DI/FCT/UNL
Mestrado Integrado em Engenharia Informática
Segurança de Redes e Sistemas de Computadores
(*Computer Systems and Network Security*)
2nd Sem., 2016/2017
(26/April/2017)

Midterm Test #1

Part I – Closed Book (45 min)

Question 1

a) Use a matrix format (table) to show relationship between the X.800 framework security services and security mechanisms. You must put services in columns and mechanisms in lines. For services consider the following definitions in columns, in the presented order.

Peer-Entity Authentication, (2) Data-Origin Authentication, (3) Access Control, (4) Connection confidentiality, (5) Traffic-Flow Confidentiality, (6) Availability, (7) Connectionless integrity, (8) Non-Repudiation

b) From the security mechanisms presented in the matrix-table sketched in a), which are considered pervasive mechanisms and which are considered specific mechanisms. Why?

Question 2

Consider a secure key-distribution protocol using a Key-Distribution Center, to establish symmetric keys between different principals that need to establish one-to-one secure communication bidirectional channels. Consider for this purpose a protocol with properties such as the Needham-Schroeder Protocol.

Discuss if with such a protocol is possible to offer guarantees of perfect forward secrecy and perfect backward secrecy conditions.

Question 3

In which circumstances we must avoid the use of ECB mode when using any symmetric encryption algorithm to encrypt data flowing in a secure channel? Why?

Question 4

To implement integrity checks against message tampering with implicit message authenticity proofs we can use Message Authentication HMAC (Hash-MAC) or CMAC (Cryptographic MAC) constructions.

Present advantages and drawbacks of using HMAC and CMAC mechanisms for the referred purpose and why we can not using simple secure hash functions for the same purpose.

Part II – Open Book (45 min)

Question 5

The Kerberos V4 protocol is represented in the following figure. Version 5 overcomes some deficiencies in the version V4.

Explain the improvements introduced by the version 5 that are related with modifications in the structure of the messages or in the message flow as represented below for the version 4. You don't need to write the complete syntax of the messages but you must explain the modifications and improvements to overcome the limitations in the V4 protocol in each one of the 6 rounds of messages of the version 4.

(1) C → AS $ID_c \,\|\, ID_{tgs} \,\|\, TS_1$

(2) AS → C $\mathrm{E}(K_c, [K_{c,tgs} \,\|\, ID_{tgs} \,\|\, TS_2 \,\|\, Lifetime_2 \,\|\, Ticket_{tgs}])$

$Ticket_{tgs} = \mathrm{E}(\mathrm{K}_{tgs}, [\mathrm{K}_{c,tgs} \,\|\, \mathrm{ID}_C \,\|\, \mathrm{AD}_C \,\|\, \mathrm{ID}_{tgs} \,\|\, \mathrm{TS}_2 \,\|\, \mathrm{Lifetime}_2])$

(a) Authentication Service Exchange to obtain ticket-granting ticket

(3) C → TGS $ID_v \,\|\, Ticket_{tgs} \,\|\, Authenticator_c$

(4) TGS → C $\mathrm{E}(K_{c,tgs}, [K_{c,v} \,\|\, ID_v \,\|\, TS_4 \,\|\, Ticket_v])$

$Ticket_{tgs} = \mathrm{E}(\mathrm{K}_{tgs}, [\mathrm{K}_{c,tgs} \,\|\, \mathrm{ID}_C \,\|\, \mathrm{AD}_C \,\|\, \mathrm{ID}_{tgs} \,\|\, \mathrm{TS}_2 \,\|\, \mathrm{Lifetime}_2])$

$Ticket_v = \mathrm{E}(\mathrm{K}_v, [\mathrm{K}_{c,v} \,\|\, \mathrm{ID}_C \,\|\, \mathrm{AD}_C \,\|\, \mathrm{ID}_v \,\|\, \mathrm{TS}_4 \,\|\, \mathrm{Lifetime}_4])$

$Authenticator_c = \mathrm{E}(\mathrm{K}_{c,tgs}, [\mathrm{ID}_C \,\|\, \mathrm{AD}_C \,\|\, \mathrm{TS}_3])$

(b) Ticket-Granting Service Exchange to obtain service-granting ticket

(5) C → V $Ticket_v \,\|\, Authenticator_c$

(6) V → C $\mathrm{E}(K_{c,v}, [TS_5 + 1])$ (for mutual authentication)

$Ticket_v = \mathrm{E}(\mathrm{K}_v, [\mathrm{K}_{c,v} \,\|\, \mathrm{ID}_C \,\|\, \mathrm{AD}_C \,\|\, \mathrm{ID}_v \,\|\, \mathrm{TS}_4 \,\|\, \mathrm{Lifetime}_4])$

$Authenticator_c = \mathrm{E}(\mathrm{K}_{c,v}, [\mathrm{ID}_C \,\|\, \mathrm{AD}_C \,\|\, \mathrm{TS}_5])$

(c) Client/Server Authentication Exchange to obtain service

Question 6

a) V4 and V5 versions of the Kerberos Protocol are vulnerable to password attacks. Explain why and discuss possible solutions to mitigate or to avoid this problem.

b) Explain how you can use a PBE Encryption scheme in the first two messages of the protocol and discuss if this can mitigate the problem in a)

Question 7

The HMAC standard (as defined in RFC 2104) used two secure hash functions in the algorithm construction. In the proposed generic standardized construction we can use any two secure hash functions, including two different hash functions in the same construction. From your analysis, what are the advantages of this flexibility compared with the alternative standardization of fixed secure hash functions.

Question 8

Consider the triple DES algorithm. We will use the algorithm to encrypt messages for confidentiality protection, using CBC mode. We will use a key of 168 bits, with the following structure in hexadecimal representation (but this is not known by an adversary) with an initialization vector known by the adversary.

Sequence of 28 bits = 0 | | Sequence of 56 bits = 1 | | Sequence of 56 bits = 0 | | Sequence of 28 bits = 0

Explain why the security of the algorithm will be minimized with such a key for the purpose (that we can consider a weak-key).

Part III – Open Book (30 min)

For these questions consider the Work Assignment # 1 specifications and your implementation.

Question 9

The Phase 2 specification uses a PBE Encryption Scheme to authenticate users, for subsequent access-control and (in case of authorization) to obtain cryptographic parameters and keys to participate in the supported multicast sessions. Explain if the specification and/or your implementation provide guarantees for perfect future secrecy and perfect backward secrecy for confidentiality support. Why?

Question 10

a) Explain, from your implementation how the initialization vectors are established when your crypto-suites include symmetric encryption modes requiring those initialization vectors.

b) Is it possible for an adversary conducting a traffic sniffing passive attack in the communication channel to know the values of established initialization vectors?

If YES , this is a flaw in the confidentiality guarantees? Why?

If NO, this adds more confidentiality guarantees? Why?