24 bits
   b) 48 bits
   c) 64 bits
   d) 128 bits
4. Which protocol encapsulates the EAP messages transported between the supplicant and authenticator in WPA/RSN?
   a) EAP-TLS
   b) EAPOL
   c) 802.11
   d) 802.1X
5. What is the purpose of the first phase of PEAP?
   a) The supplicant provides the identity to the authentication server
   b) The supplicant and authentication server negotiate the EAP method to be used
   c) The supplicant encrypt and communicate the password to the authenticator
   d) Supplicant establishes an authenticated secrecy channel to the authentication server
6. Which 802.11 frame type is cryptographically protected by the 802.11w standard?
   a) Management frames
   b) Control frames
   c) Data frames
   d) Beacon frames

7. 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 the concatenation of flag/priority bits, packetnumber, source-address, and a constant
   d) By source address, destination address and the MIC value of the MPDU
8. What is the key size of AES as used in RSN?
   a) 128 bits
   b) 192 bits
   c) 256 bits
   d) 512 bits
9. Does EAP-SIM provide mutual authentication?
   a) No, it uses the regular GSM authentication
   b) Yes, it uses the regular UMTS authentication
   c) Yes, by the regular GSM authentication and the authentication token from the AuC
   d) Yes, by the regular GSM authentication and a nonce in the encrypted AP response
10. What is the purpose of the EAPOL 4-way handshake?
    a) To exchange a fresh pairwise temporal key (PTK) from the pairwise master key (PMK)
    b) To exchange a fresh pairwise message key (PMK) from the pairwise transient key (PTK)
    c) To exchange a fresh pairwise transient key (PTK) from the pairwise master key (PMK) with bilateral key agreement and group key transfer
    d) To exchange a fresh pairwise message key (PMK) from the pairwise trusted key (PTK) generated in the 4-way key agreement including group key distribution
11. What are the four types of EAPOL messages used in WPA/RSN?
    a) Start, Key, Packet, Logoff
    b) Request, Authenticate, Result, Stop
    c) Identity, Challenge, Response, Accept
    d) Logon, Name, Password, Logoff
12. What is the purpose of the sequence number (SQN) used in 3G/UMTS networks?
    a) The USIM can detect replay of authentication messages
    b) The VLR/SGSN can detect replay of authentication messages
    c) The UE can verify the MAC values by using $f1$
    d) The HLR/AuC can generate distinct session keys
13. List the message authentication code types used in UMTS
    a) MIC, MAC
    b) MAC-A, MAC-I, MAC-S

c) IK, AK

d) AUTN, AUTS

14. What are the three most important security services in GSM?

a) User authentication, radio channel confidentiality, and temporary identities

b) Subscriber Identity Module, Visiting Location Register, and Authentication Centre

c) User identification, end-to-end encryption, and symmetric key exchange

d) The cryptographic algorithms A3, A5 and A8

15. What are the variables of the authentication token (AUTN) used in UMTS networks?

a) $SQN \oplus AK$, XRES, MAC

b) $SQN \oplus AK$, AMF, MAC

c) SQN, AMF, MAC, RAND

d) $SQN \oplus AK$, AMF, MAC, RAND

16. Which UTRAN 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

17. Which UTRAN layer provides integrity protection?

a) MAC layer

b) RLC layer

c) RRC layer

d) PHY layer

18. What is a call session control function (CSCF)?

a) A SIP server or proxy used in IMS

b) A Mobile Switching Centre (MSC) with IMS support

c) A GPRS Support Node (GSN) with IMS support

d) A Real-time Transport Protocol (RTP) session controller used in IMS

19. What is the length of the cipher key CK used in UMTS?

a) 56 bits

b) 64 bits

c) 128 bits

d) 256 bits

20. How many rounds does the KASUMI cipher use?

a) 8

b) 10

c) 12

d) 16

21. What kind of cipher is KASUMI?

a) Stream cipher

b) Feistel cipher

c) Substitution-permutation cipher

d) Nonlinear feedback shiftregister cipher

22. Why is the UICC normally easily removable from the mobile station?

a) The USIM holds an expiration date and, like credit cards, must be replaced

b) The failure rate of the integrated circuit cards (UICCs) are high because the issuers (mobile operators) want to optimize cost against subscription duration

c) End-to-end UMTS key-card plugs into the USIM slot for key distribution and management

d) The UE manufacturing and lifecycle can be managed independently from the personalization and subscription process

23. Why must the USIM implementation be tamper-proof?

a) To facilitate the mobile operator with secure computation and storage at the UE side

b) To protect the proprietary crypto-algorithms of the mobile operator

c) To protect the subscriber against unauthorized modification of the subscription parameters

d) To provide the subscriber with a PIN-protected access to the UMTS service

24. How is a oneway hash function useful in digital forensic investigations?

a) For fast recognition of known file content

b) For reconstructing the hash tables of deleted files

c) For juridical determination of incriminating file content

d) For legally sound presentation of the digital evidence

25. What are the purpose of the MILENAGE functions in UMTS?

a) Block cipher family of functions that build the algorithms for integrity code and the encryption process

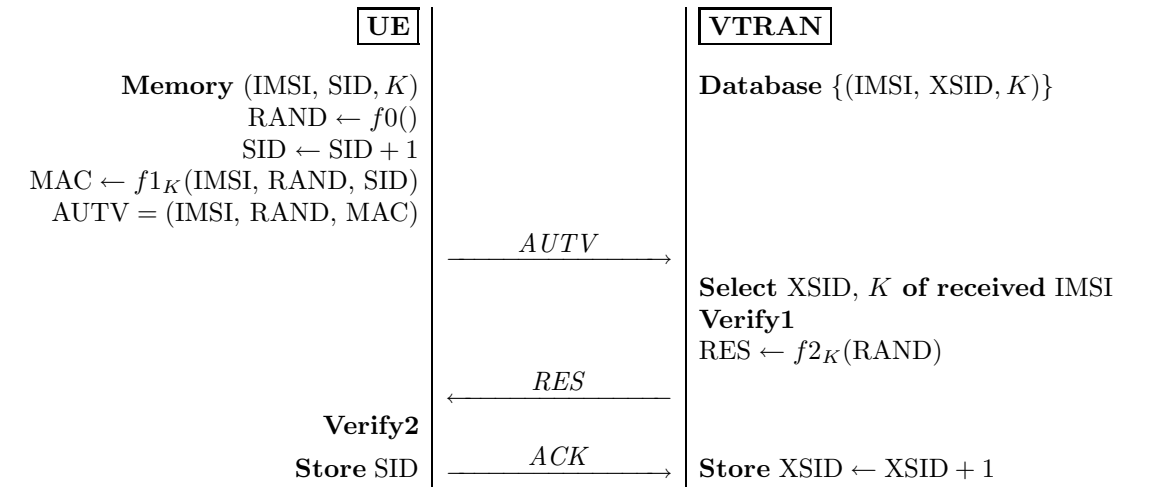
b) Transformation of keys for the inter-operation of GSM and UMTS basestations and networks

c) Pseudorandom generators that output the initializing values for the cryptographic computations

d) Algorithms for computing the cryptographic variables needed in the mutual authentication protocols

Part II. Authentication Protocols (35%)

As head of the communication security team in Telematics Inc. you are responsible for the design of the authentication protocol between mobile equipment UE and a new radio access network VTRAN being developed. You and your team start thinking about the problem by recapitulating the UMTS Authentication and Key Agreement protocol, denoted $\mathcal{U}$ here. Soon you have constructed a new and promising protocol proposal $\mathcal{V}$ to be analyzed. You want to use the same cryptographic functions as in UMTS. Here is $\mathcal{V}$:



Here in $\mathcal{V}$, the SID, XSID (session identifier) and MAC values are 64 bits each, ACK is 1 bit, and the rest of the parameters are each 128 bits.

26. Specify the procedure of the **Verify1** step on the VTRAN side, and the procedure of the **Verify2** step on the UE side. (10%)

27. Which new functions, compared to $\mathcal{U}$, do you find must be implemented for $\mathcal{V}$? Propose how these functions can be implemented.(5%)

28. Calculate the number of bits in the message exchange of $\mathcal{V}$, and compare this to $\mathcal{U}$.(5%)

29. Now refine the structure of the VTRAN into the Radio Access part (BST/RNC), the Visited Network, and the Home Network. Specify how you will enhance the protocol $\mathcal{V}$ to provide encryption and integrity keys that can be used to set up a secure channel between UE and RNC. (5%)

30. You foresee that the SID and XSID values will not remain properly synchronized under all error conditions. Specify how you will solve this problem of re-synchronization. (10%)

Part III. WEP Cryptanalysis (15%)

Shannon proposed to measure the amount of information using the concept of entropy. Here we will use the word *uncertainty*. Let $x_0, ..., x_{n-1}$ be n the possible values for a random variable X. Let $p_i = \Pr[X = x_i]$, for instance p_{42} is the probability that $X = x_{42}$. The uncertainty associated with the random variable X is defined as

$$H(X) = -\sum_{i=0}^{n-1} p_i \log_2 p_i \ .$$

The uncertainty is measured in bits, is a real number and can be smaller than 1. If the variable X is transmitted using $R(X)$ bits then the *redundancy* of this coding is defined as

$$D(X) = R(X) - H(X) \ .$$

Informally, $D(X)$ is the amount of wasted bits used to transmit X, because in theory X can be transmitted with $H(X)$ bits using the best possible lossless compression.

In cryptanalysis, the redundancy of the ciphertext, as a random variable X, may be used to extract the information about the secret key K. The *unicity distance* is the number of observations of X needed to uniquely determine K. It is defined as

$$U = \frac{H(K)}{D(X)} \ .$$

The formula can be roughly understood as follows. Every new observation of X leaks $D(X)$ bits of information about the key K, and thus decreases our original uncertainty $H(K)$ by $D(X)$ bits.

In WEP, the packet key is constructed as IV||Rk. Klein has derived a probabilistic relation between the first byte Rk[0] of the root key and the values of IV and the keystream byte Ks[2]:

$$\Pr\left[\underbrace{\mathrm{Rk}[0]}_{k} = \underbrace{S_3^{-1}[\,3 - \mathrm{Ks}[2]\,] - (S_3[3] + j_3)}_{X}\right] \approx \frac{1.36}{256} \ ,$$

where S_3 and j_3 are internal variables of RC4 that can be computed from the IV. With the introduced notation for the key byte k and the variable X we can write

$$p_k = \Pr[\,X = k\,] \approx \frac{1.36}{256} \ . \tag{1}$$

We also assume that the variable X takes on all of the other 255 values with equal probability

$$p_i = \Pr[\,X = i\,] = \frac{1 - p_k}{255}, \text{ for all } i \neq k \ . \tag{2}$$

31. When a byte variable X is assigned a random value, in other words sampled from the uniform probability distribution over $\{0, 1, ..., 255\}$, what is the probability that X takes on the value 42? Calculate the uncertainty $H(X)$.(3%)

32. Now we skew the probability distribution of X slightly. For some fixed value k, the probability that X takes the value k is given in Eq. 1 and the probability for each of the other values is given by Eq. 2. Calculate the uncertainty $H(X)$ for this probability distribution.(3%)

33. The byte variable X defined in Question 32 is transmitted using 8 bits. Calculate the redundancy $D(X)$.(3%)

34. An attacker sniffs ARP packets (known plaintext) transmitted in a wireless network that is secured by WEP. Calculate the number of observations of *distinct* IVs needed to recover uniquely the first byte Rk[0] of the network root key.(3%)

35. From the generalized birthday problem we know that when n values are randomly selected, with replacement, from a domain of m values, the expected number of *distinct* values observed is

$$E(m,n) = m\left(1 - \left(1 - \frac{1}{m}\right)^n\right) \quad .$$

Let us apply this to WEP packet sniffing where the IV values are chosen at random. Then m represents the total number of possible IV values, and n represents the number of ARP packets captured, hence $E(m,n)$ represents the expected number of *distinct* IV values observed. Calculate the total number of ARP packets that should be captured such that the expected number of distinct IVs equals the number obtained in Question 34.(3%)

TTM4137 Exam Dec. 4, 2009 Solution Outline

sfm, Dec. 16, 2009

Part I. Wireless Networks Security Facts

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

Part II. Authentication Protocols

26.

Procedure Verify1
XMAC $\leftarrow f1_k$(IMSI,RAND,XSID)
if MAC $\neq$ XMAC **then** send(ERROR)
else ...

Procedure Verify2
XRES $\leftarrow f2_K(RAND)$
if RES $\neq$ XRES **then** send(ERROR)
else send(ACK)

27. At the UE side: the random generator function $f0()$ and the Verify2 procedure. At the VTRAN side: The Verify1 procedure.

28. $|\text{AUTV}| + |\text{RES}| + |\text{ACK}| = (128 + 128 + 64) + 128 + 1 = 449$ bits. $|\text{IMSI}|+|\text{AUTN}|+|\text{RAND}|+|\text{RES}|+|\text{ACK}| = 128+128+128+\text{range}[32 \cdots 128]+1 = \text{range}[417 \cdots 513]$ bits.

29. For example, the key distribution proocol of UMTS can be used, see Fig.2.1 and 2.15 in the text book.

30. VTRAN will detect XMAC≠MAC, but VTRAN cannot determine the cause of the error without more information. If the SID value is included in AUTV then VTRAN are able to determine whether the error is caused by SID≠XSID, and initiate a resynchronization protocol. The resynchronization procedure can, for example, take the idea of AUTS in Figures 2.6 and 3.11 of the text book. Sections 2.1.1.3, 2.1.1.4 and 2.1.1.5 describe the design in UMTS.

UE $\rightarrow$ VTRAN:	(IMSI,RAND, SID$\oplus$AK, MAC-S)
UE $\leftarrow$ VTRAN:	(XSID$\oplus$AK, MAC-S)
UE	If MAC-S ok then resynch SID.

Part III. Analysis of IV implementation

31. $p_{42} = 2^{-8}$. $H(X_u) = 2^8 \cdot 2^{-8} \log_2 2^8 = 8$.

32. $p_k = \frac{1.36}{256} = 0,0053125$. $H(X_s) = p_k \cdot \log_2 \frac{1}{p_k} + 255 \frac{1-p_k}{255} \log_2 \frac{255}{1-p_k} = 0.0401433 + 7.9595273 = 7.9996707$

33. $D(X) = H(X_u) - H(X_s) = 0.0003293$

34. $U = \lceil 8/0.0003393 \rceil \frac{\text{bits}}{\text{bits/value}} = 24294$ values

35.

$$n = \lceil \frac{\ln(1 - 24294 \cdot 2^{-24})}{\ln(1 - 2^{-24})} \rceil = 24314$$

English

Norwegian University of Science and Technology
Department of Telematics

EXAM IN
TTM4137 – WIRELESS SECURITY

Contact person: Professor Stig F. Mjølsnes. (Tel. 413 05 114).

Date of exam: December 3, 2010.

Time of exam: 9:00 – 13:00 (4 hours).

Date of grade assignment: January 4, 2011.

Credits: 7.5

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

Attachments:

- 8 pages of questions,
- 1 page for multiple choice answers 1-25,
- 1 page for answer to 26.

The 38 exam questions and problems are divided into three parts, where each part is assigned an evaluation weight percentage of the total. I hope you will find Part II and III enlightening and maybe even entertaining as you work through these. 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. 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 gives 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. Is the same key used for both authentication and encryption in WEP?
   a) Yes, if 802.1X authentication is not used
   b) The same key is never used twice
   c) No
   d) Yes
2. What is the major weakness in WEP, exploited by the PTW attack used in the lab?
   a) Too short IV
   b) No protection against message replay
   c) The integrity check value
   d) The IV is part of key stream
3. What is EAP
   a) Extensible Authentication Protocol is a set of encapsulation messages for mutual authentication methods
   b) Extensible Authentication Protocol is a set of encapsulation messages for smartcard-based authentication methods
   c) Extensible Authentication Protocol is a set of encapsulation messages for upper-layer authentication methods
   d) Extensible Authentication Protocol is a set of authentication server methods
4. 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
5. Which security method is used in the first phase of PEAP?
   a) TLS
   b) EAPOL
   c) 802.1x
   d) LEAP

6. The Pairwise Transient Key (PTK) is a collection of several keys. List these keys and their length when CCMP is used.

   a) EAPOL MIC Key (128), EAPOL Encr Key (128), Data Encr Key (128), Data MIC Key (128)

   b) EAPOL MIC Key (128), EAPOL Encr Key (128), Data Encr/MIC Key (128)

   c) EAPOL MIC Key (128), EAPOL Encr Key (256), Data Encr Key (128), Data MIC Key (128)

   d) EAPOL MIC Key (128), EAPOL Encr Key (128), Data Encr/MIC Key (256)

7. What is *Michael* in WPA/RSN?

   a) The encryption algorithm in TKIP

   b) The key mixing algorithm of RC4

   c) The message integrity code of TKIP

   d) The replay protection algorithm of TKIP

8. What is the purpose of the EAPOL 4-way handshake?

   a) To compute a fresh pairwise temporal key (PTK) from the pairwise master 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

9. 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) $C = E(i) \oplus M$

10. How is the IEEE 802.11 CCMP nonce input constructed?

    a) The values of the Pairwise Transient Key, the NonceA, and the NonceB

    b) The values of the Pairwise Temporal Key, the Source Address, and the Destination Address

    c) The values of the fields Packet Number, Address1, Flag of the MPDU

    d) The values of the fields Packet Number, Address2, Priority of the MPDU

11. Does GSM provide mutual authentication?

    a) No

    b) Yes

    c) Operator dependent

    d) In cooperation with UMTS

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

    a) By the network providing temporary subscriber identities to the SIMs

    b) By storing the subscriber identity in the SIM only

    c) By storing the 128-bit secret key (K_{IMSI}) in the SIM and distributed only to trusted VLRs

    d) By using the IMEI instead of the IMSI

13. Which information is sent from the AuC to the VLR/SGSN during 3G/UMTS authentication?

    a) IMSI

    b) RAND, AUTN, XRES, CK, IK

    c) RAND, AUTN

    d) RAND, AUTN, XRES, Kc

14. Which UTRAN 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

15. What happens if the result of the UTRAN algorithm 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

    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

16. Can the security header in MAPsec be encrypted? Why/why not?

    a) No, because the header consists of {SPI ‖ Original Component ID ‖ TVP}

    b) Yes, because the header consists of {SPI ‖ Original Component ID ‖ TVP}

    c) No, because the MAPsec header must be processed at the receiving end

    d) Yes, because an IPsec tunnel is set up

17. Which CSCF handles SIP registration requests and informs the Home Subscription Server (HSS)?

    a) All

    b) P-CSCF

    c) I-CSCF

    d) S-CSCF

18. Which three modes does the confidentiality algorithm in UMTS support?

    a) RLC-Transparent, RLC-Unacknowledged, RLC-Acknowledged
    b) RRC-Transparent, RRC-Unacknowledged, RRC-Acknowledged
    c) RLC-Transparent, RRC-Unacknowledged, RLC-Acknowledged
    d) RRC-Transparent, RLC-Unacknowledged, RRC-Acknowledged

19. 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

20. What are the three functional requirements for UMTS authentication?

    a) Mutual authentication between USIM and HSS, securing the radio channel communication, and end-to-end confidentiality
    b) Mutual authentication between USIM and AuC, securing the radio channel communication, and user identity confidentiality
    c) Confidentiality and privacy for the subscriber, and mutual authentication for the service provider
    d) AV generation at AuC, key transport to the RNC, and the SQN synchronization

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

    a) No assumptions were made
    b) The kernel function must be a robust block cipher
    c) AES must be used as the kernel function
    d) The kernel function must be a oneway function

22. Which part of the IEEE 802.16 MAC PDU is encrypted?

    a) Both the header and the payload part
    b) The payload part and some fields of the header
    c) The payload part
    d) The header part

23. Which WiMAX entity is generating the Traffic Encryption Key (TEK)?

    a) The Base Station
    b) The AAA Server
    c) The Access Service Network
    d) The Network Service Provider

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

    a) The USIM holds an expiration date and, like credit cards, must be replaced

    b) The failure rate of the integrated circuit cards (UICCs) are high because the issuers (mobile operators) want to optimize cost against subscription duration

    c) The UE manufacturing and lifecycle can be managed independently from the personalization and subscription process

    d) End-to-end UMTS key-card plugs into the USIM slot for key distribution and management

25. What is Internet Key Exchange (IKE)?

    a) The security association set up protocol in the IPsec protocol suite

    b) The key exchange subprotocol of the Transport Layer Security protocol

    c) The key transformation protocol for the inter-operation of GSM and UMTS

    d) The security association center in the IMS system

Part II. Authentication Protocols (30%)

As Master of communication security in Securemore Inc. you are responsible for contributing to a NextGSM recommendation proposal for enhancing the authentication protocol in the GSM system. You start thinking about the problem by recapitulating the GSM Authentication and Key Agreement protocol. Next you construct a new and promising enhancement to this cryptoprotocol that needs to be analyzed.

26. Recall the standard entity authentication and key transport protocol of the GSM mobile network, which includes the entities SIM&MS, BS, VLR, HLR & AuC. Draw the protocol, using the supplied MSD form, and include all security messages with variables and computations starting from "Identity Request" to "Cipher Mode Command". (3%)

27. Formulate compactly the security assumptions and the logic for the security claims regarding the authentication of a SIM resulting from the protocol interactions and computations of Question 26. (6%)

28. Consider the scenario where Malice is able to set up a rogue GSM base station that can accept both incoming MS connections and establish connections to genuine GSM network operators. Make a message sequence diagram that shows how Malice is able to "catch IMSIs" and eavesdrop on the communications of calling MS. (6%)

29. Now construct your enhancement to the GSM authentication protocol, while preserving the existing GSM authentication protocol. The protocol must enable the SIM to distinguish between rogue and authentic access network connections, and assure the SIM that the link encryption key is fresh, and available at the BS. Draw your protocol diagram, and formulate the assumptions and the logic for your security claims of the new protocol construction. (7%)

30. Compare the number of bits in the message exchange and the computations of your protocol with the original GSM protocol. What is the increase in communication and computational load? (2%)

31. A successful man-in-the-middle attack can be defined as an attack that engages two independent protocol participants to communicate with the attacker in such a way that a security goal/claim of the protocol is broken. Analyze your enhanced GSM authentication protocol with respect to a man-in-the-middle attack threat, and describe your reasoning and conclusion. (6%)

Part III. Analysis of Cipher Initialization Implementation (20%)

Alice is conducting an experiment in wireless network security. Using the aircrack-ng tool suite, she tries several different attacks on a Cisco access point (AP) configured with Wired Equivalent Privacy (WEP). While running an ARP replay attack with 682 captured data frames per second, the total number of unique initialization vectors (IVs) observed seems to reach a maximum value of approximately 1 040 000 after about two hours. The Table 1 is reproducing the measurements from her lab journal. It shows the number of minutes the ARP replay attack has been running and the total number of unique IVs observed with time. The number of fresh IVs observed is close to the number of captured data frames in the first few minutes of the experiment, and then the growth gradually decreases until it is close to zero after approximately two hours.

Minutes	Unique IVs observed
2	76 874
23	629 428
30	727 198
40	824 629
50	896 612
60	945 423
80	1001 550
100	1026 429
120	1038 326
140	1043 822

Table 1: The accumulated number of different IVs observed with time.

32. State at least three different methods of IV value generation. (2%)
33. What is the size of the set of IV values in the WEP specification? (3%)
34. How do your answers to the questions above relate to the data in Alices experiment as shown in Table 1? (3%)

The lab journal of Alice shows that she did not expect this IV generator behaviour, and she has repeated the experiment several times but each time she ends up with very similar results.

35. Look into the data of Table 1 and search for an explanation why Alice did not expect this result, then settle for a plausible hypothesis of the generation of the IV values based on your observations and assumptions. State your hypothesis about the IV generation used by this AP, and explain how you found the result. (3%)

Fortunately, a mathematical friend of yours is familiar with a problem from probability theory that applies to this experiment, the general birthday problem. This problem states that when n values are selected with a uniform distribution, with replacement, from a total population of m values, the expected number of *unique* values observed is

$$E(m, n) = m(1 - (1 - 1/m)^n).$$

In the experiment, m represents the total number of possible IV values, and n represents the number of data frames captured, hence $E(m, n)$ represents the expected number of unique IV values observed.

36. Add two new columns for Table 1 and make the following computations. The first new column should show the expected number of unique IVs observed under your hypothesis at 60, 120 and 140 minutes. The second new column should show the expected number of unique IVs observed using WEP with random IV selection at 60, 120 and 140 minutes. (3%)

37. Draw interpolation plots for the experimental data and the two new columns described above at 60, 120 and 140 minutes. (2%)

As a final step, you decide to have a look at the actual IVs in the capture file. Table 2 shows 25 IV values from one of the experiments of Alice.

011100100101011011010110
011101110010100010101000
011011100100110001011100
011011010010001110001100
001111000000100101110100
001111000010000100011010
011100000000000111100000
011001100100010101110010
011101110000111011101110
011010100001110011100110
011111010100100110100110
001011110110010101101010
011101110010101010000000
011010100101111111101010
011001110010000001011110
001000010001111011100010
001011110001011100000100
001111100110011000110010
001100100001110110101010
001000000011010101011000
011110110100100011100100
011010010111100100010000
001001100100100000001100
011100110111011010100110
011010100111000101011100

Table 2: A sample of captured IVs in binary representation.

38. Does the data in Table 2 support your hypothesis? Explain why/why not. What new information can you find by looking at the actual IVs in Table 2? (4%)

TTM4137 Exam Dec. 3, 2010 Solution Outline

Stig F. Mjølsnes, Dec. 16, 2010

Part I. Wireless Networks Security Facts

1d, 2b, 3c, 4a, 5a, 6b, 7c, 8c, 9c, 10d, 11a, 12a, 13b, 14d, 15c, 16c, 17d, 18a, 19c, 20b, 21b, 22c, 23a, 24c, 25a.
Norsk utgave: 19d, 24d, ellers som for engelsk utgave.

Part II. Authentication Protocols

26. See Figure 2 and 3 in syllabus Ref. [3] and Figure 1.3 in the UTMS book.
27. The VLR authentication decision is (SRES $\stackrel{?}{=}$ XRES). The SIM receives a value SRAND and computes SRES = $A3(K_i, \text{SRAND})$. The AuC generates a random value RAND and computes the value XRES = $A3(K_i, \text{RAND})$. Assumptions:
1) Only the authorized AuC and the SIM of subscriber i can input K_i.
2) The $A3()$ is a oneway function.
3) The XRES is computed correctly by the AuC, and received correctly by the VLR.
4) The XRES is kept confidential.
5) The RAND value is not replayed by AuC or VLR.
28. The Malice BS will prompt the victim MS to send the IMSI by an *Identity Request* message, then send an arbitrary challenge value RAND, disregard the reply SRES, and then send the *Cipher mode off* command to the victim MS, enabling a non-encrypted voice stream call setup. The Malice MS can forward the victim MS call by normal network access.
29. Multiple solutions are possible and acceptable here, the students will have to engage their creativity in the synthesis. Let us use the notation introduced in the lectures where $[m]_K$ represents the cipher text of m encrypted under a key K. One solution would be to introduce a sequence counter SQN, similar to the implicit authentication mechanism of the UMTS access network, where AuC will provide an encrypted value $[\text{SQN}]_{K_i}$ to be verified by the MS. Subsequently, a two-way handshake interaction between the MS and the BS with respect to the session/call key K_c can be done by the MS sending $[\text{SRES}, \text{NONCE}]_{K_c}$ and the BS responding with $[\text{CellID}, \text{NONCE} + 1]_{K_c}$.
30 and 31. Answers depends on the solution in 29.

Part III. Analysis of IV implementation

32. Electrical noise signal, cryptographic pseudorandom generator, sequence counter register, realtime clock, or a combination
33. $2^{24} = 16777216$.
34. After 140 minutes only $\frac{1}{16}$ of the possible values have been observed, but the rate of unobserved values decreases notably. Since the rate is tapering off but does not suddenly end, it cannot be a sequence or clock time that "wrap around" early. It might be a skewed noise source or pseudorandom generator.
35. The length of the binary representation is $\log_2 1043822 = 19.99344428$. Alice was surprised because the IV domain is 2^{24} and the speed of collecting

new values should not decrease at that rate at around $\frac{1}{16}$ of the whole set. Hypothesis: The entropy of the pseudorandom generator is 20 bits.

36. See answer to question 38, exam Dec 1, 2008.
37. See answer to question 39, exam Dec 1, 2008.
38. See answer to question 40, exam Dec 1, 2008.

—

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_____

TTM4137 Exam Dec. 12, 2011 Solution Outline

Stig F. Mjølsnes, Revised Dec. 19, 2011

Part I. Wireless Networks Security Facts

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

Part II. Cryptographic Mechanisms

26. A streamcipher does a bit-by-bit encryption process, whereas a block cipher does encryption of a whole block of bits. However, the RC4 cipher shows that this stream cipher operates on a byte by byte basis. A byte is a block of bits. Hence, we might consider a stream cipher a special case of a block cipher. On the other hand, we might consider a block cipher a special case of a stream cipher, observing that the block cipher keystream is constant. A stream cipher is an approximation of a Vernam one-time cipher. A block cipher is an approximation of a one-way function.
27. A one-way function is a function for which it is computationally 'easy to compute' the function value $f(x)$ given x, but no 'easy to compute' algorithm is known that outputs an x', given a function value $y = f(x')$. 'Easy to compute' means a polynomial time algorithm with respect to the length of the input. More elaborate definitions exist.
28. $c_i = e_k(c_{i-1} \oplus m_i), i = \{1, 2, \ldots\}, c_0 = IV$.
29. The idea of a message authentication code (MAC), also called a message integrity code (MIC), or simply an authentication code, is to compute a check value by some algorithm with input the cryptographic key and all bits of the message, and send the resulting output value along with the message. The recipient will do the same computation and check that the output is equal to the received value. One example construction is the CBC-MAC variant of UIA f9, a cipher-block-chaining mode of operation.
30. The MD5 does not need a secret key input. There might be other reasons.
31. The purpose of the initialization vector is to change the cipher function even though the key is kept fixed. The same input will (very likely) result in a different output for each initialization vector value. The IV must never be reused with the same key because this opens for a replay attack, therefore the size of the IV set must be sufficiently large to avoid this reuse. The IV value can be chosen sequentially and is normally sent in the clear to the recipient. If the IV must be a non-predictable value, it must be selected by a (pseudo)random process.
32. The key space will depend on the `keyinput` length $k, 1 \geq k \leq 256$ bytes. The key space becomes $2^{8 \cdot k}$. Typical key length will be 16 bytes = 128 bits or 32 bytes = 256 bits. We do not require the student to compute the decimal representation of these integers, but here they are: The key space for 128 and 256 bit lengths are
340282366920938463463374607431768211456 (39 digits)
115792089237316195423570985008687907853269984665640564039457584007913129639936 (78 digits)
The full key length of RC4 is 256 bytes, or 2048 bits, and the key space for this is 256^{256}
32317006071311007300714876688669951960444102669715484032130345427524

6551388678908931972014115229134636887179609218980194941195591504909210950881523864482831206308773673009960917501977503896521067960576383840675682767922186426197561618380943384761704705816458520363050428875758915410658086075523991239303855219143333896683424206849747865645694948561760353263220580778056593310261927084603141502585928641771167259436037184618573575983511523016459044036976132328723122712568471082020972515710172693132346967854258065669793504599726835299863821552516638943733554360213543322960464531847860495214819355585361105959623065630 (617 digits)

33. 256 possible values of `i`, and 256 possible values of `j`, and 256! possible permutations of the values 0-255 in `S[]`
hence $256 \cdot 256 \cdot 256!$ possible states. This number has 512 digits, not required to compute this:
5621794572486853618034817575690126132234036971303636958312239270312473084252308041743992693459854350420383402179537038908831805175848609220672155081096731201894071222687293678830716240702960829647872773138160964781356335278630184319118130060334418338288125994472398335386938050153827654752634923044950884227942008865157673628382230385215000669626074626502218343125491407985594545559974362723838209077859207489822809538134165690411852814251562998169600000000000000000000000000000000000000000000000000000000000000000000000000000000
Ideally, the number of states of the generator should be approximately the same as the key space. If the key space is larger than the number of states, then many keys will collide to the same state. The cross-over for k is where $256^{k-2} \approx 256!$.

Part III. Protocols

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. This problem is open for many ingenious solutions. One solution is given in slide 15 of the Lecture Notes 13, Nov. 11, 2011. RFC3329

—

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

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

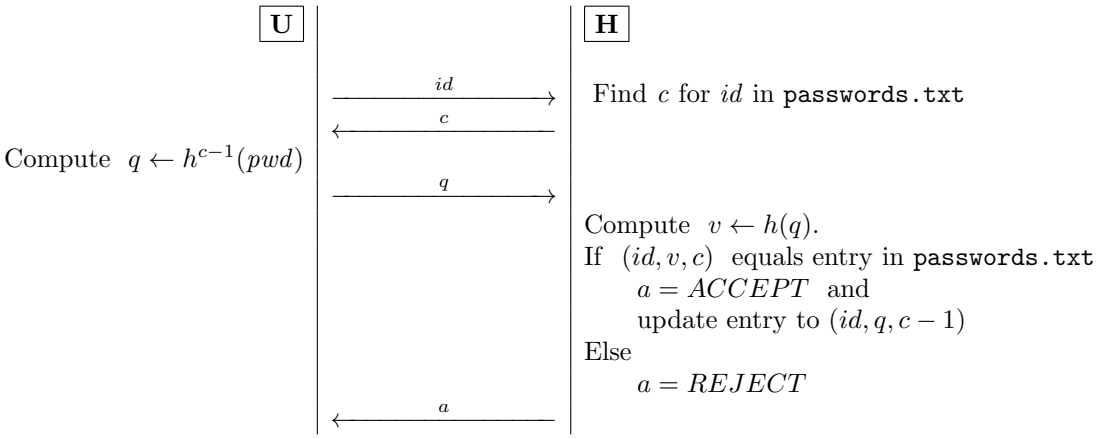
Part III. Protocols (30%)

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

TTM4137 Exam Solution Outline

12:12:12, 12.12.2012, corrections 13.12

Stig F. Mjølsnes, Joe-Kai Tsay, Simona Samardziska

Part I. Wireless Networks Security Facts

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

Part II. Password Based Authentication

26. Random password generation defeats a dictionary or wordlist attack.
27. Malin can set up her WiFi network interface controller (WNIC) in promiscuous mode to eavesdrop when Anne perform her login process, thereby acquire her password that is sent in cleartext.
28. Similar to the previous protocol, if Malin listens to the WiFi traffic, she can read the login values (id, v) that Anne send, and that is all she needs for impersonating Anne at the file server.
29. Client hash value computation is better if the client use the same password for access to other servers. If the hash value is computed at the server side, then an eavesdropping on the login to one server, can compromise the security of the other servers as well.
30. From the explanation given, the probability that any two employees have the same password has values is:

$$p \approx 1 - e^{-\frac{1}{2^{32}} \cdot \frac{100 \cdot 99}{2}} = 0.000001153$$

31. The probability for hash value collisions must be less than $p = 10^{-10}$, hence first, we need to solve the equation $p = 1 - e^{-\frac{1}{2^{k'}} \cdot \frac{100 \cdot 99}{2}}$ for the unknown k'. The solution can be computed by:

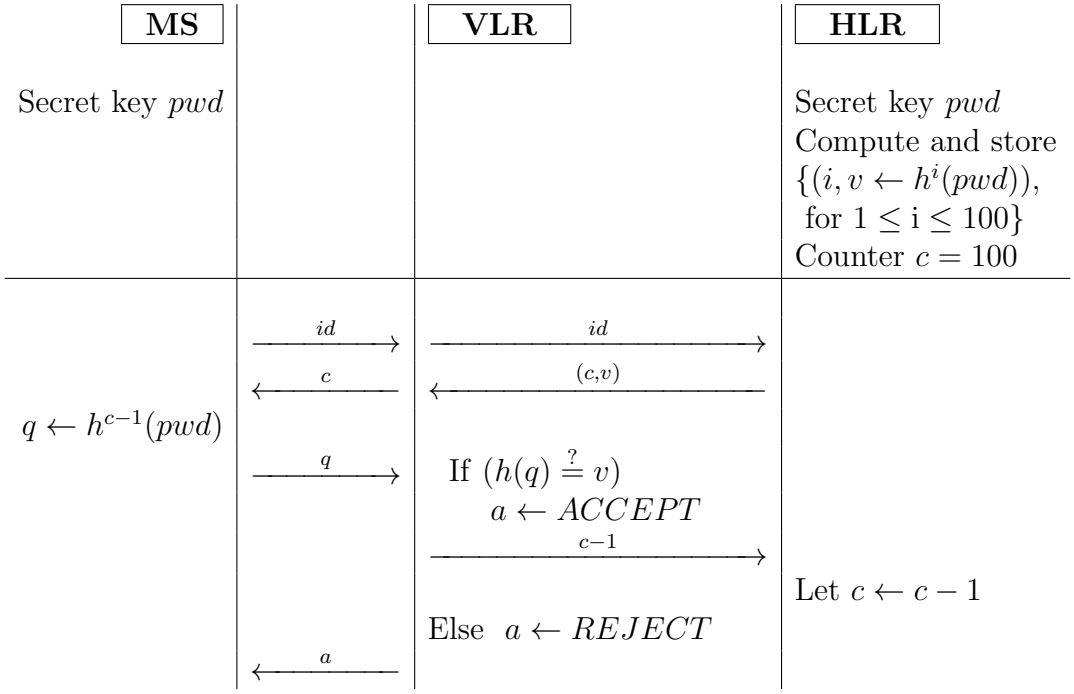
$$k' = \log_2(\frac{-100 \cdot 99}{2 \cdot \ln(1 - 10^{-10})}) = 45.49$$

Hence, for $k = \lceil k' \rceil = 46$, the probability of collision is less than 10^{-10}.

Part III. Protocols

32. The host H authenticates the user terminal U by a "Lamport onetime password scheme", thus preventing password eavesdropping.
Correctness: if U knows the password pwd, then for all c ("protocol runs") will the verification predicate be true $(h(h^{c-1}(pwd)) = h^c(pwd))$.
Security: by the oneway property of the hash function, observing the protocol triplets (id, c, q) for some c, then it is hard to compute the correct triplet for the next run $(id, c-1, v)$ such that $h(v) = q$.
33. A man-in-the-middle-attack is possible because U does not authenticate the messages from H, in other words, U has no mechanism to distinguish between messages from an attacker and the host H. Thus, Malin can send c to Anne, then receive the correct response $h^{c-1}(pwd)$ from Anne, stop the protocol with Anne, and impersonate Anne in a complete login protocol with the host. Note that, Malin can anticipate the expected c, just by listening to previous logins. But any value of c less than the previous one will also work, because Anne does not maintain the current value of c.

34. There is a lot of freedom in the answer of this question. The simplest solution is to just divide the host into two parties, the visited and the home network, without enhancing the security in any way. Q36. gives a hint on the interpretation of the function h in the mobile environment. The adaptation can be done as follows.



35. This answer will depend which protocol is constructed in Q.34. We can distinguish the following differences to the GSM authentication protocol. When the VLR sends id to the HLR, it receives back only one pair $(c, h^c(pwd))$. In GSM it may be a batch of triplets for the same user. Notice that, if the VLR has the algorithm for h it doesn't need to store the list of pairs $(i, h^i(pwd))$, for $1 \leq i \leq 100$. This is because of the counter properties of c. However, this implies that it is very easy to mount a man-in-the-middle-attack as described in Q32, which can be used to steal a call from a legitimate user. Thus, authentication of the MS to the VLR fails. The GSM key agreement part is not in our protocol, but it can be implemented as in GSM using some other function of the secret key pwd, and the counter c very similar to GSM. Again, since in this protocol there is no mutual authentication, the same man-in-the-middle-attack as in GSM can be applied in this one as well. Another difference is that the home network must be online in the process of authentication, in order to update the value from c to $c-1$ in case of successful authentication.

36. Depends on the answer of Q34. For the protocol described here in Q34. we see that there is quite a big computational load on the MS side compared to GSM, if we assume that the cost of the h function is the same as of the A3 function, i.e., for each authentication the computational load is $c-1$ times bigger. However, a time-memory trade-off can be done here, if instead of computing $h^i(pwd)$ all the values $(i, h^i(pwd)),\ 1 \leq i \leq 100$ are stored in the MS in an ordered list. Then, after every successful authentication the expired entry can be deleted, or marked as expired. Note that this modification affects security in the sense that the man-in-the-middle-attack from Q32 can be detected. Also, at the VLR side, a similar time-memory trade-off can be made, but then, the home network must send a batch of pairs $(i, h^i(pwd))$ to the visited network. In this case, there is no need for the algorithm of h at the visited network side.

—