ÉCOLE POLYTECHNIQUE
FÉDÉRALE DE LAUSANNE

Family Name: .....

First Name: .....

Section: .....

Cryptography and Security Course

(Security Part)

Exam

February 17th, 2004

Duration: 1 hour 30 minutes

This document consists of 12 pages.

Instructions

Documents are not allowed except linguistic dictionaries.

Electronic devices are not allowed.

Answers must be written on the exercises sheet.

Answers of Parts II and III must be justified.

Answers can be either in French or English.

Questions of any kind will certainly *not* be answered. Potential errors in these sheets are part of the exam.

Part I **(1 pt)**

Only one answer is correct per question. The marking is as follows: **Right answer +0.1 pt, No answer 0 pt, Wrong answer -0.1 pt**. The total grade cannot be less than zero.

Question 1: Which of the following IPSec configurations is compatible with NAT?
☐ AH / Transport. ☐ AH / Tunnel. ☐ ESP / Transport. ☐ ESP / Tunnel.

Question 2: How long is a classical brute force attack (in the worst case) on a personal workstation in order to recover an alphanumeric password, given the corresponding LM hash? (roughly)
☐ 10 seconds. ☐ 10 hours. ☐ 10 days. ☐ More than 10 years.

Question 3: HTTPS relies on...
☐ ... SSH. ☐ ... IPSec. ☐ ... SSL/TLS. ☐ ... L2TP.

Question 4: The security gap is...
☐ ... the gap between the security we think we have and what we actually have.
☐ ... the weakest point in a network architecture.
☐ ... a distributed honeypot.
☐ ... an attack based on social engineering.

Question 5: EAL1 is...
☐ ... a hash function.
☐ ... an assurance level of the Common Criteria.
☐ ... a standard issued by the German government.
☐ ... the W2k authentication algorithm used to access a NT network.

Question 6: S/MIME uses...
☐ ... PGP certificates.
☐ ... X.509 certificates.
☐ ... Kerberos tickets.
☐ ... IPSec Security Associations.

Question 7: A PKI...
☐ ... consists of a toolbox containing encryption and signature algorithms.
☐ ... is an infrastructure handling the creation and distribution of certificates.
☐ ... is a standard providing the measures to be included in a security policy.
☐ ... is the revocation certificate issued by a user whose private key has been corrupted.

Question 8: Tick the *false* assertion about HTTPS.
☐ HTTPS guarantees confidentiality of transmitted data.
☐ The server must have a certificate.
☐ The client can have a certificate but this is not mandatory.
☐ HTTPS has a HTTP-compatible mode for clients not supporting HTTPS.

Question 9: When two people know each other, what is the *worst* technique they can use to exchange and check their PGP keys (from the security point of view)?
☐ They exchange their keys by email and they check the fingerprints by phone.
☐ They get the keys from a well-known key server.
☐ They both get the expected key through a trusted friend and check that his signature on the key is valid.
☐ They post their keys on a website and physically meet together to check the fingerprints.

Question 10: Which of the following information *cannot* be found in a PGP certificate?
☐ The identity of the user.
☐ The email of the user.
☐ The signature private key of the user.
☐ The encryption public key of a user.

Part II **(1.5 pts)**

Exercice 1: HTTPS

When a client connects to a Web server using HTTPS, he receives a certificate (in answer).

1. Which key is needed by the client to verify the certificate?

2. The verification carried out by the browser can fail for many reasons. Give and explain three of them.

Exercice 2: IPSec

1. Represent a data packet protected by IPSec using DES / HMAC-SHA-96 in tunnel mode.

2. Which part of an IPSec packet is *not* authenticated with ESP?

3. Is this part completely authenticated with AH?

Exercice 3: PGP

PGP uses four keys when a user A wants to sign and encrypt an e-mail to a user B:

1. the key used to sign the content of the mail,
2. the key used to decrypt the key used in step 1,
3. the key used to encrypt the content of the mail,
4. the key used to encrypt the key used in step 3.

1. Which ones are *symmetric*?

Key 1	☐ Yes	☐ No
Key 2	☐ Yes	☐ No
Key 3	☐ Yes	☐ No
Key 4	☐ Yes	☐ No

2. Which length (in bits) seems to be adequate for a symmetric key? For an asymmetric key?

3. Explain when these keys are generated.

Part III **(2.5 pts)**

The company Tarennom, specializing in the manufacture of beet yoghurts, possesses an internal computer network which allows to manage its production line. The access from the workstations to the servers embedded in the machines requires an authentication on a centralized authentication server.

First of all, we discuss the security of the employees' workstations. The accounts of the employees are not centralized: they are hosted by the workstations. Each workstation can host several accounts. The access to these workstations, using Windows XP, requires a password. Generation of LM hashes is not disabled, so both LM hashes and NT hashes are generated when a password is created or renewed.

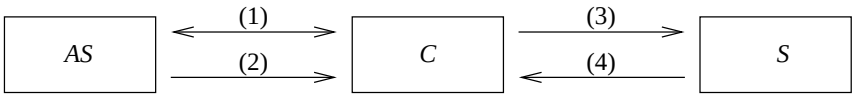
1. Explain how the authentication by password works and recall which cryptographic algorithms are used in order to compute the LM hashes and NT hashes.

2. We consider a workstation hosting three accounts, protected by random passwords of 8 alphanumeric characters. We assume that the attacker knows that the length of the passwords is exactly 8 characters. If an attacker obtains the file containing the hashes and carries out an exhaustive search, how many cryptographic operations will he have to perform (in the worst case) in order to crack the LM hashes of the three accounts?

3. From such a password, which operations does the attacker have to perform in order to find the password corresponding to the NT hash? What is the complexity of this step (in the worst case)?

4. Some operating systems decrypt the file containing the hashes when the computer is booting. This protects the access to the hashes. Explain the limitations of this technique.

We focus now on the centralized authentication. When an employee (called here *client*, denoted by C) wants to access the server controling a machine (denoted S), he must carry out the authentication protocol with the centralized authentication server (AS). If this authentication succeeds, AS sends some data to C, in particular the list of the servers to which he is authorized to connect to. We represent on the figure below the exchanges between AS, C, and a server S. We suppose that an attacker is capable of eavesdropping the communication channels. In the following, $\{M\}_{K_{A,B}}$ denotes the symmetric encryption of a message M with the key $K_{A,B}$ shared by A and B, and $||$ denotes the concatenation of messages.



(1) C and AS carry out an authentication protocol (which you will design below). We assume that they subsequently agree on a common session key $K_{C,AS}$.

(2) When C is authenticated, AS picks a random key $K_{C,S}$ and sends

$$\{V, L\}_{K_{S,AS}} || \{C, K_{C,S}, V\}_{K_{S,AS}} || \{K_{C,S}\}_{K_{C,AS}}$$

to C, where V is a validity period (sufficiently long so that the client only has to carry out the authentication procedure once a day) and L is a list of servers to which the client is authorized to connect to.

(3) Then C sends the following message to S:

$$\{V, L\}_{K_{S,AS}} || \{C, K_{C,S}, V\}_{K_{S,AS}} || \{C, \text{request}\}_{K_{C,S}}.$$

(4) Using $\{V, L\}_{K_{S,AS}}$, the server S checks that the client is authorized to access it. If so, it executes the request and possibly sends back the result.

5. Design an authentication protocol which could be used between C and AS. This protocol should *not* send passwords or hashes of passwords in clear over the network. In particular, you will answer to the following questions: (a) Is any data shared by AS and C before the authentication? (b) If yes, how have these data been transmitted? (c) If some data need to be protected (confidentiality or integrity) on the client side, explain how to proceed. (d) Describe the content of each exchanged message.

↪

6. We consider an attacker who can be correctly authenticated by AS (e.g., the attacker is an employee of Tarennom) but who does not have the rights to access a given server S'. Propose an attack such that S' accepts the request *forged* by the attacker.

7. We consider now an attacker who cannot be authenticated by AS. Explain which kind of attack he can carry out and why such an attack is possible.

8. How can the scheme be fixed in order to thwart the attacks of questions 6 and 7?

9. We point out that C must contact AS every time it wants to request a new server S. Why? How can the scheme be modified (without adding a new entity) in order to avoid this issue?

According to the security principles, an attacker always attacks the weakest link of an architecture. Thus, an attacker who would want to request some servers, could try to recover either the password of a client or a symmetric key used during the authentication.

10. Which key is the most interesting from the attacker point of view? Why ?

Please, do not turn over this sheet

before the starting signal.