| | |
|---|---|
| | Departamento de Informática<br>Faculdade de Ciências e Tecnologia<br>UNIVERSIDADE NOVA DE LISBOA |

Curso de Mestrado em Engenharia Informática (2º Ciclo)
Segurança em Sistemas e Redes de Computadores
(Computer Systems and Networks Securty, MSc Level)

**1º Sem. 2010/2011**
TESTE DE FREQUÊNCIA Nº 2
(Frequency Test 2)

Test duration: 2 hours
The test has two groups of questions

- Group 1: Answers with closed book: 1 hour
- Group 2: It is possible to use reference documentation and materials: 1 hour

| | | |
|---|---|---|
| Student Number: | Name: | |
| LEI/MEI: | Group: SSTC-G___ | Total number of pages: |

*You should number each page in the form: Page Number/TOTAL*

EVALUATION TABLE (to be used by the teacher)

| GROUP 1 (Closed book) | | | | | | | |
|---|---|---|---|---|---|---|---|
| Q1 a) | Q1 b) | Q2) | Q3 a) | Q3 b) | Q4 a) | Q4 b) | Q4 c) |
| | | | | | | | |

| GROUP 2 | | |
|---|---|---|
| 1) | 2) | 3) |
| | | |

Departamento de Informática
Faculdade de Ciências e Tecnologia
UNIVERSIDADE NOVA DE LISBOA

Curso de Mestrado em Engenharia Informática (2º Ciclo)
MSc Course /
Frequency Test 2 – 17/December/2010
SSRC

Part I (Closed book)
60 minutes

**Q1**

a) In the following figure, the Kerberos V4 protocol is represented.
Version 5 overcomes some deficiencies in the 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 type of modifications and improvements to overcome the limitations in the V4 protocol.

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

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

$Ticket_{tgs} = E(K_{tgs}, [K_{c,tgs} \| ID_C \| AD_C \| ID_{tgs} \| TS_2 \| Lifetime_2])$

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

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

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

$Ticket_{tgs} = E(K_{tgs}, [K_{c,tgs} \| ID_C \| AD_C \| ID_{tgs} \| TS_2 \| Lifetime_2])$

$Ticket_v = E(K_v, [K_{c,v} \| ID_C \| AD_C \| ID_v \| TS_4 \| Lifetime_4])$

$Authenticator_c = E(K_{c,tgs}, [ID_C \| AD_C \| TS_3])$

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

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

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

$Ticket_v = E(K_v, [K_{c,v} \| ID_C \| AD_C \| ID_v \| TS_4 \| Lifetime_4])$

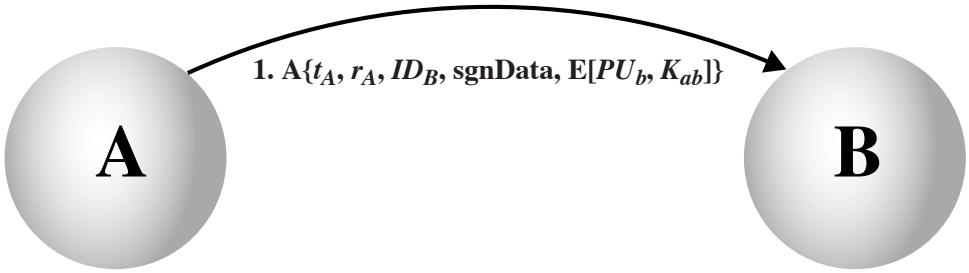
$Authenticator_c = E(K_{c,v}, [ID_C \| AD_C \| TS_5])$

**(c) Client/Server Authentication Exchange to obtain service**

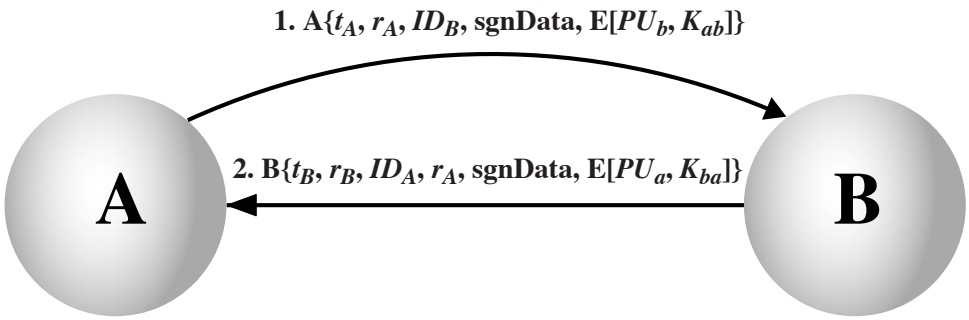
b) V4 and V5 versions of the Kerberos Protocol are vulnerable to password attacks. Explain why and discuss possible solutions to mitigate or to avoid this attack to Kerberos V4 and V5 base protocols.

**Q2**

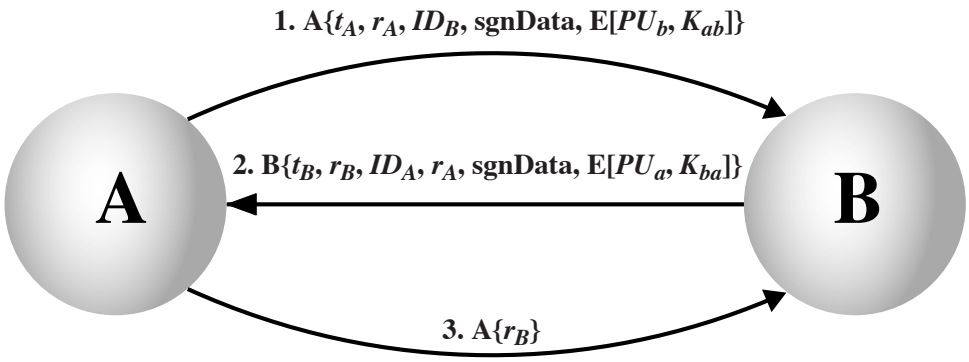
The following figure represents different authentication procedures using X509. In (a) B authenticates A in a one-way authentication process. In (b) and (c) both protocols support mutual authentication between A and B. What is the potential advantage or disadvantage between the solutions (b) and (c) to support mutual authentication? Justify you answer.




**(a) One-way authentication**




**(b) Two-way authentication**




**(c) Three-way authentication**

Q3)

a) Explain the notion of Forward Certificates and Reverse Certificates in a X509v3 certification chain.

b) In a X509 v3 certificate, the extension fields provide relevant additional information about the use of certificates and correspondent certified public keys. In annex, the generic structure of X509 certificates (versions 1, 2 and 3) is represented.

There are different extensions types in v3 certificates, structured in three different extension types:

- Key and Policy information extensions
- Certificate Subject and Issue Attributes
- Certificate Path Constraints

The Key and Policy extensions include information that must be taken into account to validate the certificate in accordance with the intended use. This information includes the following extension fields

Authority Key Identifier
Subject Key Identifier
Key Usage
Private-Key Usage Period
Certificate policies
Policy mappings

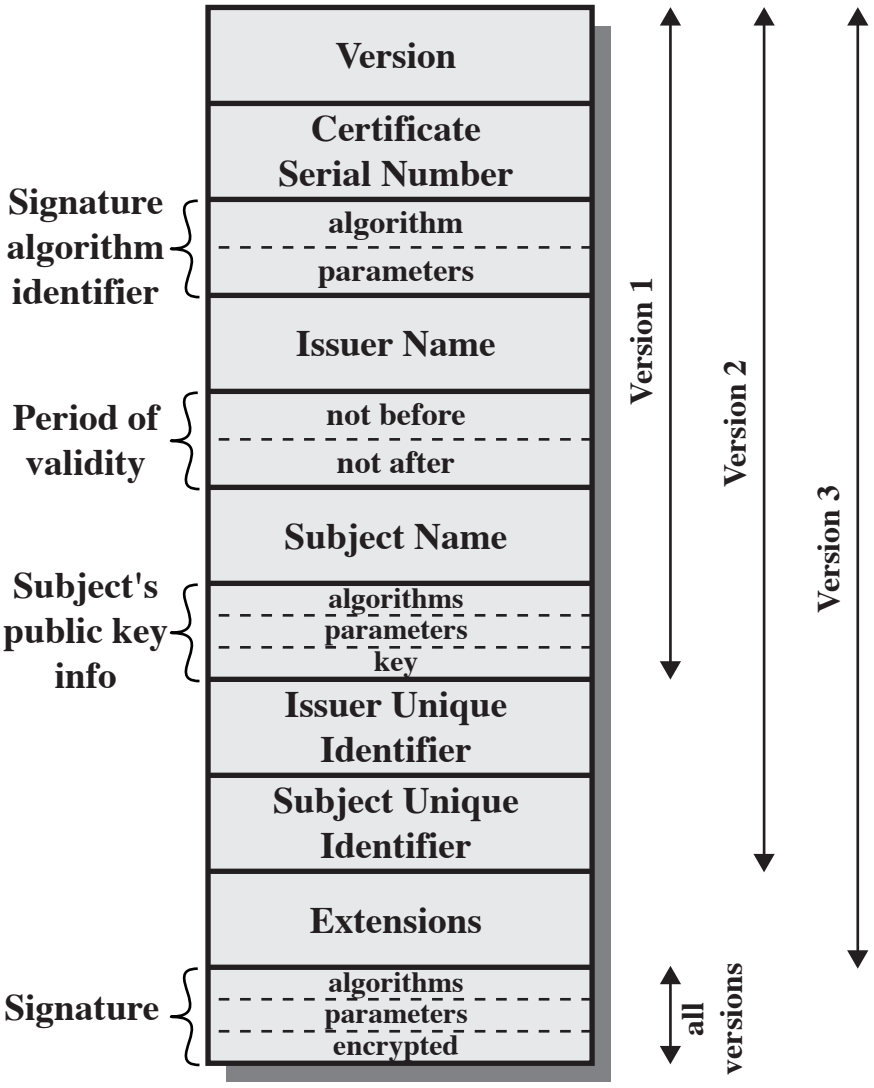
Explain the purpose of at least 4 of these fields, explaining the possible relevance with examples.

Q4)

a) Explain if a protocol as SSL (or TLS) and all its sub-protocols and mechanisms, can protect an endpoint of a secure SSL server from a denial of service attack in which an attacker in the client side send TCP SYN segments to request a connection but dows not respond to the SYN acknowledge to establish the connection fully. Note that such attack (known by SYN-flooding attack) typically leaves the server in a "half-open or incomplete connection state", around a few minutes. Consequently, repeated SYN messages from the attacker can clog the TCP server, that will so the server will be unavailable to establish connections with other correct clients.

b) Based on what you know from the security mechanisms provided by SSL, do you think that it is possible in SSL for a receiver to re-order SSL records in the Record Layer Protocol that arrive out of order ? If so explain how it can be done, discussing if, from this viewpoint, an SSL implementation over UDP car give this warranties to the principals interchanging SSL records.

c) Explain the purpose of the Change Cipher Protocol in the stack of SSL or TLS sub-protocols


Version
Certificate Serial Number
Signature algorithm identifier
algorithm
parameters
Issuer Name
Period of validity
not before
not after
Subject Name
Subject's public key info
algorithms
parameters
key
Issuer Unique Identifier
Subject Unique Identifier
Extensions
Signature
algorithms
parameters
encrypted
Version 1
Version 2
Version 3
all versions

Departamento de Informática
Faculdade de Ciências e Tecnologia
UNIVERSIDADE NOVA DE LISBOA

Curso de Mestrado em Engenharia Informática (2º Ciclo)
MSc Course /
Frequency Test 2 – 17/December/2010
SSRC

Part II
60 minutes

1) Consider the code in teste2P21.java (annex)

This program compiles but will originate an error in runtime. Why? Justify and explain the cause of the error taking in consideration the theoretical foundations of RSA and the JAVA/JCE programming support as used in both programs.

2) Consider the program DHA.java (annex)

The program implements the use of a Diffie Hellman agreement, implemented with the Java/JCE support, to setup a symmetric key shared between "A" and "B" (with "A" and "B" modeled as two different principals implemented in the same program).

Inspired by this program you must provide a solution, in which "A" will be now implemented as a client and "B" will be modeled as a server, implemented with TCP sockets. In your solution you must provide support to resist to a man-in-the middle attack, protecting the Diffie-Hellman agreement between the client and the server with an appropriate solution to avoid a "man in the middle attack" provided by a TCP proxy that can operate between the client and the server.

a) First you must present a specification of the protocol for your solution
b) Then you must provide your solution, providing the code for the client and for the server.