Sicurezza dei Sistemi e delle Reti

Indice

Capitolo 1

Introduzione

1.1 Terminologia

Un **sistema** può essere visto come (anche una combinazione di):

- *hw*
- *sw*
- persone che lavorano con *hw* e *sw*
- clienti

Un **attore** può essere:

- una *persona* che *interagisce* con il sistema
- un *dispositivo* che *interagisce* con il sistema
- un *ruolo* (cliente)
- un *ruolo complesso* (Alice che finge di essere Bob)

Una rete è una configurazione di individui interconnessi. Una **rete di computer** può essere vista sotto due punti di vista:

- ***Fisico:*** una infrastruttura *hw* che connette diversi dispositivi
- ***Logico:*** un sistema che facilita lo scambio di informazioni tra applicazioni che non condividono uno spazio di memoria

1.2 Sicurezza

La sicurezza può essere intesa come il **raggiungimento di un obiettivo in presenza di un attacco**; è difficile da assicurare perché l'obiettivo è *negativo*:

- *dimostrare che Alice può accedere ad un file è facile*
- *dimostrare che nessuno oltre ad Alice può accedervi è molto più difficile*

Di norma si raggiunge con un processo **iterativo**:

- si cerca di trovare l'*anello debole* nel sistema
- si adottano delle *contromisure*
- si continua a fare *analisi* in cerca di nuove vulnerabilità

Il concetto di *sicurezza perfetta* non è raggiungibile; per discutere di sicurezza si deve definire:

- **Politica di sicurezza:** definizione di regole di sicurezza che il sistema deve rispettare
- **Modello di minaccia:** assunzioni su cosa possa fare l'avversario per penetrare nel sistema; devo comprendere la potenza dell'avversario
- **Meccanismi:** *sw* o *hw* che cercano di assicuare che la politica sia rispettata, finché l'attaccante segue il modello di minaccia

Le reti di computer sono sistemi insicuri: abbiamo un sistema complesso (*computer*) in un sistema complesso (*rete*) $\rightarrow$ è difficile prevedere da quale punto arriveranno gli attacchi e quali vettori verranno sfruttati.
Ad oggi, le motivazioni dietro agli attacchi sono principalmente:

- economiche
- politiche / militari
- attivismo

Capitolo 2

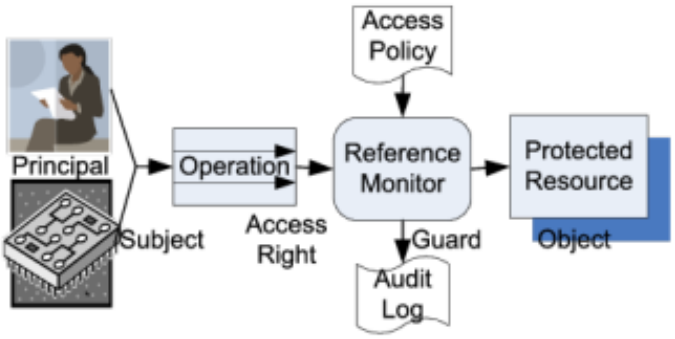
Standard e Concetti base

2.1 Standard

Ci sono diverse organizzazioni che si occupano di standard:

- NIST (*National Institute of Standars and Technology*)
- ISOC (*Internet Society*)
- ITU-T (*International Telecommunicatin Union*)
- ISO (*International Organization for Standardization*)
  - 27001: documento a cui fare riferimento per costruire un sistema di gestione della sicurezza delle informazioni che possa essere certificato da un ente indipendente
  - 27002: non è certificabile, è una raccolta di *best practices* per soddisfarre i requisiti della 27001

2.2 Reference Monitor Model - RMM



Il **reference monitor** è un **sistema dotato di una politica di controllo degli accessi**. Si occupa di:

- **autenticare chi vuole accedere**
- **autorizzare** o meno le operazioni richieste in base ai permessi
- fare **audit** → tenere un log delle azioni compiute

2.3 Definizioni

- La **sicurezza informatica** è l'insieme di strumenti, politiche, linee guida ... che possono essere utilizzate per proteggere l'ambiente e le risorse dell'organizzazione e degli utenti del cyberspazio
- I **beni dell'organizzazione e degli utenti** comprendono i dispositivi informatici connessi, personale, infrastrutture e la totalità delle informazioni trasmesse e/o archiviate nel cyberspazio
- Gli **obiettivi** generali di sicurezza comprendono *disponibilità, integrità e confidenzialità*
- *Sottoinsiemi* della sicurezza informatica:
  - **Sicurezza delle informazioni:** conservazione della CIA delle informazioni
  - **Sicurezza delle reti:** protezione delle reti e del loro servizio da modifiche non autorizzate e garanzia che la rete svolga correttamente le sue funzioni critiche

2.4 Sfide della sicurezza informatica

- Non è semplice; può avere requisiti semplici ma **meccanismi di implementazione complessi**
- Nello sviluppo di un meccanismo di sicurezza, si deve sempre **considerare potenziali attacchi**
- Le procedure utilizzate per fornire particolari servizi possono essere **controintuitive poiché complesse**
- Bisogna decidere **dove utilizzare i meccanismi di sicurezza**, sia a livello logico che a livello fisico
- I meccanismi di sicurezza in genere coinvolgono **più di un algoritmo o protocollo**
- Una battaglia **continua** tra attaccante e difensore

2.5 Principi fondamentali di progettazione della sicurezza

- **Fail-safe default:** nel caso in cui il sistema vada in default, deve rimanere in uno *stato protetto*
- **Economia di meccanismo:** i meccanismi devono essere il più semplice possibile
- **Mediazione completa:** *tutti* gli accessi devono essere controllati per assicurarsi che siano consentiti; solitamente accade che solo la prima interazione è controllata
- **Design aperto:** la sicurezza non deve dipendere dalla segretezza della sua progettazione o implementazione
- **Seperazione dei privilegi:** un sistema non dovrebbe concedere l'autorizzazione in base a *una singola* condizione
- **Minimi privilegi:** devono essere concessi il minor numero possibile di privilegi ad ogni soggetto; eventuali permessi addizionali devono essere concesso per il tempo minimo possibile
- **Accettabilità psicologica:** i meccanismi di sicurezza non dovrebbero rendere l'accesso ad una risorsa più difficile
- **Isolamento**
- **Incapsulamento**
- **Modularità**
- **Stratificazione (*layering*)**
- **Minima sorpresa:** evitare che l'utente si trovi davanti a situazioni inaspettate che potrebbero portarlo a seguire comportamenti scorretti

2.6 Superificie di attacco

Una superficie di attacco è costituita dalle **vulnerabilità raggiungibili e sfruttabili** in un sistema, come ad esempio:

- porte aperte verso l'esterno
- interfacce web
- dipendente con accesso a dati sensibili
- ...

→ è necessario **ridurre al minimo** la superificie di attacco

2.6.1 Categorie di attacco

- Superificie di attacco di **rete**: sono incluse vulnerabilità del protocollo di rete, che possono portare a DoS, interruzione dei collegamenti di comunicazioni ed altri attacchi intrusivi
- Superficie di attacco **software**: vulnerabilità nel codice delle applicazioni; un focus particolare è il software per server web
- Superificie di attacco **umano**: vulnerabilità create dal personale o da estranei, come *social engeneering*, errore umano o intrusi

2.7 Albero di attacco

Un albero di attacco è un modo ti **rappresentare le possibilità di attacco**, e quindi di progettare le **contromisure**.

2.8 Tipi di attacco

- **Passivi:** non alterano le informazioni in transito; lo scopo è ottenere informazioni sui messaggi trasmessi
- **Attivi:** modificano il flusso delle informazioni
  - *Attacco di replay:* l'attaccante osserva le informazioni e le riutilizza in un secondo momento per creare una nuova sessione di comunicazione
    $\rightarrow$ ci si tutela con *numeri casuali* e *timestamp* per, rispettivamente, controllare che i messaggi non siano già stati scambiati o che siano ancora validi
  - *DoS e DDoS*
  - ...

2.9 Implementazione della sicurezza

Quattro linee d'azione complementari:

- **Prevenzione**
- **Rilevamento**
- **Risposta** in modo da fermare un attacco e prevenire ulteriori danni
- **Ripristino** con sistemi di backup in caso l'integrità dei dati sia compromessa