Sicurezza delle Reti

Riccardo Aziani, Lorenzo Naturale, Annalisa Pasquali

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

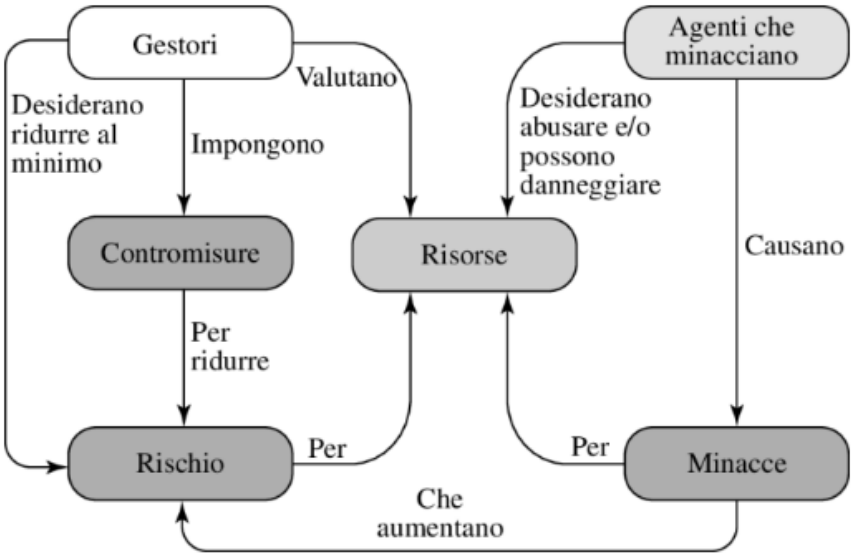


Figura 1.1: Concetti di sicurezza

- **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.

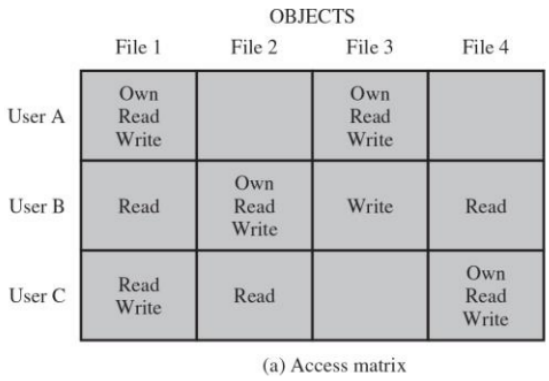


Figura 2.1: Matrice DAC

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

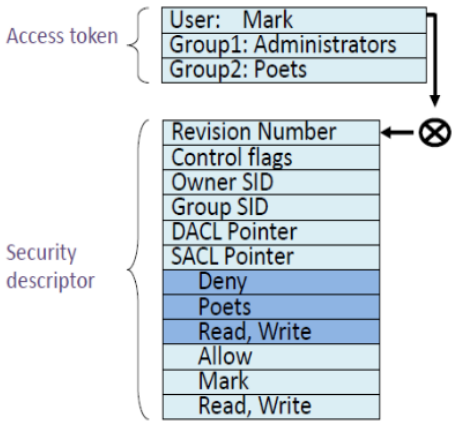
UNIX usa un modello di controllo degli accessi tramite utenti, gruppi e permessi su file.

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

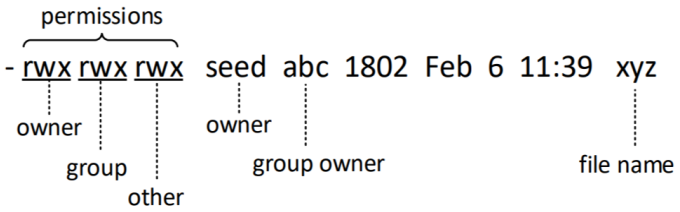
SetUID

3.1 Comandi Linux

- **Aggiungere Utenti**: from /etc/password file or *add user*. Ogni Utente ha un Unique ID e può appartenere a uno o più gruppi → definisce autorizzazioni.
- **Cambiare Utente**: *su user_name*
- **Creare Gruppo**: *sudo groupadd group_name*
- **Aggiungere Utente a Gruppo**:
  sudo usermode -a -G group_name user_name
- **Composizione Gruppi**: from /etc/group (/etc/sudoers) file or *groups* or *id*

3.2 Tipi di Accessi a File e Directory

- **R: READ - 4**
- **W: WRITE - 2**
- **X: EXECUTE - 1**



3.3 Programmi Privilegiati: Set-UID

- **Demoni**
  - processo eseguito in background, solo come root o altri utenti privilegiati.
- **Programmi Set-UID**
  - Ampiamente utilizzati nei sistemi UNIX, programma contrassegnato con un bit speciale.

3.4 Attacchi Basati su Set-UID

Meccanismo Set-UID: l'utente esegue un processo con i privilegi del proprietario del programma.

3.4.1 Privilege Escalation to execute programs:

- `cp /bin/cat ./mycat`: crea il programma `mycat` come copia di `cat`.
- `sudo chown root mycat`: cambia il proprietario di `mycat` a `root`.
- `mycat /etc/shadow`: non eseguito poiché `mycat` non ha i privilegi Set-UID.
- `sudo chmod 4755 mycat`: abilita bit Set-UID per `mycat` ($4 \rightarrow$ *EUID = RUID Process Owner*).
- `mycat /etc/shadow`: ora eseguito con privilegi elevati, consentendo l'accesso a `/etc/shadow`.

Se il programma è di proprietà di `root`, viene eseguito con i privilegi massimi (EUID = 0). Il controllo degli accessi si basa sull'EUID $\rightarrow$ identifica i privilegi del processo eseguito.

3.4.2 Privilege escalation to root shell:

- `gcc -o catall catall.c`: compila il file sorgente e genera un eseguibile chiamato `catall`.
- `sudo chown root catall`: cambia il proprietario di `catall` a `root`.
- `catall /etc/shadow`: non eseguito poiché `catall` non ha i privilegi Set-UID.
- `sudo chmod 4755 catall`: abilita bit Set-UID per `catall` ($4 \rightarrow$ *EUID = RUID Process Owner*).

- `catall /etc/shadow`: ora eseguito con privilegi elevati, consentendo l'accesso a `/etc/shadow`.
- `catall "random; /bin/sh"`: esegue il programma `catall` passando come secondo arg */bin/sh* per ottenere una shell di root se il programma è eseguito con privilegi Set-UID.

Nota: In Ubuntu 16.04, `/bin/sh` punta a `/bin/dash`, che ha una contromisura:

- il programma perde i privilegi quando viene eseguito all'interno di un processo Set-UID.

Pertanto, nell'attacco descritto, otterremo solo una shell normale. Per rimuovere questa contromisura, è possibile eseguire le seguenti operazioni:

- `sudo -ln -sf /bin/zsh /bin/sh`: prima dell'exploit, creazione link simbolico di `sh` a `zsh`:
  - **zsh non ha la stessa contromisura**
- `sudo -ln -sf /bin/dash /bin/sh`: dopo l'exploit, ripristino link simbolico originale.

3.5 Variabili d'ambiente

Un insieme di valori dinamici. Fanno parte dell'ambiente operativo in cui viene eseguito un processo.

Un possibile esempio è la variabile *PATH*.