16 Giugno 2023

ARCHITETTURE DI CALCOLO LEZIONE 26

Esercizi sullo scheduling del disco e Sicurezza nei sistemi operativi

Esercizi sullo scheduling del disco

Esercizio sullo scheduling del disco

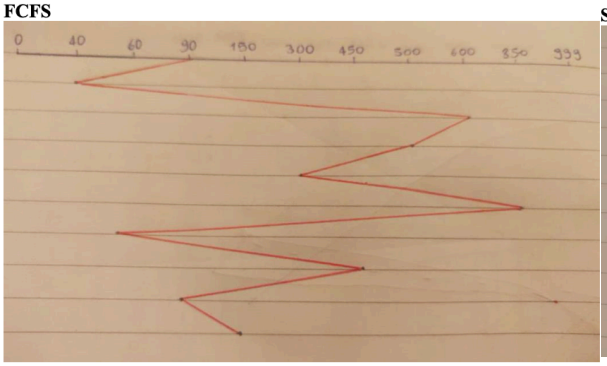
Si supponga di disporre di un disco composto da 1000 cilindri numerati da 0 a 999. Il disco sta servendo una richiesta relativa al cilindro 90 e la richiesta precedente era relativa al cilindro 50; la coda delle richieste inevase in ordine FIFO è relativa ai seguenti cilindri:

40, 600, 500, 300, 850, 60, 450, 90, 150

Assumendo come punto di partenza la posizione attuale della testina, rappresentare il movimento effettuato dal braccio del disco e calcolare la distanza totale (in cilindri) che esso percorre per soddisfare tutte le richieste inevase usando i seguenti algoritmi di scheduling:

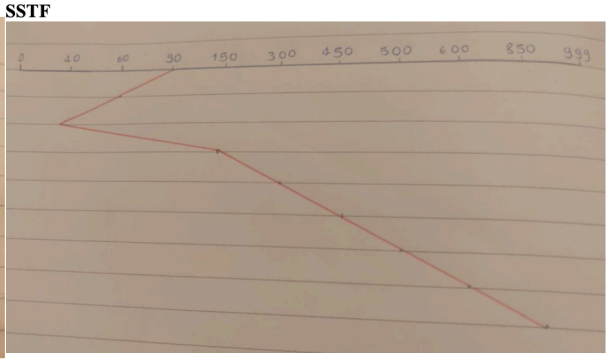
- *FCFS*
- *SSTF*
- *SCAN*
- *C-SCAN*
- *LOOK*
- *C-LOOK*

FCFS



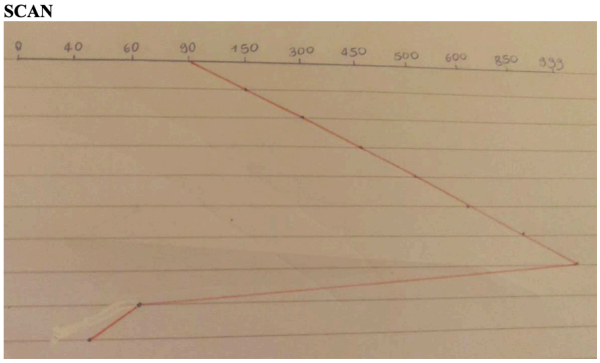
Distanza totale in cilindri: 50+560+100+200+550+790+390+360+60= 3060

SSTF



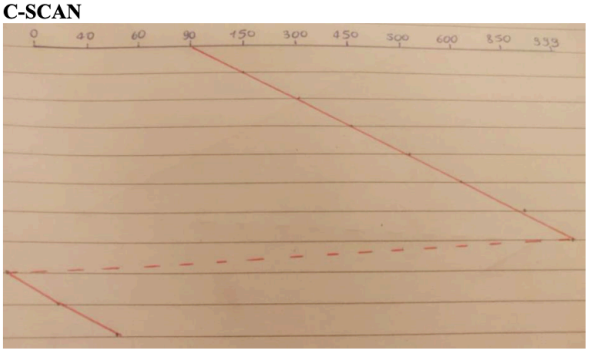
Distanza totale in cilindri (per un calcolo più rapido,): 50+810= 860

SCAN



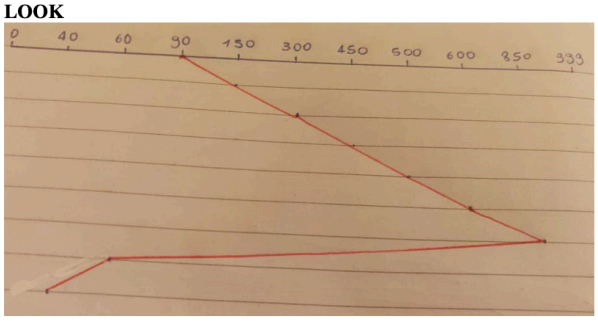
Distanza totale in cilindri:909+959=1868

C-SCAN



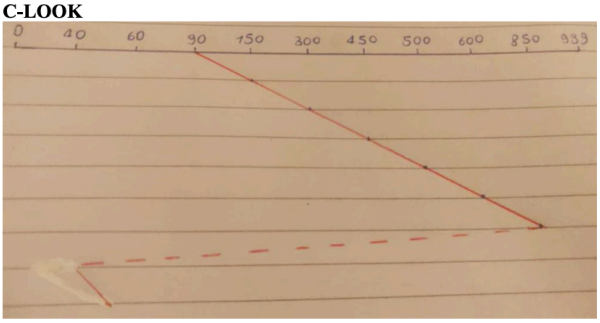
Distanza totale in cilindri:909+60= 969

LOOK



Distanza totale in cilindri: 760+810= 1570

C-LOOK



Distanza totale in cilindri:760+20= 780

Sicurezza nei sistemi operativi

Il problema della sicurezza è un problema molto importante nell'ambito dell'informatica, ed in particolare dei SO.
Ci sono tre eventi fondamentali da cui il SO si deve proteggere:

- Accessi non autorizzati.
- Modifiche o distruzioni (es. cancellare file o programmi) non autorizzate
- Introduzione accidentale di inconsistenze ed errori.

È importante sottolineare che qualsiasi cosa si faccia, non è possibile ottenere un SO totalmente sicuro e che è più facile proteggersi da abusi accidentali che da abusi volontari. Il problema della sicurezza riguarda principalmente cinque aspetti:

1. Violazione della riservatezza: qualcuno non autorizzato cerca o riesce a leggere i nostri dati. Lo scopo in molti casi è il furto di informazioni (es: dati personali, dati anagrafici, ...).
2. Compromissione dell'integrità: qualcuno cerca o riesce a modificare in modo non autorizzato un file.
3. Violazione della disponibilità: vengono cancellati dati da un server (es. sabotaggio di siti web).
4. Appropriazione del servizio: uso non autorizzato delle risorse. In questo caso il malintenzionato non vuole appropriarsi di dati sensibili ma usa macchine altrui per completare delle elaborazioni proprie.
5. Rifiuto del servizio: blocco dell'utilizzo legittimo del sistema. In inglese è detto Denial-of-service o Attacchi DOS. Per esempio, tantissimi client, coordinati fra loro, si collegano nello stesso momento a un sito web ed effettuano così tante richieste che il sito web non è in grado di servirne neanche una, finendo col negare il servizio a tutti quelli che ne dovrebbero usufruire.

Gli attacchi informatici possono essere condotti, sia attraverso la rete sia attraverso i programmi.
Le minacce legate ai programmi possono essere classificate in tre categorie:

- Malware
    - Trojan
    - Spyware

    - Ransomware
    - Trap door
    - Logic bomb
- Code injection
    - SQL injection
- Virus e worm

Malware
Il termine malware, che deriva dalla contrazione di “malicious software”, è un software capace di causare danni nei sistemi che ha infettato, sfruttandoli, disabilitandoli o danneggiandoli. Esempi di malware sono:
- Trojan
- Spyware
- Ransomware
- Trap door e Logic bomb

Trojan
Un programma che agisce in modo clandestino o malevolo, anziché eseguire semplicemente la sua funzione dichiarata; il nome deriva dal famoso “cavallo di Troia”.
Il più noto esempio di Trojan è quello che simula la finestra di login: il trojan si avvia prima del reale programma di login ed invita l’utente a digitare le proprie credenziali. Dopo averle acquisite, fa credere all’utente di aver commesso un errore nella digitazione, in modo da indurlo a inserirle nuovamente (questa volta nel reale programma di login), per poi chiudersi. Questa tecnica viene usata nelle macchine condivise.

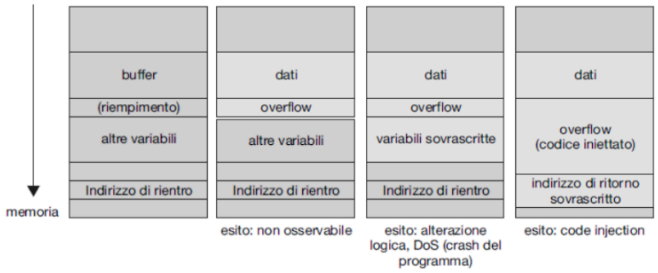
Spyware
Il termine “spy” suggerisce che lo scopo del programma è di spiare un utente. Uno spyware mira a:
- Far visualizzare annunci pubblicitari sullo schermo dell’utente, basati sulle preferenze di quest’ultimo
- Creare finestre a comparsa nel browser quando si visitano alcuni siti
- Prelevare informazioni dal sistema dell’utente per trasmetterle ad un sito di raccolta senza che l’utente ne sia a conoscenza
- Talvolta accompagna un programma che l’utente ha scelto di installare (es. plug-in dei browser)

Ransomware
È il tipo di malware che oggi rappresenta la principale minaccia economica nell’ambito della cyber-security. Il suo nome deriva dall’unione di due termini, ware (da software) e ransom (riscatto).
I ransomware criptano i dati di una persona/azienda, tramite un sistema di chiave pubblica e chiave privata, per poi richiede un riscatto in bitcoin; quando questo sarà saldato, la vittima riceverà la chiave di decifratura.

Trap door
È un tipo di malware in cui il progettista di un programma o di un sistema lascia nel programma un buco segreto a cui solo lui può accedere.
Uno dei motivi per cui si crea una trap door è che, se colui che ha commissionato lo sviluppo del programma, dopo averlo ricevuto, non completa il pagamento, il programmatore è in grado di disabilitare il programma a distanza.
Un sottotipo di trap door è la logic bomb, che si attiva solo al verificarsi di uno specifico insieme di condizioni logiche.

Principio del minimo privilegio

Il modo più efficace per difendersi dagli attacchi informatici è far rispettare ai software il principio del minimo privilegio.
Ideato da Jerome H. Saltzer nel 1974, il principio del minimo privilegio prevede che:
"in un sistema, ogni programma e ogni utente dotato di privilegi dovrebbero operare con il minimo privilegio necessario per completare il proprio lavoro".



Code injection
Un'ulteriore tecnica per ottenere l'accesso ad un computer non proprio è il code injection, in cui rientrano il buffer overflow e l'SQL injection.

Buffer overflow
Con "overflow di un buffer" si fariferimentoall'inserimento di una quantità di dati maggiore di quanto l'array (buffer) sia capace di contenere.
Questa problematica può verificarsi solo in alcuni linguaggi, come C, che non effettuano controlli. Cosa accade?
Se si inserisce una quantità di dati maggiore di quella destinata al buffer, si va a sovrascrivere il contenuto degli array successivi, finché non si giunge all'indirizzo di rientro, la cui funzione è indicare a quale parte del codice restituire il controllo, una volta terminata la funzione. Lo scopo dell'hacker è proprio quello di inserire un nuovo indirizzo di ritorno, al posto dell'originale, che rimandi alla porzione di codice scritta dal malintenzionato e che sarà eseguita con i privilegi (es. possibilità di cancellare o modificare file) del software attaccato (il grande vantaggio di questa tecnica).
Questa problematica può essere evitata se il programmatore implementa un controllo sulla quantità di dati che è possibile inserire nell'array (per esempio, se il buffer può contenere un massimo di 256 bit, input maggiori sono da ritenere non accettabili).

SQL injection
È una tecnica usata nel caso dei siti web; infatti, quando si interroga un sito web, viene generata una query (SQL), a seguito della quale si otterrà un risultato.
L'SQL injection può essere compresa più facilmente attraverso l'esempio di seguito.

```
txtUserId = getRequestString("UserId");
txtSQL = "SELECT * FROM Users WHERE UserId = " + txtUserId;
SELECT * FROM Users WHERE UserId = 105 OR 1=1;
```

Il codice nell'immagine riceve da input un nome utente, che permetterà al programma di selezionare quello specifico utente da un database e mostrare le relative informazioni personali.
Se un utente generico inserisce nel campo dello "UserId" la stringa "105 OR 1=1", si comanda al programma di mostrare tutte le informazioni degli utenti il cui UserID è 105 o 1=1; essendo quest'ultima porzione dell'input una tautologia, essa risulterà sempre vera ed il programma andrà a mostrare tutte le informazioni di tutti gli utenti del database.
Questa problematica può essere evitata effettuando un controllo sul campo dell'UserId, imponendo delle specifiche caratteristiche all'input.

Virus e worm
Le due categorie di malware che furono sviluppate per prime sono i virus ed i worm.
I virus sono così detti per via dell'analogia con gli omonimi biologici. Il virus è una porzione di codice che si attacca, generalmente all'inizio, ad un programma già esistente cosicché, quando questo sarà avviato, verrà eseguita prima la parte dannosa del codice ed in seguito il programma vero e proprio, senza che l'utente possa accorgersi di nulla.
Questa problematica può essere risolta grazie all'uso di un antivirus, capace di individuare il codice, contenuto in un database, di tutti i virus noti e non, riconoscendo eventuali pattern (similarità).
Una caratteristica fondamentale dei virus è la capacità di replicarsi, "contagiando" altri programmi, oltre allo stesso virus dropper (programma portatore del virus).
I worm ("vermi"), invece, usano una rete per replicarsi, senza aver bisogno dell'aiuto dell'uomo. Furono inventati dallo studente americano Robert Morris nel 1988; hanno un'elevata velocità di propagazione, responsabile di danni spesso incalcolabili, come accadde col Morris worm in America che portò al blocco di tutti i sistemi dell'intera nazione con una perdita economica stimata tra $100,000 e $10,000,000.

Le minacce dei sistemi operativi
Un utente malintenzionato può scegliere vari modalità di attacco:
- di rimanere passivo e intercettare il traffico di rete (questo attacco è comunemente indicato come sniffing), la più innocente tipologia di attacco, eseguita da sempre nello spionaggio fra le nazioni. È un attacco non invasivo e non distruttivo;
- di assumere un ruolo più attivo, mascherando il proprio indirizzo IP e potendo, così, impersonare qualcun altro all'interno di una rete (spoofing), non è un attacco difficile da effettuare;
- di diventare un man-in-the-middle (uomo nel mezzo) completamente attivo, che intercetta ed eventualmente modifica le transazioni tra due soggetti comunicanti, ricevendo i dati dal

mittente, modificandoli e reindirizzarli al destinatario o si può sostituire completamente a una delle due parti nella comunicazione.

Un altro tipo di attacco è il denial-of-service(DoS): tali attacchi non mirano a ottenere informazioni o a sottrarre risorse, bensì a impedire l'uso corretto di un sistema o di una funzionalità. Gli attacchi sono distribuiti su più nodi per attaccare uno stesso sistema. In una fase precedente, dei virus hanno attaccato queste macchine, introducendo un meccanismo per cui in un determinato momento tutti i nodi pongono la stessa richiesta al sistema. (DDoS)
Si divide in due diverse categorie:

1. l'aggressore occupa un numero così alto di risorse di un servizio da bloccarne completamente la funzionalità;
2. il sabotaggio di una rete che ospita un servizio.

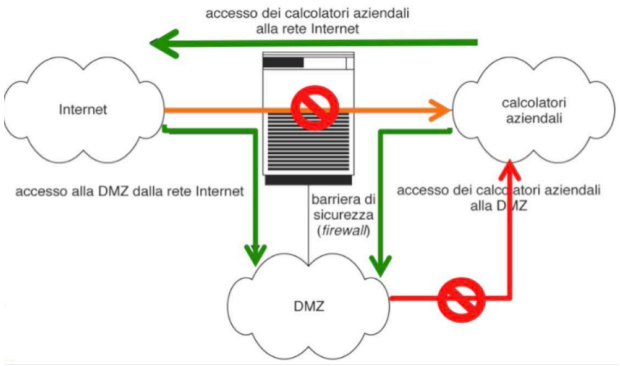
È impossibile impedire gli attacchi denial-of-service, poiché essi sfruttano gli stessi meccanismi del funzionamento normale.
RICORDA CHE: Le macchine che interrogano il sistema devono essere accese.

Azioni per monitorare i pericoli

1. Controllo di sequenze di operazioni sospette – ad esempio se vi sono numerosi tentativi di accesso usando password scorrette.
2. Audit log – ovvero la memorizzazione delle marche temporali e della tipologia per ogni accesso ad un oggetto; viene usato per il ripristino e per la definizione di misure di sicurezza. (per capire quali sono gli oggetti che sono stati compromessi dall'attacco)
3. Scan - si controlla periodicamente la presenza di "buchi", falle nella sicurezza. Esempi di buchi possono essere:
    - password facili da indovinare, di cui è semplice calcolare l'HASH (è importante impedire la creazione di password banali perché un malintenzionato, violando un semplice utente, può arrivare anche ad acquisire i privilegi dell'amministratore);
    - programmi non autorizzati in directory di sistema;
    - processi di durata molto lunga (ovviamente, non sono da considerare i programmi di sistema che sono di lunga durata per definizione);
    - protezioni di directory improprie, (es. i privilegi di lettura e scrittura sono assegnati a qualunque programma);
    - protezioni di file di sistema improprie;
    - elementi pericolosi sui percorsi di ricerca dei file;
    - modifiche ai programmi di sistema, riscontrabili dal SO tramite checksum, ovvero un codice utilizzato per garantire l'integrità di un file dopo che è stato copiato da un dispositivo ad un altro. Per i file di particolare importanza, oltre al contenuto del file, viene memorizzata anche la checksum, che viene verificata periodicamente dal sistema; in caso di incongruenze, il file viene bloccato perché considerato corrotto.

I firewall

Un firewall (“porta tagliafuoco”) è uno strumento di controllo (hardware o software) nei SO e nei router delle reti, che viene posto tra un sistema affidabile ed uno inaffidabile. Serve per monitorare e filtrare il traffico diretto. Il firewall limita e/o controlla gli accessi tra questi due tipi di sistemi (affidabile e non affidabile).
I firewall permettono di controllare accessi legati ad un particolare protocollo, per esempio, sulla base del mittente, del destinatario, dell’indirizzo http, ecc.



Osservando lo schema, si nota che il firewall è interposto tra la rete pubblica, la rete interna aziendale e la DMZ, dove si trovano i computer aziendali che devono essere accessibili dall’esterno e che non sono necessari nella produttività individuale dell’utente (come il server di posta elettronica). Il compito del firewall è di controllare blandamente la DMZ e di impedire il traffico dalla rete pubblica a quella aziendale e dalla DMZ alla rete interna, ad eccezione di quello generato in risposta alle richieste dei calcolatori aziendali.
La Demilitarized zone o zona demilitarizzata (DMZ) è una sottorete che contiene ed espone dei servizi ad una rete esterna non ritenuta sicura, come ad esempio Internet. Lo scopo di una DMZ è di proteggere la rete LAN di un'organizzazione.