Sicurezza delle Reti

Riccardo Aziani

Ottobre 2024

Indice

Capitolo 1

Standard e Concetti base

1.1 Sicurezza informatica - definizioni

Ci sono standard internazionali a cui si può fare riferimento quando si parla di sicurezza; utilizzando questi standard si può determinare se un sistema è sicuro o meno.

- insieme di approcci, linee guida, strumenti che possono essere utilizzate per proteggere l'ambiente e le risorse dell'organizzazione e degli utenti
- i beni dell'organizzazione e degli utenti comprendono i dispositivi connessi, il personale, infrastrutture, ecc. e la totalità delle informazioni trasmesse e/o archiviate nel cyberspazio
- la sicurezza informatica si impegna a garantire il raggiungimento e mantenimento delle proprietà di sicurezza dell'organizzazione contro i possibili rischi

La sicurezza informatica si può divedere in:

- **Sicurezza delle informazioni:** devono essere rispettate le proprietà come integrità, confidenzialità e disponibilità
- **Sicurezza della rete:** protezione delle reti e del loro servizio da modifiche non autorizzate; garanzia che la rete svolga sempre le sue funzioni correttamente

Le sfide della sicurezza informatica

- La sicurezza non è semplice (requisiti semplici ma meccanismi complessi)
- Nello sviluppo di un meccanismo di sicurezza, si devono sempre considerare potenziali attacchi

- Decidere dove utilizzare i meccanismi di sicurezza (fisicamente in che punto della rete e logicamente a che livello dell'architettura)
- I meccanismi di sicurezza generalmente coinvolgono più di un algoritmo o protocollo
- Battaglia tra progettista e attaccante
- Percezione di scarsi benifici dall'investemento nella sicurezza (fino a quando non si verifica un errore)
- La sicurezza richiede un monitoraggio costante
- La sicurezza è troppo spesso a posteriori (dopo che il sistema è stato progettato)
- La sicurezza avanzata può rappresentare un impedimento al funzionamento efficiente e di facile utilizzo

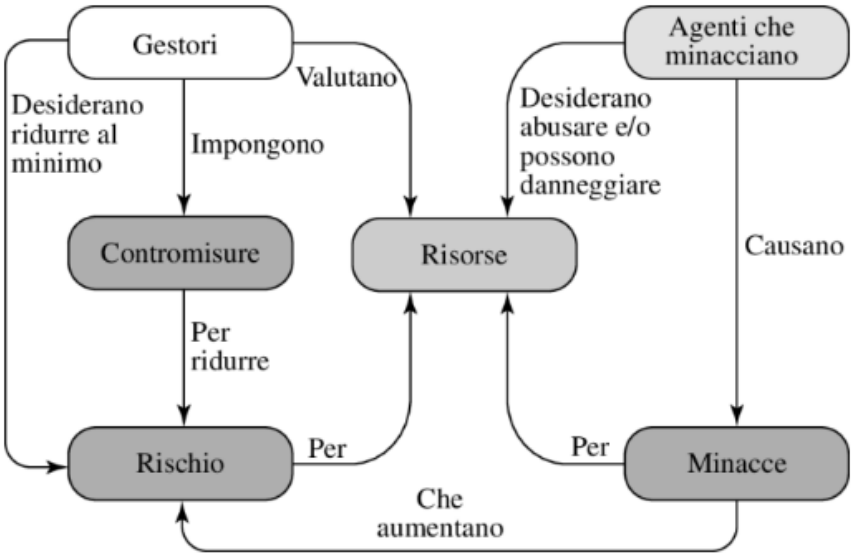


Figura 1.1: Concetti di sicurezza

- **Attacchi** alla sicurezza: qualsiasi azione che comprometta la sicurezza di un'informazione
- **Meccanismi** di sicurezza: un processo progettato per rilevare, prevenire o recuperare da un attacco
- **Servizi** di sicurezza: contrastano gli attacchi, si avvalgono di uno o più meccanismi per fornire il servizio

Attacchi passivi e attivi

- **Attacchi passivi:** NON alterano le informazioni; lo scopo dell'attacco è ottenere informazioni sui messaggi trasmessi
  - accesso al contenuto del messaggio
  - analisi del traffico di rete (la frequenza o la lunghezza dei messaggi potrebbero rivelare la natura della comunicazione)
- **Attacchi attivi:** modificano il flusso delle informazioni
  - fingere di essere qualcun'altro
  - denial of service

1.2 Minacce e conseguenze

Per threat si intende una potenziale violazione della sicurezza.

Le azioni che potrebbero causare una violazione devono essere protette o preparate; queste azione vengono chiamate **attacchi**.

Le minacce possono essere divise in quattro gruppi:

- **Divulgazione non autorizzata;** è una minaccia alla confidenzialità.
  - **esposizione**: un errore umano, software o hardware conduce alla rivelazione di dati sensibili
  - **intercettazione**
  - **inferenza**: l'attaccante è in grado di ottenere dalla sola osservazione del traffico
  - **intrusione**: un attaccante ottiene accesso a dati sensibili superando un controllo di accesso
- **Inganno;** è una minaccia all'integrità dei dati.
  - **mascheramento:** tentativo da parte dell'attacante di ottenere l'accesso a un sistema fingendosi un utente autorizzato
  - **falsificazione:** alterazione di dati validi o inserimento di dati falsi in un database
  - **ripudio:** un utente rinnega di aver inviato o ricevuto dei dati
- **Interruzione;** è una minaccia alla disponibilità o integrità di un sistema
  - **interdizione:** danneggiamento dell'hardware
  - **corruzione:** le risorse funzionano in modo non voluto
  - **ostruzione:** interferire con le comunicazioni alterandone i collegamenti

- **Usurpazione;** è una minaccia all'integrità del sistema.
  - **approprazione indebita:** ad esempio una sottrazione del servizio (DDOS)
  - **uso improprio:** ad esempio dopo che un utente ha ottenuto un accesso non autorizzato

1.3 Principi fondamentali di progettazione della sicurezza

Sono delle regole generali della sicurezza informatica.

1.3.1 Principle of Fail-Safe Defaults (default libero da fallimento)

A meno che un soggetto non abbia accesso esplicito a un oggetto, dovrebbe essergli negato l'accesso a tale oggetto.

In caso di fallimento del sistema, il sistema deve rimanere in uno stato di sicurezza

1.3.2 Principle of Economy of Mechanism (economia dei meccanismi)

I meccanismi di sicurezza dovrebbero essere il più semplice possibile; questo implica meno errori, meno controlli e testing; nella complessità si nasconde una maggiore possibilità di fallimenti o vulnerabilità.

1.3.3 Principle of Complete Mediation

Ogni accesso ad una risorsa deve sempre essere controllato da un meccanismo di sicurezza.

1.3.4 Principle of Open Design

La sicurezza di un meccanismo non dovrebbe dipendere dalla segretezza della sua progettazione o attuazione.

La sicurezza non deve essere garantita dal fatto che l'attaccante non sa come è stata progettata una cosa.

1.3.5 Principle of Separation of Privilege

Un sistema non dovrebbe concedere l'autorizzazione in base a una singola condizione; principio di separazione dei doveri.

1.3.6 Principle of Least Privilege (privilegio minimo)

A un soggetto dovrebbero essere concessi solo i privilegi di cui ha bisogno per completare il suo compito.

Un caso di eccezione può essere quando per determinate azioni, il diritto di accesso del soggetto può essere aumentato ma rilasciato immediatamente al completamento dell'azione.

1.3.7 Principle of Psychological Acceptability

I meccanismi di sicurezza non dovrebbero rendere l'accesso alla risorsa più difficile che se i meccanismi di sicurezza non fossero presenti.

1.4 Superificie di attacco

È costituita dalle vulnerabilità raggiungibili e sfruttabili in un sistema, come ad esempio:

- le porte aperte verso l'esterno
- servizi disponibili all'interno di un firewall
- codice che elabora dati in entrata
- un dipendente con accesso a dei dati sensibili (social engeneering)

Alcune superfici di attacco:

- **superificie di attacco di rete**; sono incluse vulnerabilità del protocollo di rete
- **superificie di attacco software**; sono incluse vulnerabilità nel codice delle applicazioni
- **superificie di attacco umano;** sono incluse vulnerabilità create dal personale (errori, social engeneering)

1.5 Progettazione della Sicurezza

Una strategia di sicurezza globale comprende tre aspetti:

- **Specifiche/Politiche:** cosa dovrebbe fare lo schema di sicurezza?
- **Implementazione/Meccanismi:** come funziona?
- **Correttezza/Sicurezza:** funziona davvero?

1.5.1 Implementazione della Sicurezza

Prevede quattro linee d'azione complementari:

- **Prevenzione:** uno schema di sicurezza ideale è uno schema in cui nessun attacco ha successo
- **Detection (rilevamento):** ad esempio sistemi di rilevamento di instrusioni
- **Risposta:** se viene rilevato un attacco, rispondere in modo tale da fermarlo ed evitare ulteriori danni
- **Recovery (ripristino):** ad esempio l'uso di sistemi di backup nel caso in cui venga compromessa l'integrità dei dati

Capitolo 2

Access Control

Il controllo degli accessi è un elemento centrale nella sicurezza informatica ed è definito da varie organizzazioni (ITU-T, NIST, ...).

Il controllo degli accessi implementa una politica di sicurezza che specifica chi o cosa (ad es un processo) può avere accesso a ciascuna specifica risorsa di sistema e il tipo di accesso consentito in ogni caso

Principi del AC

- **Autenticazione**: verifica validità delle credenziali.
- **Autorizzazione**: concessione dei permessi/diritti per accedere a una risorsa.
- **Auditing**: revisione e verifica indipendente delle attività.

Elementi del AC

- **Soggetto**: l'entità che accede alle risorse, come un utente o un processo.
- **Oggetto**: la risorsa protetta, che può essere un file, una directory o un programma.
- **Diritti di accesso**: definiscono le operazioni che il soggetto può eseguire sull'oggetto.

2.1 Politiche di Controllo degli Accessi

2.1.1 DAC (Controllo Discrezionale degli Accessi)

Il DAC controlla l'accesso sulla base dell'identità del entità richiedente e delle regole definite (auth).

Viene definito *discrezionale* perché un'entità potrebbe avere i privilegi di accesso che le permettono, a sua discrezione, di concedere, a un'altra entità, l'accesso a una determinata risorsa.

Spesso viene fornito utilizzando una matrice di accesso:

- elenca i soggetti in una dimensione (righe)
- elenca gli oggetti nell'altra dimensione (colonne)

La matrice spesso è sparsa.

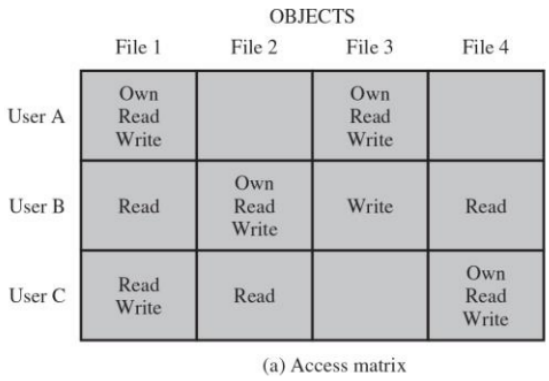


Figura 2.1: Matrice DAC

2.1.2 MAC (Controllo Obbligatorio degli Accessi)

Il MAC utilizza etichette e autorizzazioni di sicurezza per garantire che solo utenti con i giusti privilegi possano accedere a determinate risorse, è uno dei sistemi più sicuri.

Questa politica è definita obbligatoria perché è un'entità che ha l'autorizzazione accedere a una risorsa non può, solo di sua spontanea volontà, consentire a un'altra entità di farlo accedere a quella risorsa.

Vantaggi

- **Sicurezza Elevata:** a prova di manomissione; politiche di accesso non alterabili dagli utenti.
- **Automazione:** completa automatizzazione, riduzione del rischio di errori umani.
- **Integrità dei Dati:** i dati non possono essere modificati senza autorizzazione.

Svantaggi

- **Pianificazione Complessa:** progettazione iniziale che può richiedere tempo e risorse elevate.
- **Manutenzione e Aggiornamenti:** controlli e aggiornamenti regolari dei diritti di accesso.
- **Risorse Amministrative:** spesso solo admin è autorizzato a gestire i diritti di accesso.

2.1.3 RBAC (Controllo degli Accessi Basato su Ruoli)

L'accesso alle risorse è regolato in base ai ruoli degli utenti all'interno del sistema. Viene utilizzato nei sistemi organizzativi.

Ci sono quattro tipi di entità:

- **Utente:** una persona che ha accesso al sistema informatico; ogni individuo ha un ID associato
- **Ruolo:** una funzione lavorativa all'interno dell'organizzazione che controlla il sistema
- **Autorizzazione:** approvazione di una particolare modalità di accesso a uno o più oggetti
- **Sessione:** una mappatura tra un utente e un sottoinsieme attivato dell'insieme di ruoli a cui è assegnato l'utente

2.1.4 ABAC (Controllo degli Accessi Basato su Attributi)

ABAC controlla l'accesso basandosi su attributi dell'utente e condizioni ambientali.

2.2 Domini di Protezione

I domini di protezione rappresentano un insieme di oggetti con i rispettivi diritti di accesso per ciascuno di essi. Ogni utente ha un proprio dominio, e i processi generati da tale utente ereditano i suoi permessi. L'associazione tra un processo e un dominio può essere statica o dinamica:

- **User Mode**: alcune aree della memoria sono protette e certe istruzioni non sono eseguibili.
- **Kernel Mode**: è possibile eseguire istruzioni privilegiate e accedere a memoria protetta.

Il soggetto utilizza i diritti di accesso per interagire con l'oggetto in base alle politiche di sicurezza.

2.3 Access Control in Sistemi Operativi

2.3.1 UNIX Security Model

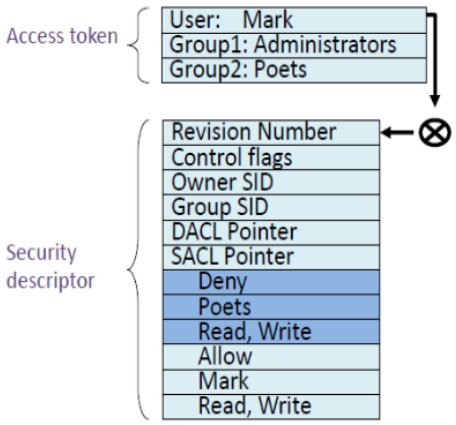
UNIX usa un modello di controllo degli accessi tramite utenti, gruppi e permessi su file.

Gli ID degli utenti (UID) e i gruppi (GID) giocano un ruolo chiave. L'utente root (UID = 0) ha accesso a tutto.

2.3.2 Windows Security Architecture

Windows ha un'architettura di sicurezza complessa costituita principalmente da:

- ACL (Access Control Lists) e SID (Security Identifiers)
- Sistema SRM (Security Reference Monitor): esegue controlli di accesso in modalità kernel
- Ogni processo ha un set di tokens chiamato *security context* che ne definisce i permessi.



Ogni oggetto ha un *security descriptor* che contiene:

- possessore e gruppo primario dell'oggetto
- diritti di accesso per gli utenti e i gruppi+

Quando un processo vuole accedere a un file oggetto, presenta il suo insieme di token (security context); Windows controlla se il security context ha accesso all'oggetto basato sul descrittore di sicurezza dell'oggetto.

2.4 Elementi di Sicurezza Specifici

2.4.1 SetUID e SetGID in UNIX

Ogni processo in un sistema ha tre diversi ID utente:

- **Effective User ID (EUID)**: determina le autorizzazioni del processo.
- **Real User ID (RUID)**: identifica l'utente che ha avviato il processo.
- **Saved User ID (SUID)**: memorizza l'EUID prima di eventuali modifiche.

Inizialmente, questi tre ID hanno lo stesso valore, corrispondente all'utente che ha avviato il processo. SetUID e SetGID permettono temporaneamente di eseguire con i privilegi del proprietario di un file.

2.4.2 MAC in Windows

Windows utilizza un sistema di controllo MAC con diversi livelli di integrità che impediscono l'accesso non autorizzato. Microsoft ha implementato livelli di integrità tramite i SID.

Capitolo 3

Security Management, Risk and Security Policy

La gestione della sicurezza è un **processo formale** per rispondere alle seguenti domande:

- *quali sono i beni da proteggere?*
- *quali sono le possibili minacce?*
- *come facciamo a contrastare le minacce?*

In ambito IT, la gestione della sicurezza si basa sulla **valutazione del rischio**.

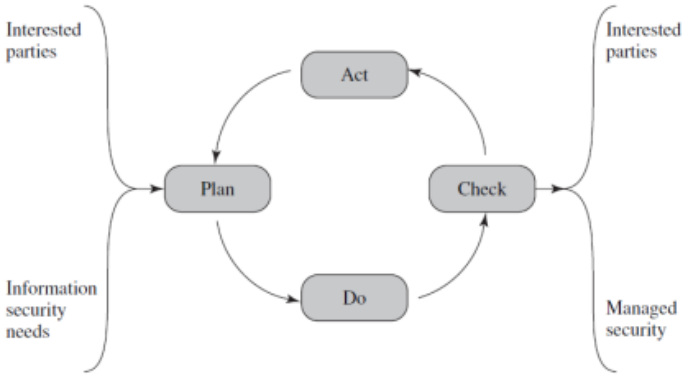
1. bisogna determinare gli obiettivi, le strategie e le politiche di sicurezza dell'organizzazione
2. eseguire una valutazione del rischio che analizzando le minacce determina i rischi risultanti
3. si devono selezionare dei controlli adeguati per proteggere in modo conveniente l'organizzazione
4. scrivere piani e procedure per attuare i controlli selezionati
5. monitorare e mantenere l'efficacia dei controlli
6. rilevare e reagire agli incidenti

La sicurezza è **lo stato in cui il rischio è inferiore al massimo rischio accettabile**.

3.1 Plan-Do-Check-Act Process Model

È uno standard (ISO 31000) che descrive un modello per la gestione della sicurezza delle informazioni, che comprende le seguenti fasi:

1. **Plan:** stabilire politiche, obiettivi e le procedure di sicurezza; si esegue una valutazione del rishcio e si sviluppa un piano di trattamento del rischio
2. **Do:** implementare il piano di trattamento del rischio
3. **Check:** monitorare e mantenere il piano di trattamento del rischio
4. **Act:** mantenere e migliorare la gestione del rischio; risposta ad incidenti o cambiamenti



3.2 Rischio

Il rischio esprime la possibilità che un attacco causi danno ad una organizzazione.

Il rischio viene valutato moltiplicando la *quantità* di danno e la probabilità che esso avvenga.

Il rischio può essere valutato utilizzando cinque categorie:

- **Damage potential:** valori dei beni interessati
- **Reproducibility:** difficoltà nel lanciare un attacco; un attacco facile da riprodurre rappresentano un rischio maggiore
- **Exploitability:** sforzo, esperienza e risorse necessarie a lanciare l'attacco
- **Affected users**
- **Discoverability:** *quando verrà rilevato l'attacco?* nel caso peggiore, non saprai mai che il sistema è stato compromesso

3.3 Vulnerabilità

È tutto ciò che può essere sfruttato per recare danno al sistema. Possono essere classificate in:

- **Critico:** possibile sfruttamento automatico
- **Moderato** sfruttamento mitigato
- **Basso:** sfruttabilità estremamente difficile

3.4 Obiettivi della sicurezza

- **Prevenzione:** impedire agli aggressori di violare la politica di sicurezza
- **Rilevamento:** rileva la violazione della politica di sicurezza da parte dell'attaccante
- **Recupero:** ferma l'attacco, valuta e ripara i danni

Capitolo 4

Malware

Un programma che viene inserito in un sistema (solitamete di nascosto) con l'intento di compromettere la riservatezza, integrità o disponibilità dei dati.

Il codice malevolo si comporta in modo inaspettato, grazie all'iniziativa di un programmatore malizioso.

4.1 Classificazione

I malware possono essere classificati:

- sulla base della propagazione (legati ad altro software, rete, social engeneering, ...)
- azioni del payload (corruzione di dati, furto di dati)
- motivazione/attori dell'attacco

Name	Description
Advanced Persistent Threat (APT)	Crimini informatici diretti contro obiettivi aziendali e politici, utilizzando un'ampia varietà di tecnologie di intrusione e malware, applicati in modo persistente ed efficace a obiettivi specifici per un periodo prolungato, spesso attribuiti a organizzazioni sponsorizzate dallo stato.
Adware	Pubblicità integrata nel software. Può provocare annunci pop-up o il reindirizzamento di un browser a un sito commerciale.
Attack kit	Insieme di strumenti per generare automaticamente nuovo malware utilizzando una varietà di meccanismi di propagazione e carico utile forniti.
Auto-rooter	Strumenti di hacker dannosi utilizzati per penetrare in nuove macchine da remoto.
Backdoor (trapdoor)	Qualsiasi meccanismo che eluda un normale controllo di sicurezza; potrebbe consentire l'accesso non autorizzato alle funzionalità di un programma o a un sistema compromesso.
Downloaders	Codice che installa altri elementi su un computer sotto attacco. Normalmente è incluso nel codice malware inserito prima in un sistema compromesso per poi importare un pacchetto malware più grande.
Drive-by-download	Un attacco che utilizza codice su un sito Web compromesso che sfrutta una vulnerabilità del browser per attaccare un sistema client quando viene visualizzato il sito.
Exploits	Codice specifico per una singola vulnerabilità o un insieme di vulnerabilità

Name	Description
Flooders (DoS client)	Utilizzato per generare un grande volume di dati per attaccare i sistemi informatici in rete, eseguendo una qualche forma di negazione del servizio (DoS) attacco.
Keyloggers	Cattura le sequenze di tasti su un sistema compromesso.
Logic bomb	Codice inserito nel malware da un intruso. Una bomba logica rimane dormiente finché non viene soddisfatta una condizione predefinita; il codice quindi attiva un carico utile.
Macro virus	Un tipo di virus che utilizza codice macro o script, generalmente incorporato in un documento o modello di documento e attivato quando il documento viene visualizzato o modificato, per essere eseguito e replicarsi in altri documenti simili.
Mobile code	Software (ad esempio, script e macro) che può essere distribuito senza modifiche a un insieme eterogeneo di piattaforme ed eseguito con la stessa semantica.
Rootkit	Insieme di strumenti hacker utilizzati dopo che l'aggressore è entrato in un sistema informatico e ha ottenuto l'accesso a livello di root.
Spammer programs	Utilizzato per inviare grandi volumi di posta elettronica indesiderata.
Spyware	Software che raccoglie informazioni da un computer e le trasmette a un altro sistema monitorando sequenze di tasti, dati sullo schermo e/o traffico di rete; o eseguendo la scansione dei file sul sistema alla ricerca di informazioni sensibili.

Name	Description
Trojan horse	Un programma per computer che sembra avere una funzione utile, ma ha anche una funzione nascosta e potenzialmente dannosa che elude i meccanismi di sicurezza, a volte sfruttando le autorizzazioni legittime di un'entità di sistema che lo invoca.
Virus	Malware che, una volta eseguito, tenta di replicarsi in un altro codice macchina o script eseguibile; quando ha successo, si dice che il codice è infetto. Quando viene eseguito il codice infetto, viene eseguito anche il virus.
Worm	Un programma per computer che può essere eseguito in modo indipendente e può propagare una versione completa e funzionante di se stesso su altri host di una rete, sfruttando le vulnerabilità del software nel sistema di destinazione o utilizzando credenziali di autorizzazione acquisite.
Zombie, bot	Programma installato su un computer infetto che viene attivato per lanciare attacchi su altri computer.

4.2 Virus

Un virus informatico è un codice informatico che può replicarsi modificando altri file o programmi per inserire codice in grado di essere replicato ulteriormente.

La **proprietà della replicazione** è ciò che distingue i virus informatici da altri tipi di malware.

Un'altra proprietà dei virus è che la replica richiede **richiede un certo tipo di assistenza da parte dell'utente** (cliccare su un allegato email, ...).

I virus cercano sempre di rimanere nell'ombra.

Composizione dei virus

Generalmente i virus sono composti da tre parti:

- **meccanismo di infezione**

- **trigger**, cioè l'evento che determina quando il payload viene attivato; è conosciuto anche come **bomba logica**
- **payload**, cioè cosa fa il virus

Fasi di un virus

I virus attraversano quattro fasi:

1. **fase dormiente:** il virus deve ancora essere attivato
2. **fase scatenante:** il virus viene attivato per svolgere la funzione per la quael era previsto
3. **fase di propagazione:** il virus inserisce una copia di sé stesso in altri programmi o aree del disco; ogni programma conterrà un clone del virus che entrerà a sua volta in fase di propagazione
4. **fase esecutiva:** la funzione viene eseguita

4.2.1 Macrovirus

Virus che si attaccano ai documenti dell'utente.
Sono minacciosi per una serie di motivi:

- è indipendente dalla piattaforma
- infetta i documenti, non porzioni di codice
- si diffondono facilmente
- più facili da scrivere

4.2.2 Classificazione dei virus

I virus possono essere classificati secondo i meccanismi che utilizzano per non essere rilevati:

- **encrypted virus:** una parte del virus crea una chiave casuale con cui cripta il resto del virus; questa chiave viene usata per decriptare quando un viene chiamato il programma infetto. Per evitare attacchi di frequenza ogni volta che il virus si replica viene usata una chiave diversa
- **stealth virus:** progettati per nascondersi dagli antivirus, usando tecniche di mutazione del codice o compressione
- **polymorphic virus:** durante la replica crea copie con la stessa funzionalità ma hanno modelli di bit diversi
- **metamorphic virus:** si riscrive completamente ad ogni iterazione, aumentando la difficoltà di rilevamento
- **compression virus:** comprimono il file eseguibile in modo che sia la versione infetta che quella non infetta abbiano la stessa lunghezza

4.3 Worm

Software analoghi ai virus ma che non hanno bisogno di un programma benigno a cui attaccarsi, ma agiscono da soli.

Hanno lo stesso funzionamento e fasi dei virus.

Attualmente i worm cercano di spaziare su più piattaforme possibili, cercando più vulnerabilità e diffondendosi velocemente. Utilizzano tecniche di polimorfismo e metamorfismo.

4.4 Drive-by-downloads

Sfruttano dei bug nelle applicazioni utente per installare malware.

Una tecnica comune sfrutta le vulnerabilità del browser: quando un utente visita un pagina web controllata dall'attaccante, scarica e installa un malware a sua insaputa sfruttando dei bug.

Questo malware attende che utenti ignari visitino la pagina Web dannosa per diffondersi sui loro sistemi.

4.5 Clickjacking

L'attaccante raccoglie i click dell'utente e lo costringe a fare una varietà di cose, come ad esempio:

- indirizzare a siti web che contengono codice dannoso
- viene posizionato un pulsante sotto ad un'altro ad insaputa dell'utente
- i click della tastiera vengono dirottati (l'utente crede di digitare da una parte ma invece digita in una porzione controllata dall'attaccante)

Si tratta sostanzialmente di dirottare i click dell'utente, utilizzando i diversi livelli di una pagina web.

4.6 Zombie & Botnet

Prende il possesso segretamente di un altro computer sfruttando i difetti del software; viene usata per lanciare indirettamente altri attacchi:

1. viene creata la rete di botnet; scansiona internet cercando di capire quali sono gli host che possono essere attaccati
2. l'attaccante installa dei *zombie agent*, ovvero dei programmi installati da remoto che danno il controllo della macchina
3. gli zombie agent fanno riferimento ad un *master*, che controlla il funzionamento della rete di macchine
4. l'attaccante dà un comando che verrà eseguito da tutte le macchine infette (DDoS, spam, keylogging, sniffing, ...)

4.7 Rootkit

Sono dei programmi che dà remoto danno l'accesso di root, dando il controllo del sistema. Superano i normali controlli di autenticazione.

Possono essere installati a diversi livelli (applicazione, kernel).

4.8 Spear Phishing

Vengono inviate mail a particolari target (impiegati di una società, ...); dopo aver studiato la vittima, e facendo affidamento al social engeneering per far apparire le email in modo convincente.

Risulta più difficile individuare questo tipo di email fasulle, sono molto mirate alla singola vittima/compagnie.

4.9 Approcci alle contromisure per i malware

Dovrebbero essere adottate diverse contromisure, come:

- assicurarsi che tutti i sistemi siano aggiornati, per ridurre il numero di vulnerabilità
- impostare controlli di accesso alle applicazioni e ai dati nel sistema, per limitare il numero di file a cui ogni utente può accedere, e di conseguenza che può infettare o corrompere

Esistono diverse azioni di mitigazione delle minacce:

- **rilevamento:** accertarsi della sua esistenza e rilevare il malware
- **identificazione:** individuare lo specifico malware
- **rimozione:** rimuovere tutte le tracce del malware in modo che non possa diffondersi ulteriormente

Capitolo 5

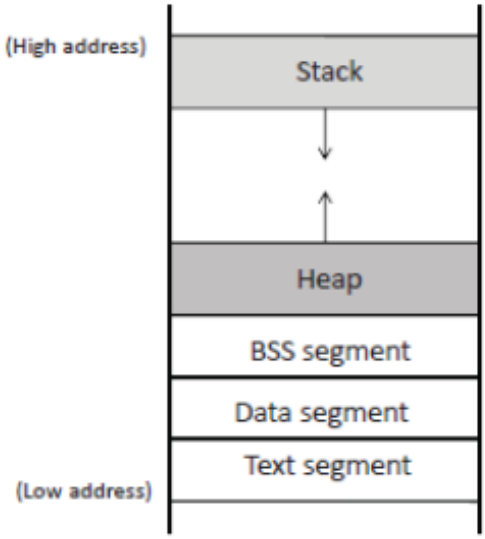
Buffer Overflow

È un meccanismo che cerca di alterare il normale funzionamento di un eseguibile, andando ad operare su aree del programma non previste dal programmatore.

5.1 Organizzazione della memoria di un programma

Quando un programma gira in memoria, ha 5 sezioni:

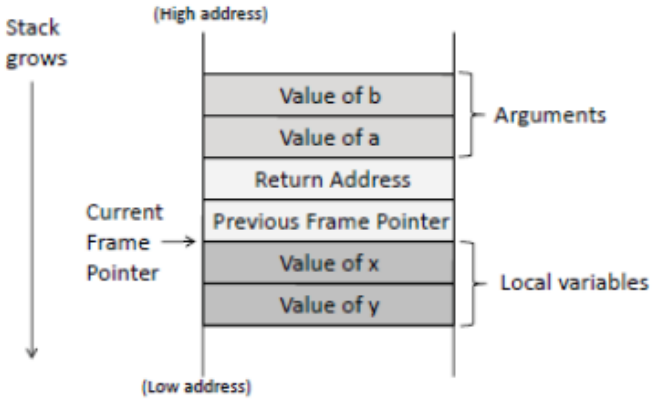
- a regione testo è fissata, contiene il codice del programma ed è a sola lettura
- La regione dati contiene i dati inizializzati e non inizializzati. Le variabili statiche vengono memorizzate in questa regione
- La regione BSS contiene static/global variabili non inizializzate
- Lo Heap è usato per dynamic memory allocation
- Lo stack è usato anche per allocare dinamicamente le variabili locali usate nelle funzioni, per passare parametri alle funzioni e per restituire valori dalle stesse.



5.2 Chiamate a funzioni

Un esempio

```
 void func(int a, int b) {
int x, y;
x = a + b;
y = a - b;
}
```



Il target dei buffer overflow è quello di sovrascrivere gli indirizzi di ritorno.