Sicurezza e Privatezza

Docente: Prof. Pierangela Samarati

Appello di Aprile - 14 Aprile 2003

Tempo a disposizione 2:30h

Domanda 1)
Descrivere l'evoluzione delle problematiche di sicurezza corrispondente all'evoluzione dei servizi forniti via Internet, da servizi "tradizionali" quali telnet, ftp etc. ad applicazioni Web. Discutere come la diffusione di applicazioni Web ha influito sulle tecniche per la protezione dei dati e delle risorse accedibili da Internet. Motivare l'osservazione che vuole che contromisure puramente tecnologiche, nel contesto odierno, non siano sufficienti in assenza di contromisure di tipo organizzativo e gestionale.

Domanda 2)
Discutere le principali tecniche per la protezione di micro e macro dati.

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

1. Cosa si intende per *Dynamic Packet Filter* (Filtraggio Dinamico di Pacchetti), detto anche *Stateful Filtering*, parlando di tecnologie di firewall?
2. Che cosa si intende con *ACK SCAN*?
3. Nell'ambito dei sistemi crittografici, dire in che cosa consiste l'*attacco basato sulle frequenze* e fornire un esempio.
4. Illustrare il funzionamento del cifrario One-time pad.
5. Descrivere le proprietà che caratterizzano le funzioni di hash one-way ed illustrare il loro utilizzo nella realizzazione di firme digitali.
6. Nell'ambito dei meccanismi di sicurezza, discutere le proprietà che deve soddistare il reference monitor.
7. Dire cosa sono i cookie e come vengono gestiti. Discutere inoltre il concetto di seal program.
8. Nell'ambito delle basi di dati multilivello discutere il concetto di cover story.

Esercizio 1)
Si consideri la seguente politica di sicurezza:

R1. Sono autorizzate sessioni Telnet (porta 23/tcp) solo tra il client esterno avente indirizzo IP 140.23.105.4 e il server interno avente indirizzo IP 192.168.1.5

R2. Sono autorizzate connessioni dal client interno avente indirizzo IP 192.168.1.100 al server esterno avente indirizzo IP 141.23.105.2 con porta applicativa di destinazione 56/udp.

R3. Ogni altra connessione non è autorizzata.

Assumendo che:

- non esistano altre politiche di sicurezza già implementate;
- si disponga di un firewall di tipo static packet filter;

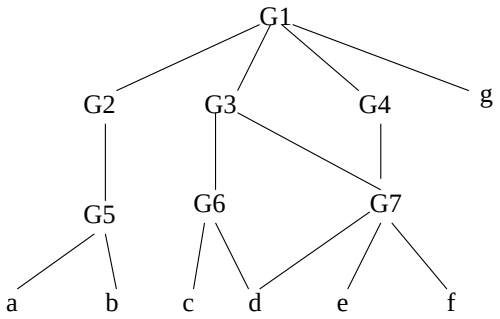
si svolgano i seguenti punti:

1. scrivere l'insieme di regole per firewall che implementano la politica di sicurezza descritta utilizzando la tabella 1 allegata.
2. dare spegazione esauriente del significato di **ogni** regola indicata e del perché queste soddisfano la politica di sicurezza (Per chiarezza la politica di sicurezza è stata suddivisa in 3 punti, R1, R2, R3. Si faccia riferimento ai punti nell'indicare quali regole si riferiscono a quali punti e perché queste soddisfano il punto corrispondente);
3. qual'è la regola di default (indicare il numero nella tabella)? a cosa serve e quando viene valutata?

Esercizio 2)

Dato il seguente grafo di composizione di gruppi utente e le seguenti autorizzazioni

(G2, − read, file1)
(G3, + read, file1)
(G4, + read, file1)
(G5, + read, file1)
(G7, − read, file1)



Completare la tabella 2 indicando il segno (o i segni) delle autorizzazioni che si applicano all'utente, assumendo propagazione delle autorizzazioni lungo la gerarchia, nelle diverse politiche di risoluzione di conflitti indicate. Se ad un utente non si applica alcuna autorizzazione indicare ∅ nella cella.

Esercizio 3)
Un vaso greco datato 130 a.C. riporta la seguente sequenza di numeri:

11 32 32 11 42 33 15 42 35 43 43 35 24 34 45 24 11 42 15 43 15 42 41 15 34 44

Vista la provenienza del vaso e la sua datazione, si intuisce che la sequenza i numeri rappresenta un messaggio cifrato con la scacchiera di Polibio. Quale è il messaggio?

COGNOME **NOME** **MATR.**

Tabella 1

Num.	Direzione	Azione	Protocollo	Ind. IP Sorgente	Porta Sorgente	Ind. IP Destin.	Porta Destin.	Flag ACK
1								
2								
…								
…								
…								
…								
…								
…								
n								

Tabella 2

	a	b	c	d	e	f	g
Nothing take precedence							
Denials take precedence							
Permissions take precedence							
Most spec. take precedence							
Most spec. along a path takes precedence							