COMPUTER SECURITY

Corso di Laurea Magistrale in Ingegneria Informatica
Prof. Alessandro Armando

Esempi

Attenzione: Si risponda alle domande utilizzando lo spazio apposito.
Tempo per lo svolgimento: 2 ore.

Nome e Cognome: _____

Matricola: _____

---

1. ***Crittografia a Chiave Multipla***

   Un sistema crittografico a chiave multipla è *caratterizzato da un insieme di n chiavi $\mathcal{K} = \{K_1, \ldots, K_n\}$ tali che se se $C_0 = P$ è un generico plaintext e $C_{i+1} = E(C_i, K_i)$ per $i = 0, \ldots, n-1$, allora $C_n = P$. Ovvero cifrando P con tutte le chiavi $K_1, \ldots, K_n$ (in qualunque ordine) si ottiene il plaintext di partenza.*

   (a) *Un sistema crittografico a chiave multipla con $n = 2$ corrisponde ad uno dei sistemi crittografici visti a lezione. Quale? Si giustifichi la risposta data.*

   Soluzione. Uno schema crittografico a chiave a chiave pubblica (ad esempio RSA), dove $\mathcal{K}$ è dato dalla chiave pubblica e dalla chiave privata.

   (b) *Si discutano i possibili utilizzi di un sistema crittografico a chiave multipla con $n > 2$.*

   Soluzione. Un primo possibile utilizzo è per la firma digitale congiunta tra due o più agenti. Ad esempio se $\mathcal{K} = \{K_1, \ldots, K_n\}$ e K_i è privata per l'agente A_i (per $i = 1, \ldots, n-1$) e K_n è pubblica, allora A_1 può firmare digitalmente un documento M cifrandone un hash con K_1 e mandando il risultato ad A_2, A_2 cifra quanto ricevuto da A_1 con la propria chiave privata K_2 e invia il risultato ad A_3, e cosìvia fino a A_{n-1} che produce

   $$E(K_{n-1}, E(K_{n-2}, \ldots E(K_2, E(K_1, H(M))) \ldots)) \quad (1)$$

   La firma può essere verificata cifrando (1) con K_n. Si osservi che la sottoscrizione di un singolo agente è verificabile solo quando è verificabile la sottoscrizione dei co-signatari. Dualmente, sotto le stesse ipotesi sulla distribuzione delle chiavi, cifrando con K_n si ottiene confidenzialità nei confronti $A_1, \ldots A_{n-1}$.

2. ***Crittografia a Chiave Pubblica***

   (a) *Quali delle seguenti attività sono svolte da una smart cart?*

      A. *memorizzare il certificato digitale del possessore*
      B. *firmare i documenti utilizzando la chiave pubblica del possessore*
      C. *firmare i documenti utilizzando la chiave privata del possessore*
      D. *verificare la firma digitale dei documenti utilizzando la chiave pubblica del possessore*

   (b) *Quali delle seguenti informazioni devono essere necessariamente presenti in un certificato digitale?*

      A. *Identità del possessore del certificato*
      B. *Identità dell'Autorità di Certificazione che ha prodotto il certificato*
      C. *Chiave privata del possessore del certificato*
      D. *Firma digitale del certificato stesso prodotta dall'autorità di certificazione*
      E. *Chiave pubblica dell'autorità di certificazione*
      F. *Chiave privata dell'autorità di certificazione*
      G. *Chiave pubblica del possessore del certificato*

   (c) *Per firmare digitalmente un documento è necessario essere connessi alla rete? Giustificare la risposta data.*

   > ***Solution:*** *No, basta la smartcard.*

   (d) *Per verificare la firma digitale di un documento è necessario essere connessi alla rete? Giustificare la risposta data.*

   > ***Solution:*** *Non è strettamente necessario se di dispone del certificato digitale di colui che ha firmato il documento e di una Certificate Revocation List recente.*

3. ***Digital Signatures***

Which of the following sentences are true?

A. *The private key of a user must be generated by the certification authority and is given to the user together with the digital certificate of the corresponding public key.*

B. *A smartcard used for digital signatures stores the private key of the owner.*

C. *Smartcards play a crucial role in the validation of digital signatures*

D. *Smartcards play a crucial role in the generation of digital signatures*

E. *Smartcards play a crucial role in the storage of digital signatures*

4. ***Security Protocols***

Suppose Alice wants to send her Bank a message that includes her promise to pay Charlie $50 dollars. Alice and the Bank have a shared secret X. Alice initiates a conversation with the Bank by sending: $A\|B\|n$ (Alice's identity, the Bank's identity, and a nonce).

(a) *Specify a valid reply for the Bank (i.e., a message generated by the Bank to be sent to Alice) that would enable Alice to verify that the reply came from someone who knows the secret X.*

> ***Solution:***
> $$B \to A : A\|B\|n\|HMAC(X, A\|B\|n)$$

(b) *In order to setup a secure communication, Alice and the Bank need a secret session key. Suppose that the Bank chooses a session key K by XORing some pseudorandom data with X and includes it with the reply in step* (a) *above. Extend message* (a) *to provide the session key to Alice securely as well.*

> ***Solution:***
> $$B \to A : A\|B\|n\|E(X, K)\|HMAC(X, A\|B\|n\|K)$$

(c) *Now, Alice can submit her message ("Pay Charlie $50 from my account") to the Bank. Write the message in such a way that Charlie cannot replay it (Hint: you will need to add something to the message that the Bank is capable of checking to prevent replay.).*

> ***Solution:*** *Call M the message and include c a counter for the messages in the session. Then*
> $$A \to B : A\|E(K, M\|c)\|HMAC(K, A\|M\|c)$$
> *protects M's secrecy, ensures that Charlie cannot replay, and protects the integrity of the message.*

5. ***Secure Programming***

Consider the program below.

```
void example(char *s) {
 char array[1024];
 strcpy(array,s);
}

int main(int argc, char **argv) {
 example(argv[1]);
}
```

What threat exists in the above program? How would you resolve it?

Solution:

6. ***Controllo degli Accessi*** *Si consideri un sistema con tre utenti: Alice, Bob e Charlie. Alice possiede il file* `alice.bat`*, Bob può solo leggerlo e scriverlo, mentre Charlie può solo eseguirlo. Charlie può solo leggere il file* `bob.bat`*, che è posseduto da Bob, mentre Alice lo può solo leggere e scrivere. Charlie possiede il file* `charlie.bat`*; Alice lo può solo scrivere e Bob può solo eseguirlo. Ogni file può essere letto, scritto ed eseguito dagli utenti che lo posseggono.*

   (a) *Si scriva la matrice di controllo degli accessi corrispondente a tale situazione.*

Soluzione.

	`alice.bat`	`bob.bat`	`charlie.bat`
Alice	rwx	rw	w
Bob	rw	rwx	x
Charlie	x	r	rwx

   (b) *Si scriva la matrice di controllo degli accessi che si ottiene se Charlie dà ad Alice il permesso di leggere* `charlie.bat` *e Alice revoca a Bob il permesso di scrivere* `alice.bat`*.*

Soluzione.

	`alice.bat`	`bob.bat`	`charlie.bat`
Alice	rwx	rw	wr
Bob	r	rwx	x
Charlie	x	r	rwx

7. ***Access Control***

Consider the Bell-La Padula security model. Indicate the permissions granted to users with the following security clearances

1. *(top secret, {red, blue}):* . . . . . .
2. *(secret, {red}):* . . . . . .
3. *(secret, {red, black}):* . . . . . .
4. *(secret, {red, blue}):* . . . . . .
5. *(confidential, {red, blue}):* . . . . . .
6. *(confidential, {blue}):* . . . . . .
7. *(top secret, {red, green, blue, black}):* . . . . . .

over a resource with security label (secret, {red, blue}).

Soluzione. Ricordiamo che (r_2, c_2) domina (r_1, c_1) (in simboli, $(r_1, c_1) \leq (r_2, c_2)$ se e solo se $r_1 \leq r_2 \wedge c_1 \subseteq c_2$ e che gli accessi nel modello di Bell-LaPadula sono governati dai seguenti due principi:

- **No Read-Up** (detta anche **Simple Security Property**): Un subject con security label x_s può leggere informazione relativa ad una risorsa con security label x_o solo se x_s domina x_o.
- **No Write-Down** (detta anche ***-Property**): Un subject con security label x_s può scrivere informazione su un oggetto con security label x_o solo se x_o domina x_s.

Dunque le risposte sono:

1. (top secret, {red, blue}): x_s domina x_o: solo lettura
2. (secret, {red}): x_o domina x_s: solo scrittura
3. (secret, {red, black}): x_s non domina x_o e x_o non domina x_s: nessun permesso.
4. (secret, {red, blue}): x_s domina x_o e x_o domina x_s: lettura e scrittura.
5. (confidential, {red, blue}): x_o domina x_s: solo scrittura.
6. (confidential, {blue}): sola scrittura.
7. (top secret, {red, green, blue, black}): x_s domina x_o: solo lettura.