COMPUTER SECURITY

Prof. Alessandro Armando

11 gennaio 2023

Nome e Cognome: Enrico Pezzano

Matricola: 4825087

---

1. **Criptography**

   Proof of work (PoW) is a form of cryptographic proof in which one party (the prover) proves to others (the verifiers) that a certain amount of a specific computational effort has been expended. One popular approach (HashCash) to PoW amounts to the problem of finding a string X whose SHA-1 hash code begins with N binary zeros, where N is a given positive integer.

   Assume that computing the SHA-1 hash code takes at most 1 ms.

   (a) How long does it take to solve the HashCash problem in the worst case if N=10?

   ~~A.~~ 1 sec

   B. 2 sec

   C. 1 min

   D. 2 min

   NO ~~E.~~ None of the above

   (b) What is the probability to solve the HashCash problem in less than 10 sec if N=20?

   (c) What is the minimum value of N for which the solution to the HashCash problem takes at least 1 hour?

b) 10 sec = 10000 msec that probability to get a SHA1 string with 20 zero is $\frac{2^{150}}{2^{160}}$ (possible string with first ten 0s / possible strings) we have to do

$2^{-10} = 1/2^{10} = 1/1024 \cong 0{,}001$ (probability to guess the string) = 0,1 %

$\frac{10000}{2^{160}/2^{150}} = \frac{10^4}{2^{10}} \approx \frac{10^4}{1024^2}$ ms $= \frac{10000}{1024^2}$ = probability to guess in less than 10 sec with N=20

c) 1 hour = 3600 sec = 36000 msec

$2^N > (3600 \cdot 10^{12}) \cong 44$

$\frac{2^{160}}{2^N} = \frac{36\,000\,000}{1} \rightarrow N = \log_2\left(\frac{36\,000\,000}{2^{160}}\right)$

2. **Digital Signature and Digital Certificates**

(a) Your browser establishes a secure SSL connection with a Web Server through a valid certificate. Which of the following sentences are true? (There could be more than one correct answer.)

A. All data the Web Server sends to your browser will be encrypted and only your browser and the Certification Authority will be able to decrypt them.

B. All data your browser sends to the Web Server will be encrypted and only the Web Server will be able to decrypt them.

C. You can securely send privacy-sensitive data to this Web Server since you are guaranteed it will be dealt with in an appropriate way.

D. You can securely send security-critical data to this Web Server since you are guaranteed it won't be disclosed to unauthorized parties.

E. All data the Web Server sends to your browser will be encrypted and only your browser will be able to decrypt them.

NO F. All data your browser sends to the Web Server will be encrypted and only the Web Server and the Certification Authority will be able to decrypt them.

(b) Which data must be included in a digital certificate of a Web Server? (There could be more than one correct answer.)

A. Digital signature of the certificate generated by the Certification Authority

NO B. Public Key of the Certification Authority

C. Domain Name of the Web Server

D. Identity of the Certification Authority that issued the certificate

E. Private key of the Web Server

F. IP Address of the Web Server

G. Public key of the Web Server

3. Security Protocols

Consider the following authentication and key agreement protocol. Alice (A) and Bob (B) want to establish a session key using a long-term symmetric key K_{AB}. First Alice generates a nonce N_A and sends it along with her identity to Bob. Bob generates his own nonce N_B and sends it together with the encryption of Alice's nonce under the long-term key K_{AB}. Alice acknowledges receipt of this message by sending the encryption of Bob's nonce under the long-term key. Finally Bob generates the session key k and sends it to Alice encrypted under K_{AB}.

$$
\begin{aligned}
A &\rightarrow B : A, N_A \\
A &\leftarrow B : \{N_A\}_{K_{AB}}, N_B \\
A &\rightarrow B : \{N_B\}_{K_{AB}} \\
A &\leftarrow B : \{k\}_{K_{AB}}
\end{aligned}
$$

where both nonces and keys consists of 128-bit.

(a) This protocol is flawed. Show how Eve could learn a session key that Alice thinks she has securely established with Bob.

(b) Propose a way to fix the protocol to defend against this attack. Explain why your fix prevents this attack.

a) $A \rightarrow E \rightarrow B : A, N_A$

$A \leftarrow E \leftarrow B : \{N_A\}_{K_{AB}}, N_B$

$A \rightarrow E \rightarrow B : \{N_B\}_{K_{AB}}$

$A \leftarrow E \leftarrow B : \{K\}_{K_{AB}}$

⋮ → At this point, Eve knows K

$A \rightarrow E : \{A, Message\}_K$

$A \leftarrow E : \{B, Msg\}_K$

⋮

b) $A \rightarrow B : \{A, N_A\}_{K_{CA}}$

$A \leftarrow B : \{N_A, K_{AB}\}_{K_{CA}}, N_B$

$A \rightarrow B : \{N_B, K_{AB}\}_{K_{CA}}$

$A \leftarrow B : \{k\}_{K_{AB}}$

Using certificates from an external entity of verification I'm sure that A is comunicating with B and viceversa; because noone can do a replay attack at this protocol, thanks to do the obligatory step of verificate yourself to the opposite entity with the certificate

4. **Access Control**

Consider the following security labeling in the Bell-LaPadula model:

Subject	Label
Alice	L4
Bob	L1
Carol	L5
Dave	L2
Eve	L3

Object	Label
P1	L4
P2	L1
P3	L5
P4	L2
P5	L3

The labels follow a complete ordering L1 > L2 > L3 > L4 > L5.

(a) Interpret the labels as security labels in the simplified Bell-LaPadula model. Fill the access column in the following table with the access (read, write) that BLP would give each subject to the corresponding object.

Subject	Object	Access
Alice	P5	write
Bob	P3	read
Carol	P5	write
Dave	P4	read write
Eve	P1	read

(b) Now consider the case where the labels have categories in addition to the completely ordered levels. We add categories red and blue. The new label assignments are:

Subject	Label
Alice	L4:{red}
Bob	L1:{red}
Carol	L5:{red,blue}
Dave	L2:{red,blue}
Eve	L3:{blue}

Object	Label
P1	L4:{red}
P2	L1:{red,blue}
P3	L5:{red}
P4	L2:{red}
P5	L3:{blue}

Interpret these labels according to the Bell-LaPadula Model. Fill the access column with the access that BLP would give each subject to the corresponding object: read, write.

Subject	Object	Access
Alice	P1	read - write
Bob	P2	write
Carol	P2	write
Dave	P4	read
Eve	P3	nothing