# Sicurezza e Privatezza

**Docente:** Prof. Pierangela Samarati

Appello di Giugno - 16 Giugno 2003

*Tempo a disposizione 2:00h*

**Domanda 1)**
Si risponda in maniera esaustiva ai seguenti punti.

1. Descrivere le funzionalità essenziali di un firewall ed il suo utilizzo tipico in una rete aziendale.
2. Descrivere le tecnologie principali impiegate nella realizzazione di firewall.
3. Si consideri l'esempio di regole di filtraggio statico presentato nella tabella seguente e si risponda ai seguenti punti:
   (a) Descrivere quale tipo di interazione viene regolato dalla politica di sicurezza descritta dalla tabella nel suo complesso;
   (b) Per ogni regola: descrivere con chiarezza quale comunicazione intercetta (chi è il client e chi il server? qual'è il significato del valore del Flag (in particolare, perché nella Regola 2 si impone il valore 1)?);
   (c) Considerando il tipo di applicazione (Posta Elettronica), la politica di sicurezza espressa dalla tabella non risulta coerente con l'uso comune. Motivare questa affermazione.

| Num. | Direzione | Azione | Prot. | Ind. IP Sorgente | Porta Sorgente | Ind. IP Destin. | Porta Destin. | Flag ACK |
|---|---|---|---|---|---|---|---|---|
| 1 | IN | Permit | TCP | Any | >1023 | 192.168.5.12 | 25 | 1/0 |
| 2 | OUT | Permit | TCP | 192.168.5.12 | 25 | Any | >1023 | 1 |
| 3 | IN/OUT | Deny | TCP | Any | Any | Any | Any | 1/0 |

Nota: Porta 25 = SMTP (posta elettronica)

**Domanda 2)**
Dire cosa si intende per firma digitale e a cosa può servire. Specificare inoltre le proprietà che una firma digitale deve soddsfare ed illustrare dettagliatamente un algoritmo per la realizzazione della firma. Si possono usare i cifrari simmetrici per la realizzazione della firma digitale? Giustificare la risposta.

**Domanda 3)**
Rispondere in modo breve ma completo alle seguenti domande:

1. Cosa si intende con *Denial of Service Distribuito* (DDoS)?
2. Descrivere in sintesi la tipologia di attacco detta *Cross-Site Scripting* (elementi principali del funzionamento, ruoli delle parti coinvolte - attaccante, vittima, terze parti coinvolte).
3. Crittosistemi a chiave simmetrica ed asimmetrica: vantaggi e svantaggi.
4. Protocollo SSH e protocollo SSL: a cosa servono? sono due protocolli equivalenti?
5. Se partendo dal messaggio in chiaro: "LANCIARE SFERA" si ottiene il messaggio cifrato: "FRROATSEAUTNE" allora possiamo concludere che è stato usato un cifrario a trasposizone oppure a sostituzione? Giustificare la risposta.
6. In relazione al problema della sicurezza delle password dire cosa si intende per:
   - spoofing
   - snooping
   - sniffing
   - masqueranding
7. Illustrare le limitazioni di una memory card rispetto ad uno smart token.
8. Concetti di storage, timing e covert channel.

**Esercizio 1)**

Si consideri un controllo di integrità multilivello, basato sui livelli di classificazione {`Alto, Basso`} e sulle categorie {`C1,C2`}. Si consideri quindi un soggetto *s* e gli oggetti, $ob1, ob2, oa1, oa2$ con la seguente classificazione:
$\lambda(s) = \langle \texttt{Alto,C1} \rangle$
$\lambda(ob1) = \langle \texttt{Basso,C1} \rangle$
$\lambda(oa1) = \langle \texttt{Alto,C1} \rangle$
$\lambda(ob2) = \langle \texttt{Basso,C2} \rangle$
$\lambda(oa2) = \langle \texttt{Alto,C2} \rangle$

Descrivere i principi base delle tre diverse politiche:

- Stretta integrità
- Low water mark per oggetti
- Low water mark per oggetti

e valutare quindi la loro applicazione nel controllo del seguente processo da parte di *s*. Per ogni operazione indicare se viene concessa o rifiutata e l'eventuale modifica alle classificazioni

**processo p**:
read(oa1)
write(ob1)
write(oa2)
read(ob1)
write(oa2)
write(oa1)
write(ob1)
read(ob1)

Svolgere l'esercizio nella tabella allegata.

**Esercizio 2)**
Data la matrice di accesso

| | **Program1** | **Program2** | **File1** | **File2** | **File3** |
|---|---|---|---|---|---|
| **Ann** | own,write read,execute | | read | write | write |
| **Bob** | | execute* | | | own,write read |
| **Carol** | | execute | | read,write | |

si richiede di:

1. formulare i comandi
   - $\text{confer}_{\text{execute}}$(`sbj1`,`sbj2`,`obj`): questo comando deve assegnare il privilegio execute ad `sbj2` su `obj` solo se `sbj1` è il proprietario di `obj`;
   - $\text{transfer}_{\text{execute*}}$(`sbj1`,`sbj2`,`obj`): questo comando deve assegnare il privilegio execute* ad `sbj2` su `obj` solo se `sbj1` ha il permesso di trasferire questo privilegio;
   - $\text{revoke}_{\text{execute}}$(`sbj1`,`sbj2`,`obj`): questo comando deve revocare il privilegio di execute su `obj` ad `sbj2` solo se `sbj1` è il proprietario di `obj`;
   - $\text{confer\_admin}_{\text{read+}}$(`sbj1`,`sbj2`,`obj`): questo comando deve assegnare il privilegio read+ ad `sbj2` su `obj` solo se `sbj1` è il proprietario di `obj`.
2. determinare lo stato che si ottiene dall'esecuzione, se possibile, dei comandi
   - $\text{confer}_{\text{execute}}$(`Ann`,`Carol`,`Program1`)
   - $\text{confer\_admin}_{\text{read+}}$(`Bob`,`Ann`,`File3`)
   - $\text{confer\_admin}_{\text{read+}}$(`Ann`,`Carol`,`File3`)
   - $\text{transfer}_{\text{execute*}}$(`Bob`,`Ann`,`Program2`)

(MATRICOLA) (COGNOME) (NOME)

**Tabella per l'Esercizio 1)**

| | **stretta integrità** | | **LWM per oggetti** | | **LWM per soggetti** | |
|---|---|---|---|---|---|---|
| **operazione** | SI/NO | modifica λ | SI/NO | modifica λ | SI/NO | modifica λ |
| read(oa1) | | | | | | |
| write(ob1) | | | | | | |
| write(oa2) | | | | | | |
| read(ob1) | | | | | | |
| write(oa2) | | | | | | |
| write(oa1) | | | | | | |
| write(ob1) | | | | | | |
| read(ob1) | | | | | | |