Department of Computer Science | **Network Security (Netwerkbeveiliging)**

Vrije Universiteit | **02-06-2005**

Answers must be in English.

The contribution of each question to the final mark (100 points) is indicated at the end of each question. A complete and correct answer will get all the points indicated. Partial answers will get only some of the points.
[The final mark will be then normalised base 10, i.e. 80 → 8, 75 → 8, 74 → 7]

1) Describe in detail how the following 3 modes of operation of DES: Electronic Code Book (ECB), Cipher Block Chaining (CBC) and Cipher Feedback Mode (CFB) work.
[10 points]

2) Describe in detail what are the type of attacks to which ECB mode is vulnerable to while CBC is not and explain why.
[10 points]

3) Describe in detail how is it possible to hash securely large messages using only secret key cryptography
[10 points]

4) On the use of Certificates Revocation Lists (CRL):
   a) Why must Certificates Revocation Lists be reissued periodically even when no new certificates have been revoked? [4 points]
   b) If there is a revocation mechanism, why do certificates need an expiration date? [4 points]
   c) Let us assume a public key algorithm used for digitally signing messages. When can a user destroy a public key? [4 points]

5) In the Lamport hash protocol, the hash value is sent in the clear over the network. Why is it more secure than a password? Can someone impersonating the server do a dictionary attack? If yes explain how, if not explain why not. [10 points]

6) Let us assume a system with the following security labels and clearance levels:

Subject	Current Clearance
Moe	SECRET (NATO, NUCLEAR, CRYPTO)
Curly	TOP SECRET (NATO, NUCLEAR)
Larry	SECRET (NATO, CRYPTO)
Shep	TOP SECRET ()

Object	Current Labels
Cream Pie	CONFIDENTIAL (NATO, CRYPTO)
Pointy Object	SECRET (NUCLEAR)
Shaved Poodle	TOP SECRET (NATO, NUCLEAR)

The system follow the Bell-LaPadula model so implementation allows read-down and write-up.

Who can read the Cream Pie? [5 points]

a) Moe.
b) Curly.
c) Larry.
d) b) and c).
e) a) and c).
f) None of the above.

Who can write the Pointy Object? [5 points]

a) Moe.
b) Larry.
c) Shep.
d) a) and c).
e) b) and c).
f) None of the above.

Who can execute the Shaved Poodle? [5 points]

a) Moe.
b) Larry.
c) Shep.
d) a) and b).
e) b) and c).
f) None of the above.

7) Examine the following authentication protocol where A and B share a prearranged secret S before the protocol starts.

$A \rightarrow B$: n, g, $g^x \bmod n$
$B \rightarrow A$: $g^y \bmod n$
$A \rightarrow B$: $h(A,B, S, g^{xy} \bmod n)$
$B \rightarrow A$: $h(B,A, S, g^{yx} \bmod n)$
$A \rightarrow B$: [msg] KAB

(where h is an hash function, $KAB = g^{xy} \bmod n$ is the established session secret key. A and B re-run this protocol every time they need to start a communication session)
Is this protocol secure? If not why? [12 points]

8) A bank wants to provide secure online access to its customers such that they can consult their bank accounts through Internet. Although the communications run over an untrusted network, customers do need to securely communicate with the bank server to access their accounts. Which cryptographic primitives can be used to solve this problem and describe how. [15 points]

9) Describe the RSA algorithm. [6 points]

5) Examine the following protocol

$A \rightarrow T$: A,B
$T \rightarrow A$: $(A,K_A+,[A,K_A+]K_T-)$, $(B,K_B+,[B,K_B+]K_T-)$
$A \rightarrow B$: $[Ks,T_A,[Ks,T_A]\ K_A-]K_B+$, $[A,K_A+]K_T-$

(where T is the Trusted Third Party, K_A+ is A's public key and K_A- is A's private key, Ks is the session key, T_A is A's timestamp, $[m]K_A-$ is m encrypted with K_A-)
Is this protocol secure? If not why and how it can be modified to be secure?
[12 points]

6) Describe in detail [system components involved, protocol description, data structured used, etc.] of at least three different mechanisms to implement certificates revocation
[10 points]

7) What is a covert channel? [2 points]
Describe an example of timing covert channel and how does it work [4 points]
Describe an example of storage covert channel and how does it work [4 points]

8) The following information applies to questions 8.1 through 8.3:

Subject	Current Clearance
Moe	SECRET (NATO, NUCLEAR, CRYPTO)
Curly	TOP SECRET (NATO, NUCLEAR)
Larry	SECRET (NATO, CRYPTO)
Shep	TOP SECRET (ALL CATEGORIES)

Object	Current Classification
Cream Pie	CONFIDENTIAL (NATO, CRYPTO)
Pointy Object	SECRET (NUCLEAR)
Shaved Poodle	TOP SECRET (NATO, NUCLEAR)

The Mandatory Access Control implementation allows read-down and write-up.

8.1) Who can read the Cream Pie? [4 points]
- a) Moe.
- b) Curly.
- c) Larry.
- d) b) and c).
- e) a) and c).
- f) None of the above.

NETWORK SECURITY 24-08-2004

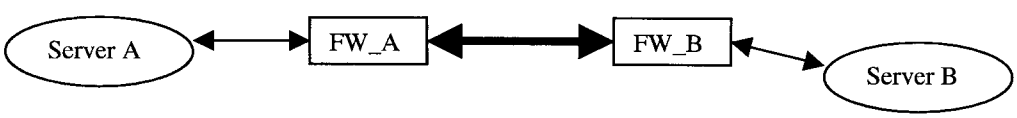
Answers must be in English.
The contribution of each question to the final mark (100 points) is indicated at the end of each question. A complete and correct answer will get all the points indicated. Partial answers will get only some of the points.
[The final mark will be then normalised base 10, i.e. 80 → 8, 75 → 8, 74 → 7]

1) A bank uses software that implements DES in all different modes of operations to implement security for its applications. The bank needs a new application that requires a secure hash function and it does not want to acquire new software. Can the bank implement a cryptographically secure hash function with the software it has? If yes, describe in detail how the hash function can be implemented.
[10 points]

2) Protocol-Designer has been told to design a scheme to prevent messages from being modified by an intruder. Protocol-Designer decides to append to each message a hash of that message. Why doesn't this solve the problem?
[6 points]

3) Let us assume to use DES in ECB mode. What are the possible attacks, if any, that an eavesdropper reading only the produced cipher text can mount on the scheme? What are the possible attacks, if the attacker can read not only the cipher text but also some correspondent plaintext? How DES can be used to make such attacks much harder? (You need not only to mention the types of attack but also to describe in detail how they work)
[14 points]

4) Let us assume that server_A of company A wishes to exchange secret and authenticated messagges with server_B of company B. In both companies, all the incoming/outgoing communications are regulated by a firewall. Both company employ IPsec in order to achieve secure communication. Which IPsec protocols and in which mode of operations are needed for the server to achieve their security goals and in order to prevent an eavesdropper to learn anything about the IP addresses of the two servers? Describe in details the format of the exchanged packet.
[12 points]



8.2) Who can write the Pointy Object: [4 points]

a) Moe.
b) Larry.
c) Shep.
d) a) and c).
e) b) and c).
f) None of the above.

8.3) Who can execute the Shaved Poodle? [4 points]

a) Moe.
b) Larry.
c) Shep.
d) a) and b).
e) b) and c).
f) None of the above.

9) A and B share a password of 6 characters (48bits). A and B want to exchange encrypted messages using DES without sharing anything else than the already known password. (We assume here that DES is secure, thus attackers cannot mount a brute force attacks to single DES). How can A and B solve the problem and meet the following requirements?

a. Do not share with the other party anything else than the password
b. A and B use powerful PC.
c. The solution must be secure against an external attacker (breaking the solution must be equivalent to breaking DES).
d. A and B cannot use hash functions

[14 points]