cns20160623.odt

Name:	Last name:	Id:

Computer and network security
Sicurezza nelle reti e nei sistemi informatici
Crittografia e sicurezza delle reti

Exam of 23rd June 2016, a.y. 2015-16. Time: 2 hours

FOR NON-ENGLISH: 2 penalty points (only applicable to Computer and network security)
FOR UNREADABLE HAND-WRITING: discretionary decision

Q1: **Secure server-mediated messaging between two parties**

We consider the scenario where two parties want to exchange messages (we shall call them *posts*) by the support of a central server S that shares a secure symmetric key with each of the parties (we denote such keys as K_A, K_B etc.). According to an informal protocol, if A wants to send a post to B then:

a) A should ask the permission to B, and the request should be routed through S.
b) B can accept/reject the request (still through S).

In case B accepts:

c) S should generate a session key K (to be used by the parties) and let the parties have it.
d) Now A can send the message directly to B (and only now B will accept messages from A). A will accept messages from B only after her first message sent to B.
e) Then, A and B can exchange any number of messages, as long as the session has not been invalidated (see below).
f) At any time, any of the two parties can invalidate the session by sending a specific message.

Q1.1 [6/30] Design the contents of the messages to be exchanged between parties/server for implementing the protocol and allowing the posts, also adding suitable contents (e.g., hashes, nonces, challenges etc.) for making the protocol secure over authentication and confidentiality of posts.

Q1.2 [4/30] Improve the scheme designed in Q1.1 by adding security for *data integrity* (of posts) and against *replay attacks*.

You can assume that:

- ❏ S is secure.
- ❏ Both A and B have no malicious behaviours.
- ❏ The network connecting all the parties is highly reliable and efficient, but not secure with respect passive/active adversaries.
- ❏ Exchanged messages can have any size.

Q2: **Kerberos**

Q2.1 [4/30] Give a general description of the Kerberos protocol, clarifying the roles of the authentication server, the ticket-granting server and describing the contents of the tickets (what is an authenticator?).

Q2.2 [2/30] Describe how a TGT can be used by a principal for requesting a service.

Q2.3 [2/30] Illustrate the concept of *realms* and the authentication between realms.

Q3: **Cryptographic hashing and one-way functions**

Q3.1 [3/30] Define what a cryptographically secure hashing function is and list its main properties.

Q3.2 [2/30] Define the concept of one-way function and describe a typical scenario where it could be usefully employed.

Q3.3 [2/30] Could a cryptographically secure hashing function be a one-way function? Elaborate.

Q4: **Session firewalls**

Mark each of the following assertions on common session firewalls (e.g.: Iptables) as TRUE or FALSE. [+0.8 for correct mark, 0 for missing mark, -0.4 for wrong mark]

- ❏ Can filter datagrams on the basis of source/destination IPs and/or source/destination ports.
- ❏ Can allow packets within an open TCP connection.

❏ Can protect against malware.
❏ Can protect users from visiting malicious web sites.
❏ Can offer some support against syn-flooding attacks.
❏ Can be useful in detecting keyloggers.

Q5: **Access control**

Provide short answers (2 lines max) to the following questions.

Q5.4 [2/30] A paramilitary organisation has classified its documents according to four levels of secrecy: confidential (C), very confidential (CC), secret (S), top-secret (TS). Which approach to access control would you recommend, and for what reason?

Q5.5 [2/30] Why DAC models are unable to protect data against Trojan Horses embedded in application programs? Elaborate.

HAVE YOU SENT 2015-16 HOMEWORKS TO THE PROF.? YES/NO (circle your answer)

If YES:
I hereby confirm that I sent no. _____ contributions (how many Qs)

Signature

_____
(please sign in both cases)