COMPUTER SECURITY

Corso di Laurea Magistrale in Ingegneria Informatica
Prof. Alessandro Armando

14 gennaio 2019

Nome e Cognome: _____

Matricola: _____

---

1. **Criptography**

   What is the probability of finding a collision for an 60-bit hash function? What is the main reason for this probability?

   Solution: Two cases:

   - if the target hash code/document is given: 2^{-60}
   - if the target hash code/document can be forged by the attacker: 2^{-30} (cf. the *birthday paradox*)

2. **Crittografia a Chiave Pubblica**

Indicate if the following questions are true or false, justifying your answers:

(a) The private key must be necessarily generated by the Certification Authority and given to the legitimate owner together with the digital certificate of the corresponding public key

Solution: FALSE

(b) A smartcard used for the digital signature stores the private key of its owner.

Solution: TRUE

(c) To verify the authenticity of a digital signature it is necessary to have a smartcard.

Solution: FALSE

(d) There exist digital certificates whose authenticity cannot be verified by checking their signature.

Solution: TRUE: the root certificates

3. **Digital Certificates**

(a) Explain the role played by digital certificates in the establishment of secure connections between web browsers and web servers.

Solution:

(b) Does the digital certificate of web-applications depend on the IP address of the server on which they are executed?

Solution: NO!

4. **Protocolli di Sicurezza**

The following protocol has been designed to generate and distribute a session key K between A and B using S as *key distribution center*:

1. $A \rightarrow S : E(K_{AS}, B)$
2. $S \rightarrow A : E(K_{AS}, [K, E(K_{BS}, [A, K])])$
3. $A \rightarrow B : E(K_{BS}, [A, K])$

where K_{AS} is a symmetric key known only to A and S and K_{BS} is a symmetric key known only to B and S. The protocol is vulnerable to a *replay attack*.

(a) Descrive an attack.

Solution: Attack #1: An eavesdropper can observe the third message (from Alice to Bob) and any subsequent traffic that Alice sends encrypted under K to Bob. Later, the eavesdropper can replay the third message and subsequent traffic to Bob, and Bob will think that the replay came from Alice.

Attack #2: An eavesdropper can observe the entire three-message exchange and all subsequent traffic sent by Alice or Bob. Later, if Alice begins to request another session to Bob, the attacker replace S's response with the second message of the prior session, and can then replay any of the traffic from the prior session (since Alice and Bob will then re-use the same key K for both sessions).

(b) Assume that A, B and S have synchronized clocks. Modify the protocol so to prevent replay attacks by adding values to the messages of the protocol. Please justify your answers.

Solution:

1. $A \rightarrow S : E(K_{AS}, B)$
2. $S \rightarrow A : E(K_{AS}, [K, T, E(K_{BS}, [A, K, T])])$
3. $A \rightarrow B : E(K_{BS}, [A, K, T])$

where T is a timestamp generated by A and checked by S and B.

5. **Secure Programming**

   (a) Write a program (preferably in C) suffering from a buffer overflow.

   Solution:

   (b) Modify the program so to prevent the buffer overflow.

   Solution:

6. **Controllo degli Accessi**

   Consider the Bell-La Padula access control model. Indicate the permissions granted to a user with *security label* (secret,{personnel, design, assistance}) on documents classifiedin the following way:

   1. (top secret, {design}): **no permission**
   2. (top secret, {personnel, production, design, assistance}): **only writing**
   3. (secret, {personnel, assistance}): **only reading**
   4. (secret, {production, design}): **no permission**
   5. (secret, {}): **only reading**
   6. (confidential, {personnel, assistance}): **only reading**
   7. (confidential, {production, design}): **no permission**
   8. (confidential, {}): **only reading**