Sicurezza e Privatezza

1. Basic Concepts and Principles

1.1 Fundamental goals of computer security

La **sicurezza informatica** è definita come l'arte, la scienza e la pratica ingegneristica combinata per proteggere gli asset informatici da azioni non autorizzate e le loro conseguenze, prevenendo tali azioni o rilevandole e recuperando da esse.

Obiettivi Fondamentali

1. **Confidenzialità (Confidentiality)**
   - **Definizione**: Proprietà delle informazioni non pubbliche che rimangono accessibili solo alle parti autorizzate, sia archiviate (a riposo) che in transito (in movimento).
   - **Meccanismi di Supporto**:
     - **Controllo degli Accessi**: Inclusi meccanismi applicati dal sistema operativo.
     - **Crittografia dei Dati**: Utilizzo di algoritmi crittografici con chiave segreta.
     - **Metodi Procedurali**: Accesso fisico limitato ai media di memorizzazione offline da parte di individui autorizzati.
2. **Integrità (Integrity)**
   - **Definizione**: Proprietà di dati, software o hardware di rimanere inalterati, salvo che da parte di soggetti autorizzati.
   - **Meccanismi di Supporto**:
     - **Controlli di Accesso**
     - **Checksum Crittografici**
     - **Codici di Rilevamento e Correzione degli Errori**: Per gestire errori benigni, inclusi quelli hardware.
3. **Autorizzazione (Authorization)**
   - **Definizione**: Proprietà delle risorse di calcolo di essere accessibili solo da entità autorizzate, come approvate dal proprietario delle risorse o dall'amministratore del dominio.
   - **Meccanismi di Supporto**:
     - **Controlli di Accesso**: Restrizioni su dispositivi fisici, servizi software e informazioni.
4. **Disponibilità (Availability)**
   - **Definizione**: Proprietà delle informazioni, dei servizi e delle risorse di calcolo di rimanere accessibili per uso autorizzato.
   - **Meccanismi di Supporto**:
     - **Hardware e Software Affidabili**
     - **Protezione da Eliminazione e Disruptioni Intenzionali**: Inclusi attacchi di Denial of Service (DoS).
5. **Autenticazione (Authentication)**
   - **Definizione**: Garanzia che un principal, dati o software siano genuini rispetto alle aspettative derivanti da apparenze o contesti.
   - **Tipi**:
     - **Autenticazione dell'Entità**: Conferma che l'identità di un principal coinvolto in una transazione sia come dichiarato, supportando l'autorizzazione.
     - **Autenticazione dell'Origine dei Dati**: Assicura che la fonte dei dati o del software sia come dichiarato e implica l'integrità dei dati.
6. **Responsabilità (Accountability)**
   - **Definizione**: Capacità di identificare i principal responsabili di azioni passate.
   - **Meccanismi di Supporto**:
     - **Evidenze di Transazioni o Log Elettronici**: Inclusi identificatori dei principal coinvolti, che impediscono la negazione credibile di azioni precedenti.

Principals

Definizione: Agenti che rappresentano utenti, entità comunicanti o processi di sistema.
Privilegi: Specificano le risorse a cui un principal è autorizzato ad accedere.
Identità: Importante e deve essere verificata per garantire l'autenticità e supportare l'autorizzazione.

1.2 Computer security policies and attacks

La sicurezza informatica richiede definizioni precise e un vocabolario specifico per eliminare l'ambiguità, considerata nemica della sicurezza. Essa protegge risorse o asset come informazioni, software, hardware e servizi di calcolo e comunicazione. La manipolazione dei dati informatici permette il controllo di risorse del mondo fisico, come asset finanziari, proprietà fisica e infrastrutture.

La sicurezza è formalmente definita in relazione a una **politica di sicurezza**, che specifica l'intento progettuale delle regole e delle pratiche di un sistema, delineando cosa è permesso e cosa no. La politica può:

- Identificare gli asset che necessitano protezione.
- Specificare gli utenti autorizzati ad accedere a determinati asset.
- Definire i metodi di accesso consentiti.
- Stabilire i servizi di sicurezza da fornire.
- Indicare i controlli di sistema necessari.

Idealmente, un sistema applica le regole imposte dalla sua politica. La politica può derivare dai requisiti di sicurezza del sistema o viceversa, a seconda del punto di vista e della metodologia adottata.

Un sistema si dice **non sicuro** quando non viene rispettata la policy. Una policy può essere progettata:

- top-down: si crea una policy e la si implement
- bottom-up: dopo un eventuale attacco si implementano delle pezze che riparano. Costo minore.

Teoria vs Pratica

Teoria: Una politica di sicurezza formale definisce ogni stato del sistema come autorizzato (sicuro) o non autorizzato (non sicuro). Le azioni del sistema causano transizioni di stato e una violazione della politica si verifica quando il sistema entra in uno stato non autorizzato.

Pratica: Le politiche di sicurezza sono spesso documenti informali che includono linee guida e aspettative riguardo a problemi di sicurezza noti. Formulare politiche precise è complesso e richiede tempo, e il loro valore viene spesso riconosciuto solo dopo incidenti di sicurezza.

Attacchi e agenti

Un **attacco** è l'esecuzione deliberata di azioni volte a violare la sicurezza, come il controllo non autorizzato di un dispositivo client. Gli attacchi sfruttano **vulnerabilità** specifiche del sistema, che possono includere:

- difetti di progettazione
- errori di implementazione
- problemi di configurazione o distribuzione (ad esempio, mancanza di isolamento fisico, uso continuo di password predefinite conosciute, interfacce di debug lasciate attive).

La fonte o l'agente minaccioso dietro un potenziale attacco è chiamato **avversario** e viene spesso definito **attaccante** una volta che la minaccia si concretizza in un attacco reale.

Minaccia (Threat)

Una minaccia è una combinazione di circostanze ed entità che potrebbe danneggiare gli asset, causando violazioni della sicurezza. **Minaccia Credibile**: Possiede sia mezzi capaci che intenzioni di attaccare.

Obiettivi Tipici degli Attacchi:

- **Estrazione di Informazioni**: Recupero di dati strategici o personali.
- **Interruzione dell'Integrità**: Compromissione di dati o software, inclusa l'installazione di programmi maligni.
- **Utilizzo Remoto delle Risorse**: Controllo maligno di un computer.
- **Denial of Service (DoS)**: Blocco dell'accesso alle risorse di sistema da parte degli utenti autorizzati.

Mitigazione delle Minacce

Obiettivo: Proteggere gli asset identificando ed eliminando le vulnerabilità, disabilitando i vettori di attacco.
Passaggi Chiave:

1. **Identificazione delle Vulnerabilità**: Rilevare debolezze nel sistema.

2. **Eliminazione delle Vulnerabilità**: Correggere difetti di progettazione, implementazione e configurazione.
3. **Disabilitazione dei Vettori di Attacco**: Rimuovere o proteggere i metodi di attacco.

Controlli (Controls)

Scopo: Supportare e far rispettare le politiche di sicurezza per prevenire o rilevare violazioni.
Tipi di Controlli:

- **Processi Operativi e di Gestione**: Procedure e pratiche per gestire la sicurezza.
- **Enforcement del Sistema Operativo**: Monitoraggio tramite software e controlli di accesso.
- **Meccanismi di Sicurezza Tecnici**: Dispositivi specializzati, tecniche software, algoritmi o protocolli.

1.3 Risk, risk assessment, and modeling expected losses

Il **rischio** è definito come la perdita attesa dovuta a eventi futuri dannosi, relativi a un insieme implicito di asset e su un periodo di tempo fisso. Il rischio dipende da:

- **Agenti Minacciosi**: Entità che possono eseguire attacchi.
- **Probabilità di Attacco**: La probabilità che un attacco si verifichi e abbia successo, il che richiede la presenza di vulnerabilità.
- **Perdite Attese**: Il danno o il costo derivante da un attacco riuscito.

Valutazione del Rischio

La **valutazione del rischio** comporta l'analisi dei fattori sopra menzionati per stimare il rischio complessivo. Esistono due approcci principali:

1. Valutazione del Rischio Quantitativa
   - **Obiettivo**: Calcolare stime numeriche del rischio.
   - **Sfide**: Spesso difficile da realizzare con precisione a causa della complessità e dell'incertezza.
2. Valutazione del Rischio Qualitativa
   - **Obiettivo**: Confrontare i rischi tra loro e classificarli.
   - **Utilità**: Permette di prendere decisioni informate su come prioritizzare un budget difensivo limitato tra vari asset.

Equazioni del Rischio

Un'equazione popolare per modellare il rischio è: **R = T × V × C** *(Equazione 1.1)*

Componenti dell'Equazione:

1. **T (Threat Information)**: rappresenta la probabilità che specifiche minacce vengano realizzate dagli attaccanti in un determinato periodo.
2. **V (Vulnerabilità)**: riflette l'esistenza di vulnerabilità nel sistema che possono essere sfruttate dagli attaccanti.
3. **C (Costo/Impatto)**: rappresenta il valore degli asset e il costo o l'impatto di un attacco riuscito.

Aumento del Rischio:

- **Con l'Aumento delle Minacce**: Maggiore è la probabilità che vengano lanciati attacchi.
- **Presenza di Vulnerabilità**: Necessaria per la realizzazione del rischio.
- **Valore degli Asset**: Un aumento nel valore degli asset incrementa il rischio complessivo.

Equazione Alternativa

L'equazione *(1.1)* può essere riscritta combinando T e V in una variabile **P** che denota la probabilità che un agente minaccioso esegua un'azione che sfrutta con successo una vulnerabilità: **R = P × C** *(Equazione 1.2)*

Stima delle Incognite

La **valutazione del rischio** richiede competenza e familiarità con ambienti operativi specifici e le tecnologie utilizzate. I singoli attacchi sono meglio analizzati in combinazione con vulnerabilità specifiche sfruttate dai vettori di attacco associati. La produzione di stime quantitative precise del rischio solleva molte domande, tra cui:

1. **Popolazione Accurata dei Parametri T, V e C**: Come determinare accuratamente T, V e C?

2. **Combinazione di Minacce Distinte**: Combinare minacce diverse in un unico valore T è problematico poiché potrebbero esserci innumerevoli minacce a diversi asset, con probabilità dipendenti dagli agenti dietro ciascuna minaccia.
3. **Dipendenza del Rischio da Combinazioni di Minacce, Vulnerabilità e Asset**: Per una data categoria di asset, il rischio complessivo R si calcola sommando attraverso combinazioni di minacce e vulnerabilità.
4. **Variabilità dell'Impatto C**: L'impatto o il costo C relativo a un dato asset varia a seconda dello stakeholder.

Modellazione delle Perdite Attese

Per perseguire stime quantitative, si nota che il rischio è proporzionale all'impatto per ogni occorrenza di evento. Questo permette una formula per l'**Annual Loss Expectancy (ALE)**, per un dato asset:

ALE = Σ (Fi × Ci) per i = 1..n *(Equazione 1.3)*

- **Fi**: Frequenza annualizzata stimata di eventi di tipo i.
- **Ci**: Perdita media attesa per occorrenza di un evento di tipo i.

Dettagli dell'Equazione:

- **Sommatoria su Tutti gli Eventi di Sicurezza**: La somma è fatta su tutti gli eventi di sicurezza modellati dall'indice i, che possono differire per diversi tipi di asset.
- **Frequenza e Impatto**: Considera una combinazione di minacce e vulnerabilità che permettono alle minacce di tradursi in attacchi riusciti.