Sicurezza e Privatezza

Docente: Prof. Pierangela Samarati

Appello di Gennaio - 9 Gennaio 2004

Tempo a disposizione 2:00h

Domanda 1)

Spiegare il concetto di autenticazione e discutere le principali tecniche di autenticazione conosciute.

Domanda 2)

Caratterizzare le politiche discrezionali per il controllo dell'accesso definendo i concetti di politica aperta e politica chiusa. Dire per quale ragione si può combinare l'uso di autorizzazioni positive e negative indicando quali problemi questo può portare e descrivendo possibili politiche per la risoluzione dei conflitti. Caratterizzare le principali tecniche di implementazione. Discutere quindi il problema del Trojan Horse ed il principio alla base della politica mandatoria per la sua soluzione (suggerimento: differenza fra soggetti e utenti).

Domanda 3)

Rispondere brevemente, ma in modo completo, alle seguenti domande.

1. Spiegare il funzionamento dell'opzione di Source Routing e il motivo per cui può rappresentare un problema di sicurezza.
2. Considerate le tecniche di scanning per il riconoscimento dei sistemi operativi (OS fingerprint). Si richiede di spiegare:
   (a) quale meccanismo permette il riconoscimento di sistemi operativi diversi?
   (b) per quale motivo informazioni sul tipo di sistema operativo sono rilevanti per la sicurezza?
3. Spiegare perché nella operazione di decifratura del DES è sufficiente invertire la schedulazione delle chiave per decifrare il messaggio.
4. Dare la definizione di funzione hash one-way e illustrare le caratteristiche di queste funzioni.
5. Dato il reticolo di classificazione ottenuto dai livelli (U,C,S,TS) e dalle categorie {Research, Admin}, quale è il lub di ⟨C,{}⟩ e ⟨C,{Admin}⟩? E il glb di ⟨TS,{Research}⟩ e ⟨C,{Admim}⟩?
6. Definire i principi di separazione statica e dinamica dei privilegi. Fornire per entrambi un esempio.

Esercizio 1)

Una rete aziendale è protetta da un firewall di tipo static packet filter avente tre interfacce di rete. La prima connessa ad Internet, la seconda connessa ad una sottorete DMZ dedicata ai servizi pubblici (Web server, DNS etc.) e la terza connessa alla rete aziendale interna (workstation, database, server applicativi etc.).

Si risponda in maniera esaustiva ai seguenti punti.

1. Spiegare i motivi alla base della scelta di una tale architettura di sicurezza (Internet/DMZ/Rete interna);
2. Descrivere le caratteristiche principali di un firewall di tipo stateful (dynamic packet filter) e le differenze con la tecnologia di tipo static packet filter.
3. Definire una politica di sicurezza per autorizzare connessioni da client esterni verso:
   (a) il Web server (porta: 80/tcp).
   (b) il DNS (porte: 56/tcp e 56/udp).
   (c) Ogni altra connessione, in ingresso e in uscita, tra Internet e la sottorete DMZ dei servizi pubblici deve essere impedita (scrivere regola). **Per rispondere a questa domanda utilizzare la tabella allegata (il numero di righe non è indicativo).**
   Oltre a compilare la tabella è **obbligatorio** descrivere in maniera precisa il significato di OGNI regola definita in tabella.

Esercizio 2)

Si consideri il problema di pubblicare la tabella di frequenza sottostante che riporta il numero di aziende, per importo e tipologia, che ricevono un finanziamento dalla Comunità Europea.

Si consideri ora la regola secondo la quale non possono essere pubblicate tabelle con celle il cui valore sia uguale al totale parziale o che permetterebbe all'utente di determinare il contributo all'interno di un intervallo di 50.000 Euro.

Indicare quali righe della tabella non possono essere pubblicate e perché. Dire come queste potrebbero essere raggruppate permettendo quindi la pubblicazione riportando la tabella risultante.

Importo in migliaia di Euro

Tipologia	**0-19**	**20-39**	**40-59**	**60-79**	**80-99**	**100+**	**Totale**
Piccola	2	4	18	20	7	1	52
Media	-	-	7	9	-	-	16
Grande	-	6	30	15	4	-	55
Gigante	-	-	2	-	-	-	2

(MATRICOLA) (COGNOME) (NOME)

Tabella per l'Esercizio 1, Punto 3.(c)

Num.	Direzione	Azione	Prot.	Ind. IP Sorgente	Porta Sorgente	Ind. IP Destin.	Porta Destin.	Flag ACK
1								
2								
3								
4								
5								
6								
7								
8								
9								
10								