UNIVERSITÀ DEGLI STUDI DI PERUGIA
Dipartimento di Matematica e Informatica

Cybersecurity

Appunti Bistarelli

Anno accademico 2022/2023

Indice

Capitolo 1

Cybersecurity

1.1 Introduzione alla sicurezza informatica

Il rapporto interno/interagenzia NIST NISTIR 7298 (Glossario di informazioni chiave Termini di sicurezza, maggio 2013) definisce il termine sicurezza informatica come segue:

Misure e controlli che garantiscono riservatezza, integrità, e disponibilità delle risorse del sistema informativo inclusi hardware, software, firmware, e le informazioni che vengono elaborate, archiviate e comunicate.

Questa definizione introduce tre obiettivi chiave che sono al centro della cybersecurity:

- **Confidentiality** (Riservatezza): conservazione delle restrizioni autorizzate all'accesso alle informazioni e divulgazione, compresi i mezzi per proteggere la privacy personale e le proprie informazione. Una perdita di riservatezza è la divulgazione non autorizzata di informazioni. Questo termine copre due concetti correlati:
  - **Data Confidentiality** : garantisce che le informazioni private o riservate non siano disponibili o divulgate a soggetti non autorizzati.
  - **Privacy**: assicura che le persone controllino o influenzino le informazioni ad essi relativi, esse possono essere raccolte e conservate, inoltre si definisce da chi e a chi possono essere divulgate.
- **Integrity** (Integrità): prevenire la modifica o la distruzione impropria delle informazioni, compresa la garanzia del non ripudio e dell'autenticità delle informazioni. Una perdita di l'integrità è la modifica o la distruzione non autorizzata di informazioni. Questo termine copre due concetti correlati:

  - **Data integrity**: garantisce che le informazioni e i programmi vengano modificati solo in modo determinato e autorizzato.
  - **System integrity**: assicura che un sistema svolga la sua funzione prevista in modo inalterato, libero da intenzionali o involontarie manipolazioni non autorizzate del sistema.

- **Availability**(Disponibilità): garantisce un accesso tempestivo e affidabile nell'utilizzo delle informazioni. Una perdita di disponibilità è l'interruzione dell'accesso o dell'uso di informazioni o un sistema informativo.

Questi tre concetti formano quella che viene spesso definita la triade della CIA. I tre concetti incarnano gli obiettivi di sicurezza fondamentali sia per i dati che per le informazioni e servizi informatici. Ad esempio, lo standard FIPS 199 del NIST (Standards for Security Categorization of Federal Information and Information Systems , febbraio 2004) elenca la riservatezza, integrità e disponibilità come i tre obiettivi di sicurezza per le informazioni e per i sistemi informativi.

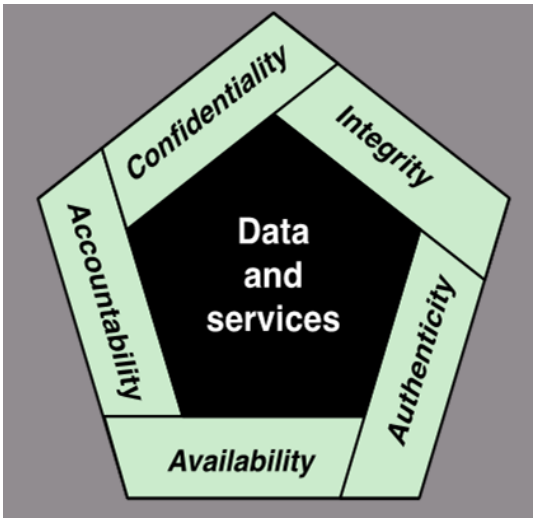


Figura 1.1: Requisiti essenziali in Cybersecurity.

Sebbene l'uso della triade della CIA per definire gli obiettivi di sicurezza sia ben consolidato, alcuni nel campo della sicurezza ritengono che siano necessari concetti aggiuntivi da presentare un quadro completo. Due dei più comunemente citati sono i seguenti:

- **Authenticity** (Autenticità): la proprietà di essere genuini e di poter essere verificati e di essere trusted. Fiducia nella validità di una trasmissione di un messaggio o di un

messaggio originatore. Ciò significa verificare che gli utenti siano chi dicono di essere e che ogni input che arriva al sistema proviene da una fonte attendibile.

- **Accountability**(Rendicontabilità): è la capacità di un sistema di identificare un singolo utente, di determinarne le azioni e il comportamento all'interno del sistema stesso. La rendicontabilità è un aspetto del controllo di accesso e si basa sulla concezione che gli individui siano responsabili delle loro azioni all'interno del sistema. Questo supporta il non ripudio, deterrenza, isolamento dei guasti, rilevamento e prevenzione delle intrusioni, il recupero post-azione in concomitanza con l'azione legale . Poiché i sistemi veramente sicuri non sono ancora un obiettivo realizzabile, dobbiamo essere in grado di tracciare una violazione della sicurezza al/ai responsabile/i. I sistemi devono tenere traccia delle loro attività per consentire successive analisi forensi per rintracciare violazioni della sicurezza o per aiutare nelle controversie sulle transazioni.

Si noti che FIPS 199 include l'autenticità sotto integrità.
La sicurezza informatica è allo stesso tempo affascinante e complessa, alcuni dei motivi sono:

1. *La sicurezza informatica non è così semplice come potrebbe sembrare a un principiante.* I requisiti sembrano essere semplici,in effetti, la maggior parte dei requisiti principali per i servizi di sicurezza possono essere definiti con etichette formate autoesplicative formate da una sola parola: riservatezza, autenticazione, non ripudio e integrità. Ma i meccanismi utilizzati per soddisfare tali requisiti possono essere piuttosto complessi, e capirli può portare a un ragionamento piuttosto sottile.

2. *Nello sviluppo di un particolare meccanismo di sicurezza o algoritmo, bisogna sempre considerare potenziali attacchi a tali funzionalità di sicurezza.* In molti casi gli attacchi di successo sono progettati guardando un problema in un modo completamente differente, dunque sfruttando una debolezza inaspettata del meccanismo.

3. *A causa del punto 2 , le procedure usate per fornire dei servizi particolari sono spesso controintuitive.* Tipicamente, un meccanismo di sicurezza è complesso e non è ovvio dalle dichiarazioni di una particolare esigenza che tali misure elaborate sono necessarie. Solo quando si prendono in considerazione i vari aspetti della minaccia si elaborano i meccanismi di sicurezza hanno un senso.

4. *I meccanismi di sicurezza in genere coinvolgono più di un particolare algoritmo o protocollo.*Richiedono inoltre che i partecipanti siano in possesso di un'informazione segreta (ad es. una chiave di crittografia), che sollevano domande sulla creazione,

distribuzione e protezione di tali informazioni segrete. Potrebbe esserci anche una dipendenza sui protocolli di comunicazione il cui comportamento può complicare il compito di sviluppare il meccanismo di sicurezza. Ad esempio, se il corretto funzionamento del meccanismo di sicurezza richiede la definizione di limiti di tempo per il tempo di transito di un messaggio dal mittente al destinatario, allora qualsiasi protocollo o rete che introduce variabili e/o ritardi imprevedibili può rendere tali termini privi di significato.

5. *La sicurezza informatica è essenzialmente una battaglia di ingegni tra un perpetratore che prova a trovare buchi e il progettista o l'amministratore che tenta di chiuderli.* Il grande vantaggio che l'attaccante ha è che lei o lui ha solo bisogno di trovare una singola vulnerabilità, mentre il progettista deve trovare e eliminare tutte le vulnerabilità per ottenere una sicurezza perfetta.

6. *La sicurezza è ancora troppo spesso un'"aggiunta" (surplus) per essere incorporata in un sistema dopo che il progetto è completo, piuttosto che essere parte integrante del processo di progettazione.*

7. *La sicurezza richiede un monitoraggio regolare, anche costante, e questo è difficile nei tempi attuali.*

8. *C'è una naturale tendenza da parte di utenti e gestori di sistema a percepire pochi vantaggi nell'investimento sulla sicurezza fino a quando non si verifica un problema.*

9. *Molti utenti e persino gli amministratori della sicurezza vedono una sicurezza forte come un ostacolo al funzionamento o all'uso efficiente di un sistema informativo o di un'informazione.*

1.1.1 Terminologie

La maggior parte delle terminologie sono riportate nel Capitolo **??** degli appunti Prof. Santini, di seguito riporto alcuni termini non citati in precedenza.

Risorsa di sistema (Asset)

Una applicazione maggiore, un sistema di supporto generale, un programma ad alto impatto,un impianto fisico, un sistema mission-critical, personale, apparecchiature o un gruppo di sistemi logicamente correlati.

Minaccia

Qualsiasi circostanza o evento che potrebbe avere un impatto negativo sulle operazioni organizzative (inclusi missione, funzioni, immagine o reputazione), risorse organizzative, individui, altre organizzazioni o la Nazione stessa attraverso un sistema informativo tramite accesso, distruzione, divulgazione, modifica non autorizzati delle informazioni , e/o negazione del servizio.

Contromisure

Dispositivo o tecniche che hanno come obiettivo la compromissione dell'efficacia operativa di attività indesiderate o contraddittorie, o la prevenzione di spionaggio, sabotaggio, furto o accesso o utilizzo non autorizzato di informazioni sensibili o di sistemi informativi.

Rischio

Una misura del grado in cui un'entità è minacciata da una potenziale circostanza o evento, e tipicamente una funzione di stima:

1. degli impatti negativi che si verificherebbero se la circostanza o l'evento si verificassero
2. della probabilità che si verifichi.

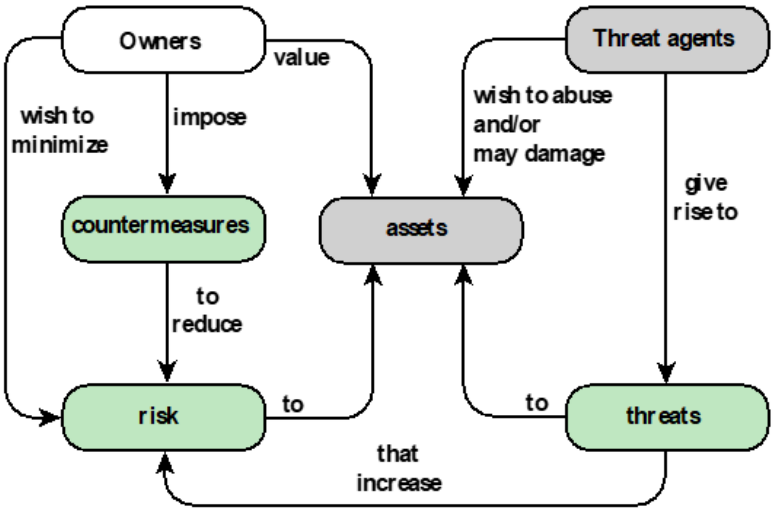


Figura 1.2: Concetti di sicurezza e le loro relazioni.

1.1.2 Asset di un sistema informatico

Gli asset di un sistema informatico possono essere suddivisi come di seguito:

- **Hardware**: compresi i sistemi informatici e altri trattamenti di dati, archiviazione dei dati,e dispositivi di comunicazione dati;
- **Software**: include il sistema operativo, le utilità di sistema e le applicazioni;
- **Data**: inclusi file e database, nonché dati relativi alla sicurezza, ad esempio file di password.
- **Strutture e reti di comunicazione**: rete locale e geografica collegamenti di comunicazione, bridge, router e così via.

1.1.3 Vulnerabilità, minacce e attacchi

Nel contesto della sicurezza, la nostra preoccupazione riguarda le vulnerabilità delle risorse del sistema. [NRC02] elenca le seguenti categorie generali di vulnerabilità di un sistema informatico o di una risorsa di rete:

- Il sistema può essere danneggiato (**corrupted**), quindi fa la cosa sbagliata o dà risposte sbagliate. Ad esempio, i valori dei dati memorizzati possono differire da quello che dovrebbero essere perché sono stati modificati in modo improprio.
- Il sistema avere delle perdite (**be leaky**). Ad esempio, qualcuno che non dovrebbe avere accesso ad alcune o a tutte le informazioni disponibili attraverso la rete ottengono tale accesso.
- Il sistema può diventare non disponibile (**unavailable**) o molto lento. Cioè, usando il sistema o la rete diventa impossibile o impraticabile.

Questi tre tipi generali di vulnerabilità corrispondono ai concetti di integrità, riservatezza e disponibilità, enumerati in precedenza. Una **minaccia** rappresenta un potenziale danno alla sicurezza di una risorsa. Un **attacco** è una minaccia che viene eseguita (azione di minaccia) e, in caso di successo, comporta una violazione indesiderata della sicurezza o a una conseguenza della minaccia. L'agente che effettua l'attacco viene definito **attaccante** o **agente di minaccia**. Possiamo distinguere gli attacchi in due tipi:

- **Attacco attivo**: un tentativo di alterare le risorse del sistema o di influenzare il funzionamento.

- **Attacco passivo**: un tentativo di imparare o di fare use delle informazioni da un sistema che non influenza le risorse di quest'ultimo.

Possiamo classificare gli attacchi in base all'origine di questi:

- **Attacco interno**: iniziato da un entità interna al perimetro di sicurezza (un "insider"). L'insider è autorizzato all'accesso alle risorse del sistema ma le usa in un modo non approvato da coloro che ne garantiscono l'accesso.

- **Attacco esterno**: iniziato fuori dal perimetro, da un utente non autorizzato o illegittimo del sistema (un "outsider"). Su Internet, potenziale aggressori esterni variano dai dilettanti "burloni" a criminali organizzati, internazionali terroristi e governi ostili.

Infine, una contromisura è qualsiasi mezzo adottato per affrontare un attacco alla sicurezza. Idealmente, una contromisura può essere escogitata per prevenire un particolare tipo di attacco dall'avere successo. Quando la prevenzione non è possibile, o in alcuni casi fallisce, l'obiettivo è rilevare l'attacco e poi riprendersi dagli effetti . Una contromisura stessa può introdurre nuove vulnerabilità. In ogni caso, vulnerabilità residue possono rimanere dopo l'imposizione di contromisure. Tali vulnerabilità possono essere sfruttato da attaccanti che rappresentano un livello di rischio residuo per gli asset. I proprietari dell'asset cercheranno di ridurre al minimo tale rischio dati altri vincoli.

Threat Consequence	Threat Action (Attack)
Unauthorized Disclosure A circumstance or event whereby an entity gains access to data for which the entity is not authorized.	**Exposure:** Sensitive data are directly released to an unauthorized entity. **Interception:** An unauthorized entity directly accesses sensitive data traveling between authorized sources and destinations. **Inference:** A threat action whereby an unauthorized entity indirectly accesses sensitive data (but not necessarily the data contained in the communication) by reasoning from characteristics or by-products of communications. **Intrusion:** An unauthorized entity gains access to sensitive data by circumventing a system's security protections.
Deception A circumstance or event that may result in an authorized entity receiving false data and believing it to be true.	**Masquerade:** An unauthorized entity gains access to a system or performs a malicious act by posing as an authorized entity. **Falsification:** False data deceive an authorized entity. **Repudiation:** An entity deceives another by falsely denying responsibility for an act.
Disruption A circumstance or event that interrupts or prevents the correct operation of system services and functions.	**Incapacitation:** Prevents or interrupts system operation by disabling a system component. **Corruption:** Undesirably alters system operation by adversely modifying system functions or data. **Obstruction:** A threat action that interrupts delivery of system services by hindering system operation.
Usurpation A circumstance or event that results in control of system services or functions by an unauthorized entity.	**Misappropriation:** An entity assumes unauthorized logical or physical control of a system resource. **Misuse:** Causes a system component to perform a function or service that is detrimental to system security.

Figura 1.3: Conseguenze delle minacce e azioni che le causano

La tabella 1.3 basata su RFC 4949, descrive quattro tipi di conseguenze ed elenca i tipi di attacchi che risultano in ciascuna conseguenza.

La divulgazione non autorizzata (Unauthorized disclosure) è una minaccia alla riservatezza. I seguenti tipi di attacchi possono portare a queste conseguenze

- **Esposizione**: quando un insider rilascia intenzionalmente informazioni sensibili a un estraneo, come ad esempio i numeri di carta di credito. Può anche essere il risultato di un errore umano, hardware o software, che si traduce nell'azione da parte di un'entità di avere l'accesso non autorizzato di dati sensibili. Ce ne sono stati numerosi casi di questo, come le università che pubblicano accidentalmente le informazioni confidenziali degli studenti sul Web.

- **Intercettazione**: l'intercettazione è un attacco comune nel contesto delle comunicazioni. Su una rete locale condivisa (LAN), come una LAN wireless o a broadcast Ethernet, qualsiasi dispositivo collegato alla LAN può ricevere una copia dei pacchetti destinati a un altro dispositivo. Su Internet, un determinato hacker può accedere al

traffico di posta elettronica e ad altri trasferimenti di dati. Tutte queste situazioni possono portare all'accesso non autorizzato ai dati.

- **Inferenza**: un esempio di inferenza è noto come analisi del traffico, in cui un avversario è in grado di ottenere informazioni osservando l'andamento del traffico una rete, come la quantità di traffico tra particolari coppie di host sulla rete. Un altro esempio è l'inferenza di informazioni dettagliate da un database di un utente che ha solo un accesso limitato, questo è realizzato da query ripetute i cui risultati combinati consentono l'inferenza.

- **Intrusione**: un esempio di intrusione è un avversario che ottiene l'accesso non autorizzato a dati sensibili superando le protezioni di controllo degli accessi del sistema.

L'inganno (Deception) è una minaccia per l'integrità del sistema o per l'integrità dei dati. I seguenti tipi di attacchi possono portare a queste conseguenze:

- **Masquerade**: un esempio di masquerade è un tentativo di accesso a un sistema da parte di un utente non autorizzato spacciandosi per uno autorizzato, questo può succedere se l'utente non autorizzato conosce l'ID di accesso e la password di un altro utente. Un altro esempio è la logica dannosa (malicious logic), come un cavallo di Troia, che appare per eseguire una funzione utile o desiderabile, ma in realtà ottiene l'accesso non autorizzato alle risorse di sistema o induce un utente a eseguire altre logiche dannose.

- **Falsificazione**: si riferisce all'alterazione o sostituzione di dati validi o all'introduzione di dati falsi in un file o database. Ad esempio, uno studente può alterare i suoi voti su un database scolastico.

- **Ripudio**: in questo caso, un utente nega l'invio di dati o nega di ricevere o possedere i dati.

L'interruzione (Disruption) è una minaccia alla disponibilità o all'integrità del sistema. I seguenti tipi di attacchi possono portare a queste conseguenze:

- **Incapacità**: questo è un attacco alla disponibilità del sistema. Ciò potrebbe verificarsi come risultato della distruzione fisica o del danneggiamento dell'hardware del sistema. Più tipicamente, un software dannoso, come Trojan, virus o worm, potrebbero operarein modo tale da disabilitare un sistema o alcuni dei suoi servizi.

- **Corruzione**: questo è un attacco all'integrità del sistema. Un Software dannoso in questo contesto potrebbe funzionare in modo tale che le risorse di sistema o i servizi funzionino in modo non intenzionale. Oppure un utente potrebbe ottenere l'accesso non autorizzato a un sistema e modificarne alcune funzioni. Un esempio di quest'ultimo è un posizionamento di una logica backdoor (backdoor logic) nel sistema per fornire il successivo accesso al sistema stesso e alle sue risorse con una procedura diversa da quella abituale.

- **Ostruzione**: un modo per ostacolare il funzionamento del sistema è interferire con le comunicazioni disabilitando i collegamenti di comunicazione o alterando la comunicazione delle informazioni di controllo. Un altro modo è sovraccaricare il sistema mettendo un carico in eccesso sul traffico di una comunicazione o sulle risorse di elaborazione.

L'usurpazione (Usurpation) è una minaccia per l'integrità del sistema. I seguenti tipi di attacchi possono portare a queste conseguenze:

- **Appropriazione indebita**: può includere il furto del servizio. Un esempio è un attacco Denial of Service distribuito, quando il software dannoso è installato su degli host da utilizzare come piattaforme per avviare il traffico verso un host di destinazione. In questo caso, il software maligno fa uso non autorizzato delle risorse del processore e del sistema operativo.

- **Uso improprio**: l'uso improprio può verificarsi per mezzo di una malicious logic o di un hacker che ha ottenuto un accesso non autorizzato a un sistema. In entrambi i casi, le funzioni di sicurezza possono essere disabilitate o contrastate.

1.1.4 Asset e minacce

Le risorse di un sistema informatico possono essere classificate come hardware, software, dati, linee e reti di comunicazione. In questa sottosezione li descriviamo brevemente e mettendoli in relazione con i concetti di integrità, riservatezza e disponibilità.

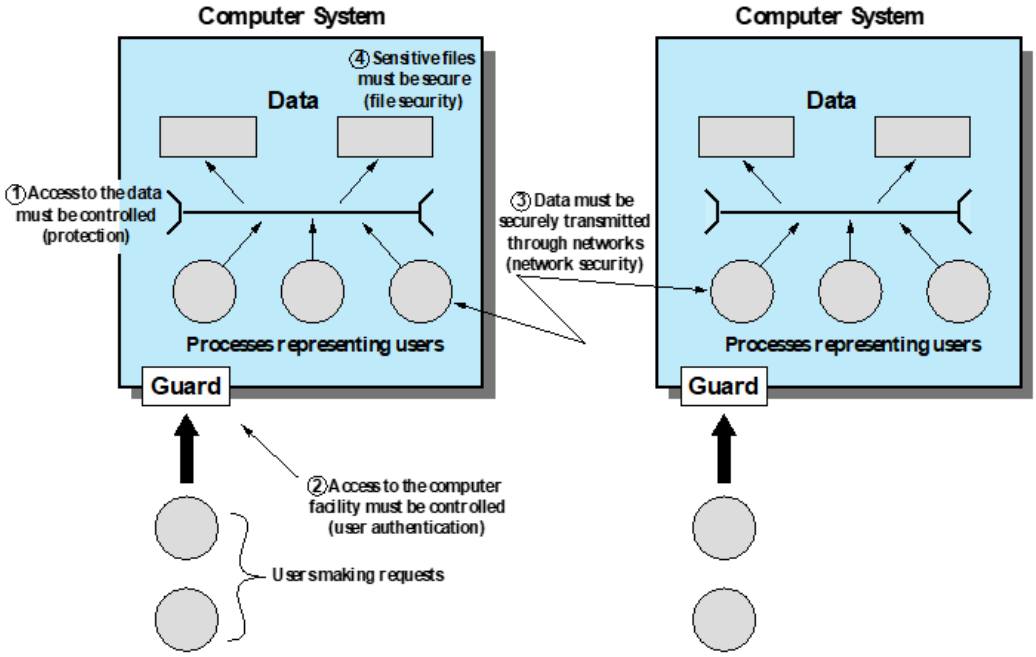


Figura 1.4: Scopo della sicurezza informatica.

Hardware. Una delle principali minacce per l'hardware del computer è la minaccia alla disponibilità. L'hardware è il più vulnerabile agli attacchi e il meno suscettibile ai controlli automatizzati. Le minacce includono danni accidentali e deliberati alle apparecchiature così come il furto. La proliferazione di personal computer e workstation e l'uso diffuso delle LAN aumenta il potenziale di perdite in quest'area. Il furto delle unità USB può portare alla perdita di riservatezza. Le misure di sicurezza fisiche e amministrative sono necessarie per far fronte a queste minacce.

Software. Il software include il sistema operativo, le utilità e l'applicazione programmi. Una delle principali minacce al software è un attacco alla disponibilità. Il Software, in particolare quello applicativo, è spesso facile da eliminare. Il software può anche essere modificato o danneggiato per renderlo inutilizzabile. Un'attenta gestione della configurazione del software, che include il mantenere dei backup della versione più recente, può mantenere una disponibilità alta. Un problema più difficile da affrontare è la modifica del software che si ha in un programma il quale funziona ancora ma che si comporta in modo diverso rispetto a prima, questa è una minaccia per l'integrità/autenticità. Rientrano in questa categoria i virus informatici e i relativi attacchi. Un ultimo problema è la

protezione contro la pirateria del software. Sebbene siano disponibili alcune contromisure, in linea di massima il problema di copie non autorizzate del software non è stata risolta.

Data. Un problema molto più diffuso è la sicurezza dei dati, che coinvolge file e altre forme di dati controllati da individui, gruppi e organizzazioni aziendali.
I problemi di sicurezza relativi ai dati sono ampi e comprendono disponibilità, segretezza e integrità. In caso di disponibilità, la preoccupazione è con la distruzione di file di dati, che può verificarsi accidentalmente o intenzionalmente. Una preoccupazione evidente per la segretezza è la lettura non autorizzata di file di dati o database, e quest'area è stata forse oggetto di ulteriori ricerche e sforzi rispetto a qualsiasi altro settore della sicurezza informatica. Una minaccia meno ovvia alla segretezza comporta l'analisi dei dati e si manifesta nell'utilizzo delle cosiddette banche dati statistiche, che forniscono informazioni di sintesi o aggregate. Presumibilmente, l'esistenza delle informazioni aggregate non minacciano la privacy delle persone coinvolte. Tuttavia, con la crescita dell'uso delle banche dati statistiche, c'è un rischio crescente per la divulgazione di informazioni personali. In sostanza, le caratteristiche di un individuo possono essere identificate attraverso un'analisi attenta. Ad esempio, se una tabella registra l'aggregato dei redditi degli intervistati A, B, C e D e un altro registra l'aggregato dei redditi di A, B, C, D ed E, la differenza tra i due aggregati sarebbe il reddito di E. Questo problema è esasperato dal desiderio crescente di combinare set di dati. In molti casi, abbinando diversi set di dati per coerenza tra i diversi livelli di aggregazione è necessario l'accesso alle singole unità. Pertanto, le singole unità, che sono oggetto di problemi di privacy, sono disponibili in varie fasi del trattamento dei set di dati. Infine, l'integrità dei dati è una delle principali preoccupazioni nella maggior parte delle installazioni.Le modifiche ai file di dati possono avere conseguenze che vanno da minori a disastrose.

1.1.5 Attacchi passivi e attivi

Gli attacchi alla sicurezza della rete possono essere classificati come attacchi passivi e attacchi attivi. Un attacco passivo tenta di imparare o fare uso delle informazioni del sistema, ma non influisce sulle risorse di quest'ultimo. Un attacco attivo tenta di alterare le risorse di sistema o di influenzare il loro funzionamento.

Attacchi passivi

Gli **attacchi passivi** generalmente riguardano l'intercettazione o il monitoraggio di trasmissioni di dati. L'obiettivo dell'attaccante è ottenere le informazioni che vengono

trasmesse. Due tipi di attacchi passivi sono il rilascio del contenuto dei messaggi e dell'analisi del traffico.

Rilascio dei contenuti di un messaggio Il **rilascio dei contenuti** del messaggio è facilmente comprensibile. Una conversazione telefonica, un messaggio di posta elettronica e un file trasferito possono contenere dati sensibili o informazioni confidenziali. Vorremmo impedire a un avversario di imparare il contenuto di queste trasmissioni.

Analisi del traffico. Un secondo tipo di attacco passivo, **l'analisi del traffico**, è più sottile. Supponiamo che noi abbiamo un modo per mascherare il contenuto dei messaggi o altre informazioni del traffico di dati, in modo che gli oppositori, anche se hanno catturato il messaggio, non possono estrarre le informazioni dal messaggio. La tecnica comune per mascherare i contenuti è la crittografia. Anche se disponiamo di una protezione crittografica, un avversario potrebbe comunque essere in grado di osservare lo schema di questi messaggi. L'avversario potrebbe determinare la posizione e l'identità degli host nella comunicazione e potrebbe osservare la frequenza e la lunghezza dei messaggi scambiati. Queste informazioni potrebbero essere utili per indovinare la natura della comunicazione che stava avvenendo.

Gli attacchi passivi sono molto difficili da rilevare perché non coinvolgono alterazione dei dati. In genere, il traffico dei messaggi viene inviato e ricevuto in un modo apparentemente normale e né il mittente né il destinatario sono consapevoli che una terza parte ha letto i messaggi o osservato l'andamento del traffico. Tuttavia, è possibile prevenire il successo di questi attacchi, di solito mediante crittografia. Pertanto, l'enfasi nell'affrontare gli attacchi passivi è sulla prevenzione piuttosto che il rilevamento.

Attacchi attivi

Gli attacchi attivi comportano alcune modifiche del flusso di dati o la creazione di un falso flusso, esso può essere suddiviso in quattro categorie: replay, masquerade, modifica dei messaggi e denial of service.

Replay. Il replay comporta l'acquisizione passiva di un'unità di dati e la sua successiva ritrasmissione per produrre un effetto non autorizzato.

Masquerade. Una masquerade ha luogo quando un'entità finge di essere un'entità diversa. Un attacco di questo tipo di solito include una delle altre forme di attacco attivo.

Per esempio, le sequenze di autenticazione possono essere catturate e riprodotte dopo che è avvenuta una sequenza di autenticazione valida, abilitando così un'entità autorizzata con pochi privilegi a ottenere privilegi extra impersonando un'entità che dispone di tali privilegi.

Modifica di un messaggio. La modifica dei messaggi significa semplicemente che una parte di un legittimo messaggio è alterato, o che i messaggi sono ritardati o riordinati, per produrre un effetto non autorizzato. Ad esempio, un messaggio che afferma: "Consenti a John Smith di leggere dati di file riservati" viene modificato per dire "Consenti a Fred Brown di leggere dati di file riservati".

DOS. La negazione del servizio impedisce o inibisce il normale utilizzo o gestione delle strutture di comunicazione. Questo attacco può avere un obiettivo specifico, per esempio un'entità può sopprimere tutti i messaggi diretti a una particolare destinazione (ad esempio, la sicurezza del servizio di audit). Un'altra forma di rifiuto del servizio è l'interruzione di un'intera rete, o disabilitando la rete o sovraccaricandola di messaggi in modo da degradarne le prestazioni.
Gli attacchi attivi presentano le caratteristiche opposte degli attacchi passivi. Invece gli attacchi passivi sono difficili da rilevare, sono disponibili misure per prevenirli con successo. D'altra parte, è abbastanza difficile prevenire assolutamente gli attacchi attivi, perché per farlo richiederebbe la protezione fisica di tutte le strutture e i percorsi di comunicazione in ogni momento. Invece, l'obiettivo è rilevarli e riprendersi da qualsiasi disservizio o ritardi da essi causati. Poiché il rilevamento ha un effetto deterrente, esso può anche contribuire alla prevenzione.

1.1.6 Requisiti di sicurezza

Esistono diversi modi per classificare e caratterizzare le contromisure che possono essere utilizzate per ridurre le vulnerabilità e affrontare le minacce alle risorse di sistema. In questa sottosezione, vediamo contromisure in termini di requisiti funzionali, e seguiamo la classificazione definita in FIPS 200. Questo standard enumera 17 aree relative alla sicurezza con riguardo alla protezione della riservatezza, dell'integrità e della disponibilità delle informazioni di sistemi e le informazioni elaborate, archiviate e trasmesse da tali sistemi.

1. **Accesso controllato**: limitare l'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati, o ai dispositivi (inclusi altri

sistemi informativi) e alle tipologie di transazioni e funzioni che gli utenti autorizzati possono esercitare.

2. **Consapevolezza e Formazione**: garantire che i gestori e gli utenti dei sistemi informativi organizzativi siano consapevole dei rischi per la sicurezza associati alle proprie attività e delle leggi, dei regolamenti e delle politiche applicabili relativi alla sicurezza dei sistemi informativi organizzativi e garantire che il personale sia adeguatamente addestrato a svolgere i compiti e le responsabilità assegnate in materia di sicurezza delle informazioni.

3. **Audit e responsabilità**: creare, proteggere e conservare i record di audit del sistema informativo per consentire il monitoraggio, l'analisi, l'indagine e la segnalazione di atti illeciti, non autorizzati o di attività non appropriate del sistema informativo. Garantire inoltre che le azioni dei singoli individui nel sistema possano essere ricondotte in modo univoco a tali utenti in modo che possano essere ritenuti responsabili di esse.

4. **Certificazione, accreditamento e valutazioni di sicurezza**: valutare periodicamente i controlli di sicurezza nei sistemi informativi organizzativi per determinare se i controlli sono efficaci nella loro applicazione. Sviluppare e attuare piani d'azione volti a correggere le carenze e ridurre o eliminare le vulnerabilità in questi sistemi. Autorizzare l'esercizio dei sistemi informativi organizzativi ed eventuali connessioni associate a questi. Monitorare continuamente i controlli di sicurezza del sistema informativo per garantire la continua efficacia di essi.

5. **Gestione della configurazione**: stabilire e mantenere le configurazioni di base e gli inventari dei sistemi (inclusi hardware, software, firmware e documentazione) durante i rispettivi cicli di vita di sviluppo del sistema. Stabilire e far rispettare le impostazioni di configurazione di sicurezza per i prodotti informatici utilizzati nei sistemi.

6. **Pianificazione di emergenza**: stabilire, mantenere e implementare piani di risposta alle emergenze, operazioni di backup, e il ripristino post-disastro per i sistemi in modo da garantire la disponibilità di risorse informative critiche e continuità operativa in situazioni di emergenza.

7. **Identificazione e autenticazione**: identificare gli utenti del sistema, i processi che agiscono per conto degli utenti o dei dispositivi e autenticare (o verificare) le identità di tali utenti, processi o dispositivi, come prerequisito per consentire l'accesso ai sistemi.

8. **Risposta all'incidente**: stabilire una capacità operativa di gestione degli incidenti per le informazioni organizzative dei sistemi che includono un'adeguata preparazione, rilevamento, analisi, contenimento, recupero e un controllo delle attività di risposta dell'utente. Tracciare, documentare e segnalare gli incidenti ai funzionari appropriati e/o alle autorità.

9. **Manutenzione**: eseguire la manutenzione periodica e tempestiva dei sistemi, fornire controlli efficaci sugli strumenti, sulle tecniche, sui meccanismi e sul personale utilizzato per condurre una manutenzione del sistema informativo.

10. **Protezione dei media**: proteggere i media dei sistemi, sia cartacei che digitali, limitare l'accesso alle informazioni dei media agli utenti autorizzati e sanificare o distruggere prima i supporti del sistema informativo prima dello smaltimento o del rilascio per il riutilizzo.

11. **Protezione fisica e ambientale**: limitare l'accesso fisico dei soggetti autorizzati ai sistemi informativi, alle apparecchiature e ai rispettivi ambienti operativi. Proteggere l'impianto fisico e l' infrastruttura di supporto per i sistemi. Fornire utilità di supporto per i sistemi informativi e proteggere quest'ultimi dai rischi ambientali fornendo adeguati controlli ambientali alle strutture che li contengono.

12. **Pianificazione**: sviluppare, documentare, aggiornare periodicamente e implementare piani di sicurezza per le informazioni organizzative dei sistemi che descrivono i controlli di sicurezza esistenti o previsti e le regole di comportamento dei soggetti che accedono ai sistemi.

13. **Sicurezza del personale**: garantire che le persone che occupano posizioni di responsabilità all'interno delle organizzazioni (compresi i fornitori di servizi di terze parti) siano affidabili e soddisfino i criteri di sicurezza stabiliti per quelle posizioni. Garantire che le informazioni organizzative e i sistemi informativi siano protetti durante e dopo le azioni del personale quali licenziamenti e trasferimenti. Applicare sanzioni formali per il personale che non fa rispettare le politiche e le procedure di sicurezza dell'organizzazione.

14. **Valutazione del rischio**: valutare periodicamente il rischio per le operazioni organizzative (inclusi missioni, funzioni, immagine o reputazione), risorse organizzative e individui, risultanti dal funzionamento del sistema e il relativo trattamento, archiviazione o trasmissione di informazioni organizzative.

15. **Acquisizione di sistemi e servizi**: Allocare risorse sufficienti per proteggere adeguatamente l'organizzazione dei sistemi. Impiegare processi del ciclo di vita dello sviluppo del sistema che incorporano considerazioni sulla sicurezza. Imporre limitazioni all'utilizzo e all'installazione del software e garantire che i fornitori di terze parti adottino adeguate misure di sicurezza per proteggere le informazioni, le applicazioni e/o i servizi "esternalizzati" dall'organizzazione.

16. **Protezione del sistema e delle comunicazioni**: monitorare, controllare e proteggere le comunicazioni organizzative (vale a dire, le informazioni trasmesse o ricevute dai sistemi) ai confini esterni e interni. Impiegare progetti "architettonici", sviluppo software tecniche e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno di dei sistemi organizzativi.

17. **Integrità del sistema e delle informazioni**: identificare, segnalare e correggere le informazioni e le falle del sistema in modo tempestivo. Fornire protezione da codice dannoso in posizioni appropriate all'interno del sistema organizzativo e monitorare gli avvisi di sicurezza del sistema informativo e adottare le azioni appropriate in risposta.

Capitolo3

1.2 Principi dell'autenticazione digitale

L'autenticazione dell'utente è la base per la maggior parte dei controlli di accesso e per la responsabilità dell'utente. L'autenticazione dell'utente comprende due funzioni.

1. L'utente si identifica al sistema presentando una credenziale, come l'ID utente.
2. Il sistema verifica l'utente attraverso lo scambio di informazioni di autenticazione.

Esempio. L'utente Alice Toklas potrebbe avere l'identificatore utente ABTOKLAS. Queste informazioni devono essere memorizzate su qualsiasi server o sistema di computer che Alice desidera utilizzare, e potrebbero essere note agli amministratori di sistema e ad altri utenti. Una tipica informazione di autenticazione associata a questo ID utente è una password, che è tenuta segreta (nota solo ad Alice e al sistema). Se nessuno è in grado di ottenere o indovinare la password di Alice, allora la combinazione di ID utente e password di Alice permette agli amministratori di impostare i permessi di accesso di Alice e di controllare la sua attività. Poiché l'ID di Alice non è segreto, gli utenti del sistema possono inviarle e-mail, ma poiché la sua password è segreta, nessuno può fingere di essere Alice.

- **L'identificazione** è il mezzo con cui un utente fornisce un'identità dichiarata al sistema.
- **l'autenticazione** dell'utente è il mezzo per stabilire la validità della dichiarazione.

NIST SP 800-63-3 (Digital Authentication Guideline, ottobre 2016). Definisce l'autenticazione digitale degli utenti come il processo per stabilire la fiducia nelle identità degli utenti che sono presentate elettronicamente a un sistema informativo. I sistemi possono usare l'identità autenticata per determinare se l'individuo autenticato è autorizzato ad eseguire particolari funzioni, come le transazioni su database o l'accesso alle

risorse del sistema. In molti casi, l'autenticazione e la transazione, o altre funzioni autorizzate, avvengono attraverso una rete aperta come Internet.

1.2.1 Un modello per l'autenticazione digitale degli utenti

NIST SP 800-63-3 Definisce un modello generale per l'autenticazione dell'utente che coinvolge una serie di entità e procedure.

Il requisito iniziale per eseguire l'autenticazione dell'utente è che l'utente deve essere registrato nel sistema. La seguente è una tipica sequenza per la registrazione.

- **Un richiedente** si rivolge a un'autorità di registrazione (RA) per diventare un abbonato di un fornitore di servizi di credenziali (CSP).
- **La RA** è un'entità fidata che stabilisce e garantisce l'identità di un richiedente a un CSP
- **Il CSP** poi si impegna in uno scambio con l'abbonato. A seconda dei dettagli del sistema di autenticazione globale, il CSP rilascia una sorta di credenziale elettronica al abbonato.
- **La credenziale** è una struttura di dati che lega autorevolmente un'identità e attributi aggiuntivi a un token posseduto da un abbonato, e può essere verificata quando viene presentata al verificatore in una transazione di autenticazione.
- **Il token** potrebbe essere una chiave di crittografia o una password criptata che identifica l'abbonato. Il token può essere emesso dal CSP, generato direttamente dall'abbonato o fornito da una terza parte.

Il token e la credenziale possono essere usati in successivi eventi di autenticazione.

Table 3.1 **Identification and Authentication Security Requirements (NIST SP 800-171)**

Basic Security Requirements:
1 Identify information system users, processes acting on behalf of users, or devices.
2 Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.
Derived Security Requirements:
3 Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.
4 Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.
5 Prevent reuse of identifiers for a defined period.
6 Disable identifiers after a defined period of inactivity.
7 Enforce a minimum password complexity and change of characters when new passwords are created.
8 Prohibit password reuse for a specified number of generations.
9 Allow temporary password use for system logons with an immediate change to a permanent password.
10 Store and transmit only cryptographically-protected passwords.
11 Obscure feedback of authentication information.

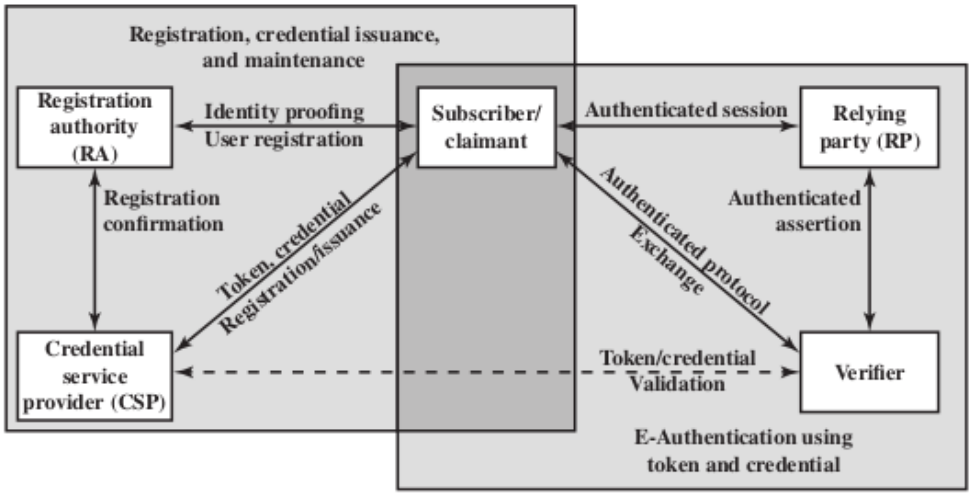


Figure 3.1 **The NIST SP 800-63-3 E-Authentication Architectural Model**

Una volta che un utente è registrato come abbonato, l'effettivo processo di autenticazione può avvenire tra l'abbonato e uno o più sistemi che eseguono l'autenticazione e, successivamente, l'autorizzazione. La parte che deve essere autenticata è chiamata richiedente e la parte che verifica tale identità è chiamata verificatore. Quando un richiedente dimostra con successo il possesso e il controllo di un token a un verificatore attraverso un protocollo di autenticazione, il verificatore può verificare che il richiedente sia il sottoscrittore indicato nella credenziale corrispondente. Il verificatore passa un'asserzione sull'identità del sottoscrittore alla parte fidata (RP).

1.2.2 Mezzi di Autenticazione

Ci sono quattro mezzi generali per autenticare l'identità di un utente, che possono essere usati da soli o in combinazione:

1. **Qualcosa che l'individuo conosce**

   Come una password, un numero di identificazione personale (PIN), o le risposte a una serie di domande prestabilite.

2. **Qualcosa che l'individuo possiede**

   Come le keycard elettroniche, smart card e chiavi fisiche. Questo tipo di autenticatore è chiamato token.

3. **Qualcosa che l'individuo è (biometria statica)**

   Come il riconoscimento per impronta digitale, retina e faccia.

4. **Qualcosa che l'individuo fa (biometria dinamica)**

   Come il riconoscimento tramite il modello di voce, le caratteristiche della scrittura a mano e il ritmo di battitura.

Tutti questi metodi, correttamente implementati e utilizzati, possono fornire un'autenticazione l'autenticazione dell'utente. Tuttavia, ogni metodo ha dei problemi. Un avversario può essere in grado di indovinare o rubare una password. Allo stesso modo, un avversario può essere in grado di falsificare o rubare un token. Un utente può dimenticare una password o perdere un token.

L'autenticazione a più fattori si riferisce all'uso di più di uno dei mezzi di autenticazione nella lista precedente. La forza dei sistemi di autenticazione è ampiamente determinata dal numero di fattori incorporati dal sistema. Le implementazioni che usano due fattori sono considerate più forti di quelle che usano un solo fattore. I sistemi che incorporano tre fattori sono più forti di quelli che ne incorporano solo due, e così via.

1.2.3 Valutazione dei rischi per l'autenticazione degli utenti

Ci sono tre concetti separati che vogliamo mettere in relazione l'uno con l'altro: livello di sicurezza, impatto potenziale e aree di rischio.

- **Livello di sicurezza**

  Un livello di sicurezza descrive il grado di certezza di un'organizzazione che un utente ha presentato una credenziale che si riferisce alla sua identità. Più specificamente, la sicurezza è definita come:

- **Il grado di fiducia nel processo di controllo** utilizzato per stabilire l'identità dell'individuo a cui la credenziale è stata rilasciata.

- **Il grado di fiducia che l'individuo** che utilizza la credenziale sia l'individuo a cui la credenziale è stata rilasciata.

SP 800-63-3 riconosce quattro livelli di sicurezza:

1. **Livello:** poca o nessuna fiducia nella validità dell'identità asserita.

   Un esempio in cui questo livello è appropriato è un consumatore che si registra per partecipare a una discussione sul sito web di un'azienda. La tipica tecnica di autenticazione a questo tipica a questo livello sarebbe un ID e una password forniti dall'utente al momento della transazione.

2. **Livello:** una certa fiducia nella validità dell'identità asserita.

   Le credenziali di livello 2 sono appropriate per un'ampia gamma di affari con il pubblico dove le organizzazioni che richiedono un'affermazione iniziale dell'identità (i cui dettagli sono verificati indipendentemente prima di qualsiasi azione). A questo livello, deve essere usato un qualche tipo di protocollo qualche tipo di protocollo di autenticazione sicura deve essere usato, insieme a uno dei mezzi di autenticazione riassunti in precedenza e discussi nelle sezioni successive.

3. **Livello:** Alta fiducia nella validità dell'identità asserita Questo livello è appropriato per permettere ai clienti o agli impiegati di accedere a servizi limitati di alto valore ma non al valore più alto.

4. **Livello:** Fiducia molto alta nella validità dell'identità asserita Questo livello è appropriato per permettere ai clienti o agli impiegati di accedere a servizi limitati di alto valore o per i quali un accesso improprio è molto dannoso.

Un concetto strettamente legato a quello di livello di sicurezza è **il potenziale d'impatto**, definisce tre livelli di impatto potenziale sulle organizzazioni o sugli individui in caso di violazione della sicurezza (nel nostro contesto, un errore nell'autenticazione autenticazione dell'utente):

Potenziale D'impatto

- **Low** Un errore di autenticazione potrebbe avere un effetto negativo limitato sulle operazioni organizzative, sulle risorse organizzative o sugli individui. Più specificamente, possiamo dire che l'errore potrebbe:
  - Causare una degradazione della capacità capacità di missione in misura e durata tali che l'organizzazione sia in grado di eseguire le sue funzioni primarie, ma l'efficacia delle funzioni è notevolmente ridotta
  - Provocare un danno minore ai beni dell'organizzazione
  - Provocare una perdita finanziaria minore perdita finanziaria per l'organizzazione o gli individui
  - Risultare in un danno minore agli individui.
- **Moderate** Un errore di autenticazione potrebbe avere un serio effetto negativo effetto. Più specificamente, l'errore potrebbe:
  - Causare una degradazione significativa nella capacità della missione in una misura e durata tale che l'organizzazione è in grado di eseguire le sue funzioni primarie, ma l'efficacia delle funzioni è significativamente.
  - Provocare un danno significativo ai beni dell'organizzazione
  - Provocare comporti una perdita finanziaria significativa
  - Comporti un danno significativo alle persone che non che non implichi la perdita di vite umane o lesioni gravi in pericolo di vita.
- **High** Un errore di autenticazione potrebbe avere un effetto negativo grave o catastrofico. L'errore potrebbe:
  - Causare una grave degradazione o perdita della capacità della missione in misura e durata tali che l'organizzazione non sia in grado di eseguire una o più delle sue funzioni primarie

- Causare un grave danno ai beni dell'organizzazione
- Causare una grave perdita finanziaria all'organizzazione o agli individui
- Causare un danno grave o catastrofico agli individui che comporta la perdita della vita o lesioni gravi che mettono in pericolo la vita.

La mappatura tra l'impatto potenziale e il livello appropriato di garanzia che è soddisfacente per affrontare l'impatto potenziale dipende dal contesto. La tabella 3.2 mostra una possibile mappatura per vari rischi a cui un'organizzazione può essere esposta. Questa tabella suggerisce una tecnica per fare la valutazione dei rischi. Per un dato sistema informativo o asset di servizio di un'organizzazione, l'organizzazione deve determinare il livello di impatto se si verifica un errore di autenticazione, usando le categorie di impatto, o aree di rischio, che sono preoccupanti. Per esempio, considerate il potenziale di perdita finanziaria se c'è un errore di autenticazione che risulta in un accesso non autorizzato a un database. A seconda della natura del del database, l'impatto potrebbe essere:

Area di Rischio

- **Low** Nel peggiore dei casi, una perdita finanziaria insignificante o irrilevante perdita per qualsiasi parte, o nel peggiore dei casi, un'organizzazione insignificante o irrilevante responsabilità.
- **Moderate** Nel peggiore dei casi, una grave perdita finanziaria irrecuperabile per qualsiasi parte, o una grave responsabilità dell'organizzazione.
- **High** Grave o catastrofica perdita finanziaria irrecuperabile per qualsiasi parte; o grave o catastrofica responsabilità dell'organizzazione.

1.3 Autenticazione basata su password

Una linea di difesa molto usata contro gli intrusi è il sistema di password. Praticamente tutti i sistemi multiutente, server basati sulla rete, siti di e-commerce basati sul web e altri servizi simili richiedono che un utente fornisca non solo un nome o un identificatore (ID) ma anche una password. Il sistema confronta la password con una password precedentemente memorizzata per quell'ID utente, conservata in un file di password di sistema. La password serve ad autenticare l'ID dell'individuo che accede al sistema. A sua volta, l'ID fornisce sicurezza nei seguenti modi:

- **L'ID determina se l'utente è autorizzato ad accedere ad un sistema.**

  In alcuni sistemi, solo coloro che hanno già un ID depositato nel sistema sono permesso di accedere.

- **L'ID determina i privilegi accordati all'utente.**

  Alcuni utenti possono avere lo stato di amministratore o "superutente" che permette loro di leggere file ed eseguire funzioni che sono particolarmente protette dal sistema operativo. Alcuni sistemi hanno account ospiti o anonimi, e gli utenti di questi account hanno privilegi più privilegi più limitati degli altri.

- **L'ID è usato in quello che viene chiamato controllo di accesso discrezionale.**

  Per esempio esempio, elencando gli ID degli altri utenti, un utente può concedere loro il permesso di leggere i file di proprietà di quell'utente.

1.3.1 Vulnerabilità delle password

- **Attacco a dizionario offline:**

  L'attaccante ottiene il file delle password di sistema e confronta gli hash delle password con gli hash delle password comunemente usate. Se viene trovata una corrispondenza, l'attaccante può ottenere l'accesso con quella combinazione ID/password.

  - **Contromisure**

    Includono controlli per prevenire l'accesso non autorizzato al file delle password, misure di rilevamento delle intrusioni per identificare una compromissione, e una rapida riemissione delle password se il file delle password viene compromesso.

- **Attacco all'account specifico**

  L'attaccante prende di mira un account specifico e presenta password indovinate finché non viene scoperta la password corretta.

  - **Contromisure**

    è un meccanismo di blocco dell'account, che blocca l'accesso all'account dopo un certo numero di tentativi di accesso falliti. La pratica tipica è non più di di cinque tentativi di accesso.

- **Attacco con password popolare**

  Una variante dell'attacco precedente consiste nell'utilizzare una password popolare e provarla contro una vasta gamma di ID utente. La tendenza di un utente è quella di scegliere una password che sia facilmente ricordabile; questo purtroppo rende la password facile da indovinare.

  - **Contromisure**

    Includono politiche per inibire la selezione da parte degli utenti di password comuni e la scansione degli indirizzi IP delle richieste di autenticazione e dei cookie del client per i modelli di invio.

- **Indovinare la password contro un singolo utente**

  L'attaccante tenta di ottenere la conoscenza del titolare dell'account e delle politiche di password del sistema e usa tale conoscenza per indovinare la password.

- **Contromisure**

  Includono la formazione e l'applicazione di politiche sulle password che rendono le password difficili da indovinare.

- **Dirottamento della stazione di lavoro** L'attaccante aspetta fino a quando una stazione di lavoro loggata non è sorvegliata.

  - **Contromisure**

    è la registrazione automatica della workstation dopo un periodo di inattività. Gli schemi di rilevamento delle intrusioni possono essere usati per rilevare i cambiamenti nel comportamento dell'utente.

- **Sfruttare gli errori dell'utente**

  Se il sistema assegna una password, allora l'utente è più probabile che la scriva perché è difficile da ricordare. Questa situazione crea il potenziale per un avversario di leggere la password scritta. Un utente può condividere intenzionalmente una password, per permettere ad un collega di condividere i file, per esempio. Inoltre, gli aggressori hanno spesso successo nell'ottenere le password utilizzando tattiche di ingegneria sociale tattiche di ingegneria sociale che ingannano l'utente o un account manager a rivelare una password. Molti sistemi informatici sono forniti con password preconfigurate per gli amministratori di sistema. A meno che queste password preconfigurate non vengano cambiate, sono facilmente indovinate.

  - **Contromisure**

    la formazione degli utenti, il rilevamento delle intrusioni e password più semplici combinate con un altro meccanismo di autenticazione.

- **Sfruttare l'uso di password multiple**

  Gli attacchi possono anche diventare molto più efficaci o dannosi se diversi dispositivi di rete condividono la stessa password o una password simile per un dato utente.

  - **Contromisure**

    includono una politica che proibisce la stessa o password simili su particolari dispositivi di rete.

- **Monitoraggio elettronico**

  Se una password viene comunicata attraverso una rete per accedere ad un sistema remoto, è vulnerabile alle intercettazioni. La semplice crittografia non risolve questo problema, perché la password criptata è, in effetti, la password e può essere osservata e riutilizzata da un avversario.

1.3.2 Uso di password con hash

Una tecnica di sicurezza delle password molto diffusa è l'uso di password con hash e di un valore di sale. Questo schema è presente in quasi tutte le varianti di UNIX e in numerosi altri sistemi operativi. Si utilizza la seguente procedura (vedi Figura 3.3). Per caricare una nuova password nel sistema, l'utente sceglie o gli viene assegnata una password. Questa password viene combinata con un valore di sale a lunghezza fissa. Nelle vecchie implementazioni, questo valore è legato al momento in cui la password è stata assegnata all'utente.

Le implementazioni più recenti utilizzano un numero pseudorandom o casuale. La password e il sale servono come input a un algoritmo di hashing per produrre un codice hash di lunghezza fissa.

L'algoritmo di hash è progettato per essere lento nell'esecuzione al fine di contrastare gli attacchi. La password hash viene memorizzata, insieme a una copia in chiaro del sale, nel file delle password dell'ID utente corrispondente. file delle password per l'ID utente corrispondente. È stato dimostrato che il metodo della password hash è sicuro contro una serie di attacchi crittoanalitici.

Quando un utente tenta di accedere a un sistema UNIX, fornisce un ID e una password (vedi Figura 3.1). e una password (vedi Figura 3.3b). Il sistema operativo utilizza l'ID per indicizzare il file delle password e recuperare "il sale" in chiaro e la password crittografata. "Il sale" e la password forniti dall'utente vengono utilizzati come input per la routine di crittografia. Se il risultato corrisponde al valore memorizzato, la password viene accettata.

Il "sale" ha tre funzioni:

1. Impedisce che le password duplicate siano visibili nel file delle password.

   Anche se due utenti scelgono la stessa password, a queste password saranno assegnati valori di valori di sale diversi. Di conseguenza, le password con hash dei due utenti saranno diverse.

2. Questo aumenta notevolmente la difficoltà degli attacchi a dizionario offline.

   Per un sale di lunghezza bits, il numero di password possibili aumenta di un fattore 2b, aumentando la difficoltà di indovinare una password la difficoltà di indovinare una password in un attacco a dizionario.

3. Diventa quasi impossibile scoprire se una persona che ha password su due o più sistemi due o più sistemi abbia usato la stessa password su tutti.

Per capire il secondo punto, considerate il modo in cui funzionerebbe un attacco a dizionario offline. L'attaccante ottiene una copia del file delle password. Supponiamo innanzitutto che il sale non venga utilizzato. L'obiettivo dell'attaccante è indovinare una singola password. A tal fine, l'attaccante sottopone alla funzione di hashing un gran numero di password probabili. Se una delle ipotesi corrisponde a uno degli hash del file, l'attaccante ha trovato una password che si trova nel file. Ma con lo schema UNIX, l'aggressore deve prendere ogni ipotesi e sottoporla alla funzione di hash una volta per ogni valore di sale nel file del dizionario, moltiplicando il numero di ipotesi da verificare. Lo schema di password UNIX è soggetto a due minacce. In primo luogo, un utente può ottenere l'accesso a una macchina utilizzando un account ospite o con altri mezzi e poi eseguire un programma per indovinare le password, chiamato password cracker, su quella macchina. L'attaccante dovrebbe essere in grado di controllare molte migliaia di possibili password con un consumo minimo di risorse. Inoltre, se l'avversario è in grado di ottenere una copia del file della password, il programma di cracking può essere eseguito a piacere su un altro computer. In questo modo, l'avversario può esaminare milioni di possibili password in un periodo di tempo ragionevole.

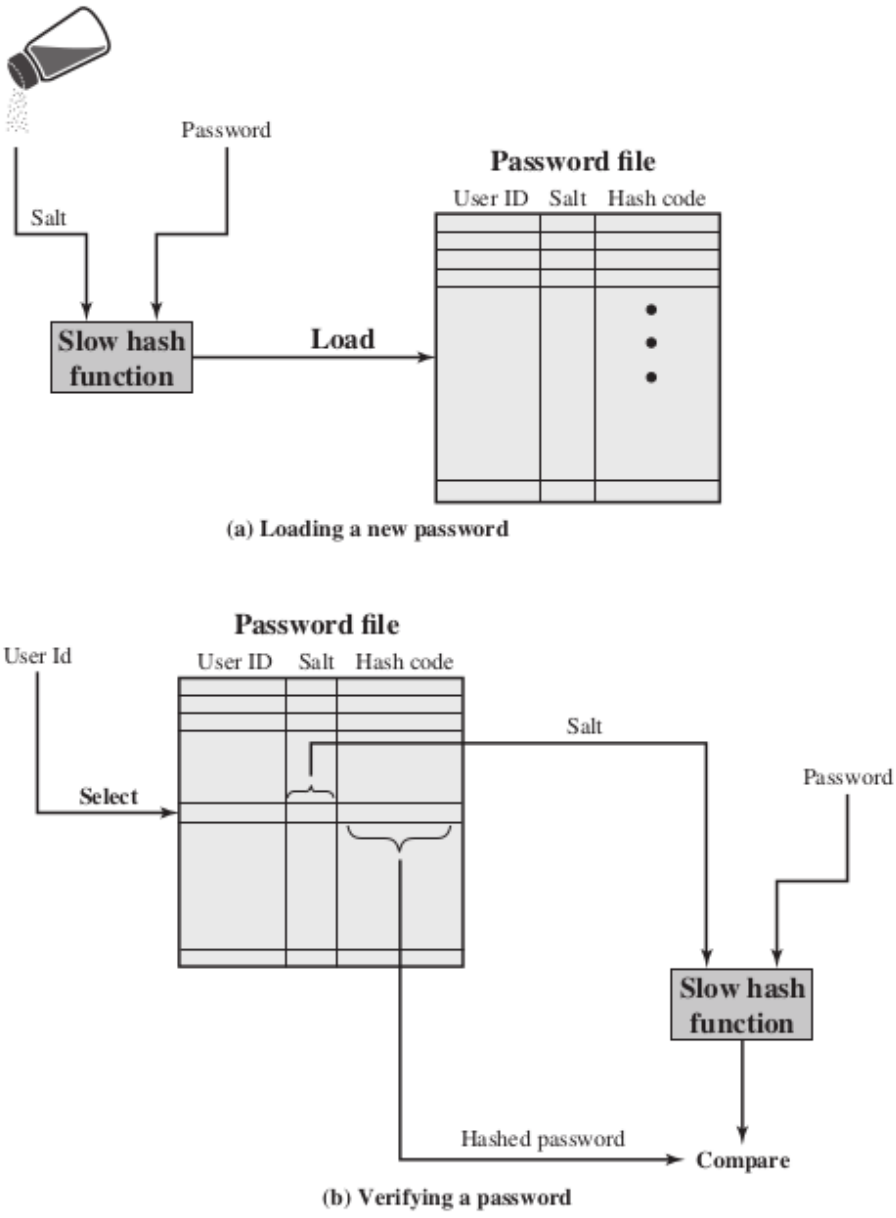


Figure 3.3 **UNIX Password Scheme**

1.3.3 Cracking delle password scelte dall'utente

Approccio Tradizionale L'approccio tradizionale all'indovinare le password, è quello di sviluppare un grande dizionario di possibili password e di provare ognuna di queste con il file delle password. Questo significa che ogni password deve essere sottoposta a un hash usando ogni valore di sale disponibile e poi confrontata con i valori di hash memorizzati. Se non viene trovata alcuna corrispondenza, il programma di cracking prova variazioni su tutte le parole del suo dizionario di password probabili. Tali variazioni includono l'ortografia a ritroso delle parole, numeri aggiuntivi o caratteri speciali, o sequenze di caratteri. Un'alternativa è quella di barattare lo spazio con il tempo precompilando i potenziali valori di hash. In questo approccio l'attaccante genera un grande dizionario di possibili password. Per ogni password, l'attaccante genera i valori di hash associati ad ogni possibile valore di sale. Il risultato è una mastodontica tabella di valori di hash nota come tabella arcobaleno.

Approccio Moderno Purtroppo, questo tipo di vulnerabilità non è diminuita negli ultimi 25 anni o giù di lì. Gli utenti stanno facendo un lavoro migliore nel selezionare le password e le organizzazioni e le organizzazioni stanno facendo un lavoro migliore nel costringere gli utenti a scegliere password più forti, un concetto noto come politica delle password complesse. Tuttavia, le tecniche di cracking delle password sono migliorate per tenere il passo. I miglioramenti sono di due tipi. In primo luogo, la capacità di elaborazione disponibile per il cracking delle password è aumentata drammaticamente. Ora utilizzati sempre più per il calcolo, i processori grafici permettono ai programmi di cracking delle password di lavorare migliaia di volte più velocemente di quanto non facessero solo un dieci anni fa su PC di prezzo simile che usavano solo CPU tradizionali. Un PC che esegue una singola GPU AMD Radeon HD7970, per esempio, può provare in media una 8,2 * 109 combinazioni di password ogni secondo, a seconda dell'algoritmo utilizzato.

La seconda area di miglioramento nel cracking delle password è l'uso di algoritmi sofisticati per generare potenziali password. I migliori risultati sono stati raggiunti studiando esempi di parole in uso. Per sviluppare tecniche che siano più efficienti ed efficaci dei semplici dizionario e degli attacchi brute-force, ricercatori e hacker hanno studiato la struttura struttura delle password. Per fare questo, gli analisti hanno bisogno di un grande pool di password di parole reali da studiare, cosa che ora hanno. La prima grande svolta è avvenuta alla fine del 2009, quando un attacco SQL injection contro il servizio di giochi online RockYou.com ha esposto 32 milioni di password in chiaro usate dai suoi membri per accedere ai loro account. Da da allora, numerosi set di file di password trapelate sono diventati disponibili per l'analisi.

1.3.4 Controllo dell'accesso ai file di password

Un modo per contrastare un attacco con password è negare all'avversario l'accesso al file delle password. Se la porzione di password hash del file è accessibile solo da un utente privilegiato, allora l'avversario non può leggerla senza conoscere già la password di un utente privilegiato. Spesso, le password hash sono tenute in un file separato dagli ID utente, indicato come un file di password ombra.
Si presta particolare attenzione a rendere il file shadow password protetto da accessi non autorizzati. Anche se la protezione del file delle password sia certamente utile, rimangono delle vulnerabilità:

- Molti sistemi, compresa la maggior parte dei sistemi UNIX, sono suscettibili di intrusioni.

  Un hacker potrebbe essere in grado di sfruttare una vulnerabilità del software nel sistema operativo sistema operativo per bypassare il sistema di controllo degli accessi abbastanza a lungo da estrarre il file di password. In alternativa, l'hacker può trovare una debolezza nel file system o nel sistema di gestione del database che permette l'accesso al file.

- Un incidente di protezione potrebbe rendere il file delle password leggibile, rendendo così compromessi tutti gli account.

- Alcuni utenti hanno account su altre macchine in altri domini di protezione, e usano la stessa password. Quindi, se le password potrebbero essere lette da chiunque su una macchina, una macchina in un'altra posizione potrebbe essere compromessa.

- Una mancanza o una debolezza nella sicurezza fisica può fornire opportunità per un hacker.

  A volte, c'è un backup del file delle password su un disco di riparazione disco di riparazione di emergenza o un disco di archiviazione. L'accesso a questo backup permette all'attaccante di leggere il file della password. In alternativa, un utente può avviare da un disco che esegue un altro sistema operativo come Linux e accedere al file da questo sistema operativo.

- Invece di catturare il file delle password di sistema, un altro approccio per raccogliere ID utente e password è attraverso lo sniffing del traffico di rete.

Quindi, una politica di protezione delle password deve integrare le misure di controllo dell'accesso con tecniche per forzare gli utenti a scegliere password difficili da indovinare.

1.3.5 Strategie selezione password

Quando non sono costretti, molti utenti scelgono una password troppo corta o troppo facile da indovinare. All'altro estremo, se agli utenti vengono assegnate password che consistono di otto caratteri stampabili scelti a caso, il cracking della password è effettivamente impossibile. Ma sarebbe quasi altrettanto impossibile per la maggior parte degli utenti ricordare le loro password. Il nostro obiettivo, quindi, è quello di eliminare le password indovinabili mentre permettendo all'utente di scegliere una password che sia memorizzabile. Quattro tecniche di base sono in uso:

1. Educazione dell'utente
2. Password generate dal computer
3. Controllo reattivo delle password
4. Politica delle password complesse

Gli utenti possono essere informati dell'importanza di usare password difficili da indovinare e possono essere fornire delle linee guida per la selezione di password forti. Questa strategia di educazione degli utenti è improbabile che abbia successo nella maggior parte delle installazioni, in particolare dove c'è una grande una vasta popolazione di utenti o molto turnover. Molti utenti semplicemente ignoreranno le linee guida. Altri possono non essere buoni giudici di ciò che è una password forte. Per esempio, molti utenti (erroneamente) credono che invertire una parola o scrivere in maiuscolo l'ultima lettera renda una password indovinabile

1.4 Autenticazione Basata sui token

Gli oggetti che un utente possiede ai fini dell'autenticazione sono chiamati token.

1.4.1 Memory Cards

Le **Memory Cards** possono immagazzinare ma non elaborare dati.

La più comune di queste carte è la carta bancaria con una banda magnetica sul retro. Una banda magnetica può memorizzare solo un semplice codice di sicurezza, che può essere letto (e sfortunatamente riprogrammato) da un economico lettore di carte. Ci sono anche schede di memoria che includono una memoria elettronica interna. Le carte di memoria possono essere usate da sole per

- l'accesso fisico, come ad esempio in una stanza d'albergo.
- Per autenticazione, un utente fornisce sia la scheda di memoria che una qualche forma di password o numero di identificazione personale (PIN).

  Un'applicazione tipica è uno sportello automatico automatico (ATM). La scheda di memoria, se combinata con un PIN o una password, fornisce una sicurezza significativamente maggiore di una password da sola. Un avversario deve ottenere il possesso fisico possesso fisico della carta (o essere in grado di duplicarla) e in più deve ottenere la conoscenza del PIN.

  Tra i potenziali inconvenienti NIST SP 800-12 (An Introduction to Computer Sicurezza: The NIST Handbook, ottobre 1995) nota quanto segue:

  – **Richiede un lettore speciale**

    Questo aumenta il costo di utilizzo del token e crea l'obbligo di mantenere la sicurezza dell'hardware e del software del lettore.

  – **Perdita dei token**

    Un token perso impedisce temporaneamente al suo proprietario di ottenere l'accesso al sistema. Quindi, c'è un costo amministrativo nella sostituzione del token perso. Inoltre, se il token viene trovato, rubato o falsificato, allora un avversario deve solo determinare il PIN per ottenere un accesso non autorizzato.

  – **Insoddisfazione dell'utente**

    Anche se gli utenti possono non avere difficoltà ad accettare l'uso di una scheda di memoria per l'accesso al bancomat, il suo uso per l'accesso al computer può essere considerato scomodo.

1.4.2 Smart Cards

Un'ampia varietà di dispositivi si qualificano come token intelligenti. Questi possono essere classificati lungo quattro dimensioni che non si escludono a vicenda:

- **Caratteristiche fisiche**

  I token intelligenti includono un microprocessore incorporato. Un token intelligente che assomiglia a una carta bancaria è chiamato smart card. Altri smart token possono assomigliare a calcolatrici, chiavi o altri piccoli oggetti portatili.

- **Interfaccia Utente**

  Le interfacce manuali includono una tastiera e un display per l'interazione uomo / interazione tra uomo e token.

- **Interfaccia Elettronica**

  Una smart card o un altro token richiede un'interfaccia elettronica elettronica per comunicare con un lettore/scrittore compatibile.

  Una carta può avere uno o entrambi i seguenti tipi di interfaccia:

  - **Contatto**

    Una smart card a contatto deve essere inserita in un lettore di smart card con una connessione diretta a una piastra di contatto conduttiva sulla superficie della carta (tipicamente placcata in oro).

    La trasmissione di comandi, dati e stato della carta avviene attraverso questi punti di contatto fisico.

  - **Senza Contatto**

    Una carta senza contatto richiede solo la vicinanza di un lettore.

    Sia il lettore che la carta hanno un'antenna, e i due comunicano utilizzando frequenze radio. La maggior parte delle carte senza contatto derivano anche l'energia per il chip interno da questo segnale elettromagnetico. La portata è tipicamente da un mezzo a tre pollici per le carte non alimentate a batteria, ideale per applicazioni come l'ingresso in un edificio e il pagamento che richiedono un'interfaccia della carta molto veloce.

  - **Protocollo di autenticazione**

    Lo scopo di un token intelligente è quello di fornire un mezzo per l'autenticazione dell'utente.

Possiamo classificare i protocolli di autenticazione usati con token intelligenti in tre categorie:

1. **Statico**
   Con un protocollo statico, l'utente si autentica con il token, poi il token autentica l'utente al computer. L'ultima metà di questo protocollo è simile al funzionamento di un token di memoria.
2. **Generatore dinamico di password**
   In questo caso, il token genera una password unica password unica periodicamente (ad esempio, ogni minuto). Questa password viene poi inserita nel sistema informatico per l'autenticazione, sia manualmente dall'utente o elettronicamente tramite il token. Il token e il sistema informatico devono essere inizializzati e mantenuti sincronizzati in modo che il computer conosca la password che è corrente per questo token.
3. **Sfida-risposta**
   In questo caso, il sistema informatico genera una sfida, come una stringa casuale di numeri. Il token intelligente genera una risposta basata sulla sfida. Per esempio, si potrebbe usare la crittografia a chiave pubblica e il token potrebbe criptare la stringa di sfida con la chiave privata del token.

1.4.3 Elettronic Identity Cards

Un'applicazione di crescente importanza è l'uso di una smart card come carta d'identità nazionale per i cittadini. Una carta d'identità elettronica nazionale (eID) può servire agli stessi scopi di altre carte d'identità nazionali, e carte simili come la patente di guida, per l'accesso ai servizi governativi e commerciali. Inoltre, una carta eID può fornire una prova di identità più forte ed essere usata in una più ampia varietà di applicazioni. In effetti, una carta eID è una smart card che è stata verificata dal governo nazionale come valida e autentica.

L'identity cards conterrà:

- Dati personali

  Come nome, data di nascita e indirizzo

- Numero del documento

  Un identificatore alfanumerico di nove caratteri unico per ogni carta.

- Numero di accesso alla carta (CAN)

  Un numero decimale casuale di sei cifre stampato sulla faccia della carta.

- Zona a lettura ottica (MRZ)

  Tre righe di testo leggibile dall'uomo e dalla macchina sul retro della carta. Anche questo può essere usato come password.

Le funzioni dell'identiry cards sono:

- **ePass**

  Questa funzione è riservata all'uso governativo e memorizza una rappresentazione digitale dell'identità del titolare della carta. Questa funzione è simile a, e può essere usata per, un passaporto elettronico. Anche altri servizi governativi possono usare ePass. La funzione ePass deve essere implementata sulla carta.

- **eID**

  Questa funzione è per uso generale in una varietà di applicazioni governative e commerciali. applicazioni commerciali. La funzione eID memorizza un record di identità a cui i servizi autorizzati possono accedere con il permesso del titolare della carta. I cittadini scelgono se vogliono attivare questa funzione.

- **eSign**

  Questa funzione opzionale memorizza una chiave privata e un certificato che verifica la chiave; è usata per generare una firma digitale. Un centro di fiducia del settore privato emette il certificato.

1.5 Autenticazione Biometrica

Un sistema di autenticazione biometrica tenta di autenticare un individuo sulla base di le sue caratteristiche fisiche uniche. Queste includono:

- **Caratteristiche statiche**

  come le impronte digitali, la geometria della mano, le caratteristiche del viso e i modelli della retina e dell'iride

- **Caratteristiche dinamiche**

  come l'impronta vocale e la firma.

In sostanza, la biometria si basa sul riconoscimento dei modelli. Rispetto alle password e ai token, l'autenticazione è tecnicamente più complessa e costosa. Sebbene sia usata in un numero di applicazioni specifiche, la biometria deve ancora maturare come strumento standard per l'autenticazione degli utenti ai sistemi informatici.

1.5.1 Caratteristiche fisiche utilizzate nelle applicazioni biometriche

Un certo numero di diversi tipi di caratteristiche fisiche sono in uso o in fase di studio per l'autenticazione dell'utente. Le più comuni sono le seguenti:

- **Caratteristiche facciali**

  Le caratteristiche facciali sono il mezzo più comune per l'identificazione da uomo a uomo; quindi è naturale considerarle per l'identificazione tramite computer. L'approccio più comune è quello di definire le caratteristiche basate sulla posizione relativa e la forma delle caratteristiche facciali chiave, come occhi, sopracciglia, naso, labbra e forma del mento.

- **Impronte digitali**

  Le impronte digitali sono state usate come mezzo di identificazione per secoli, e il processo è stato sistematizzato e automatizzato in particolare per l'applicazione della legge. Un'impronta digitale è il modello di creste e solchi sulla superficie del polpastrello. Si ritiene che le impronte digitali siano uniche in l'intera popolazione umana. In pratica, il riconoscimento automatico delle impronte digitali e sistema di corrispondenza estrae un certo numero di caratteristiche dall'impronta digitale per memorizzarle come surrogato numerico del modello completo dell'impronta digitale.

- **Geometria della mano**

  I sistemi di geometria della mano identificano le caratteristiche della mano, compresa la forma, la lunghezza e la larghezza delle dita.

- **Modello della retina**

  Il modello formato dalle vene sotto la superficie della retina è unico e quindi adatto all'identificazione. Un sistema biometrico retinico ottiene un'immagine digitale del modello retinico proiettando un fascio di luce visiva o infrarossa a bassa intensità nell'occhio.

- **Iride**

  Un'altra caratteristica fisica unica è la struttura dettagliata dell'iride.

- **Firma**

  Ogni individuo ha uno stile unico di scrittura e questo si riflette specialmente nella firma, che è tipicamente una sequenza scritta frequentemente. Tuttavia, più campioni di firma di un singolo individuo non saranno identici.

- **La voce**

  Mentre lo stile della firma di un individuo riflette non solo gli unici attributi fisici dello scrittore ma anche l'abitudine alla scrittura che si è sviluppata, i modelli di voce sono più strettamente legati alle caratteristiche fisiche e anatomiche del parlante. Ciononostante, c'è ancora una variazione da campione a campione nel tempo dallo stesso parlante, complicando il compito di riconoscimento biometrico.

1.5.2 Funzionamento di un sistema di autenticazione biometrica

Ogni individuo che deve essere incluso nel database degli utenti autorizzati deve prima essere iscritto al sistema. Questo è analogo all'assegnazione di una password a un utente. Per un sistema biometrico, l'utente presenta al sistema un nome e, tipicamente, un qualche tipo di password o PIN. Allo stesso tempo, il sistema rileva alcune caratteristiche biometriche di questo utente (ad esempio, l'impronta digitale del dito indice destro). Il sistema digitalizza l'input e poi estrae un insieme di caratteristiche che possono essere memorizzate come un numero o un insieme di numeri che rappresentano questa caratteristica biometrica unica; questo insieme di numeri viene chiamato template dell'utente. L'utente è ora iscritto al sistema, che mantiene per l'utente un nome (ID), forse un PIN o una password, e il valore biometrico.

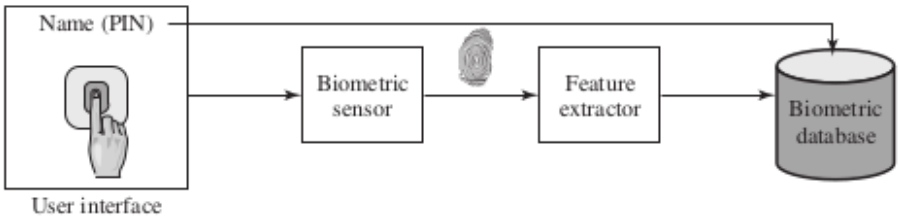
A seconda dell'applicazione, l'autenticazione dell'utente su un sistema biometrico comporta la verifica o l'identificazione.

- **Verifica**

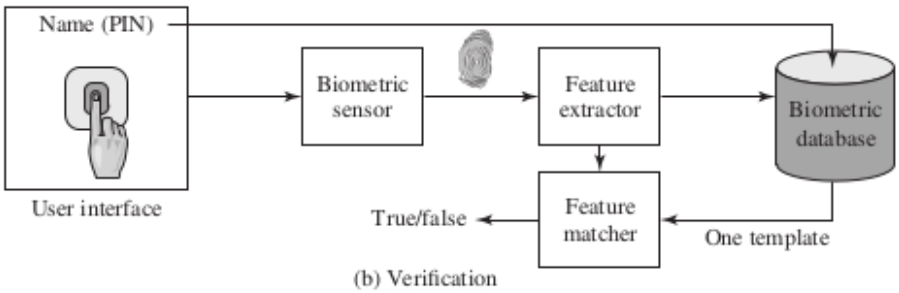
  è analoga a quella di un utente che accede a un sistema usando una scheda di memoria o una smart card accoppiata a una password o a un PIN. Per la verifica biometrica, l'utente inserisce un PIN e utilizza anche un sensore biometrico. Il sistema estrae la caratteristica corrispondente e la confronta con il modello memorizzato per questo utente. Se c'è una corrispondenza, allora il sistema autentica questo utente.

- **Identificazione**

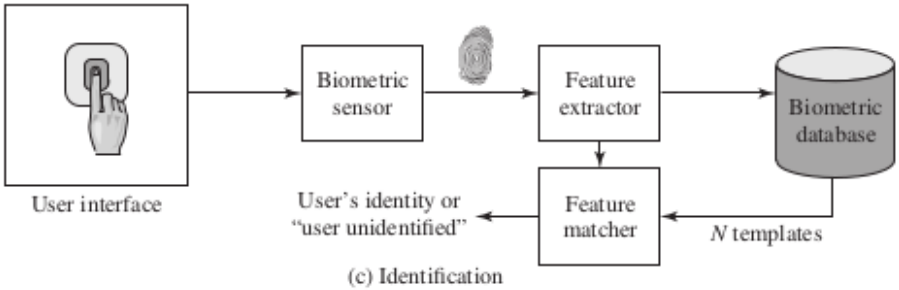
  l'individuo usa il sensore biometrico ma non presenta informazioni aggiuntive. Il sistema quindi confronta il modello presentato con l'insieme dei modelli memorizzati. Se c'è una corrispondenza, l'utente viene identificato. Altrimenti, l'utente viene rifiutato.



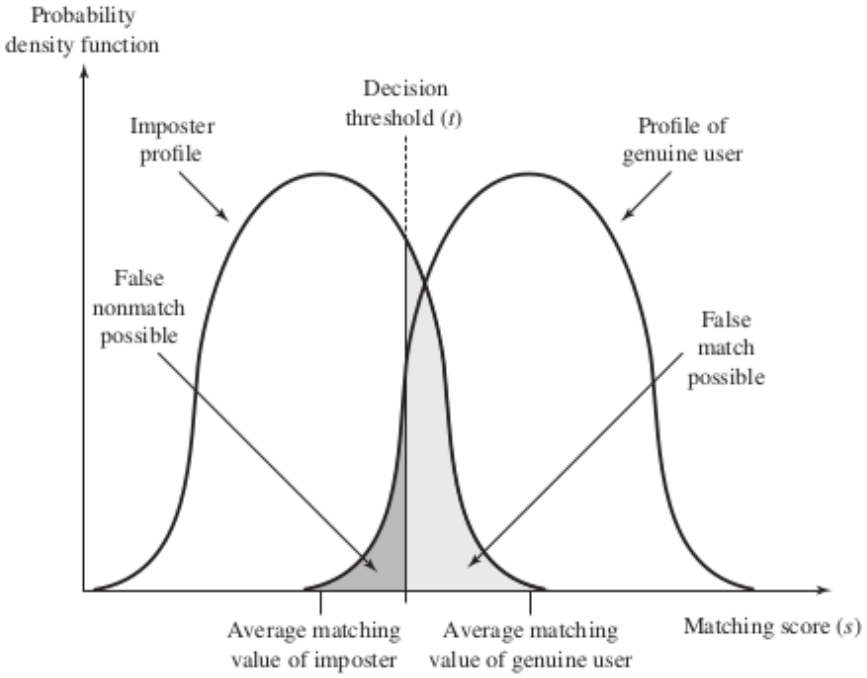
(a) Enrollment



(b) Verification



(c) Identification



1.5.3 Precisione Biometrica

In qualsiasi schema biometrico, alcune caratteristiche fisiche dell'individuo sono mappate in una rappresentazione digitale. Per ogni individuo, una singola rappresentazione digitale, o template, è memorizzata nel computer. Quando l'utente deve essere autenticato, il sistema confronta il modello memorizzato con il modello presentato. Data la complessità delle caratteristiche fisiche, non ci si può aspettare che ci sia una corrispondenza esatta tra i due modelli. Piuttosto, il sistema usa un algoritmo per generare un punteggio (tipicamente un singolo numero) che quantifica la somiglianza tra l'input e il modello memorizzato. Per procedere con la discussione, definiamo i seguenti termini.

- Il tasso di falsa corrispondenza

  è la frequenza con cui i campioni biometrici provenienti da diverse fonti diverse sono erroneamente valutati come provenienti dalla stessa fonte. Il tasso di falsa non corrispondenza è la frequenza con cui i campioni della stessa fonte sono erroneamente valutati essere di fonti diverse.

- La funzione di densità

  tipicamente forma una curva a campana.

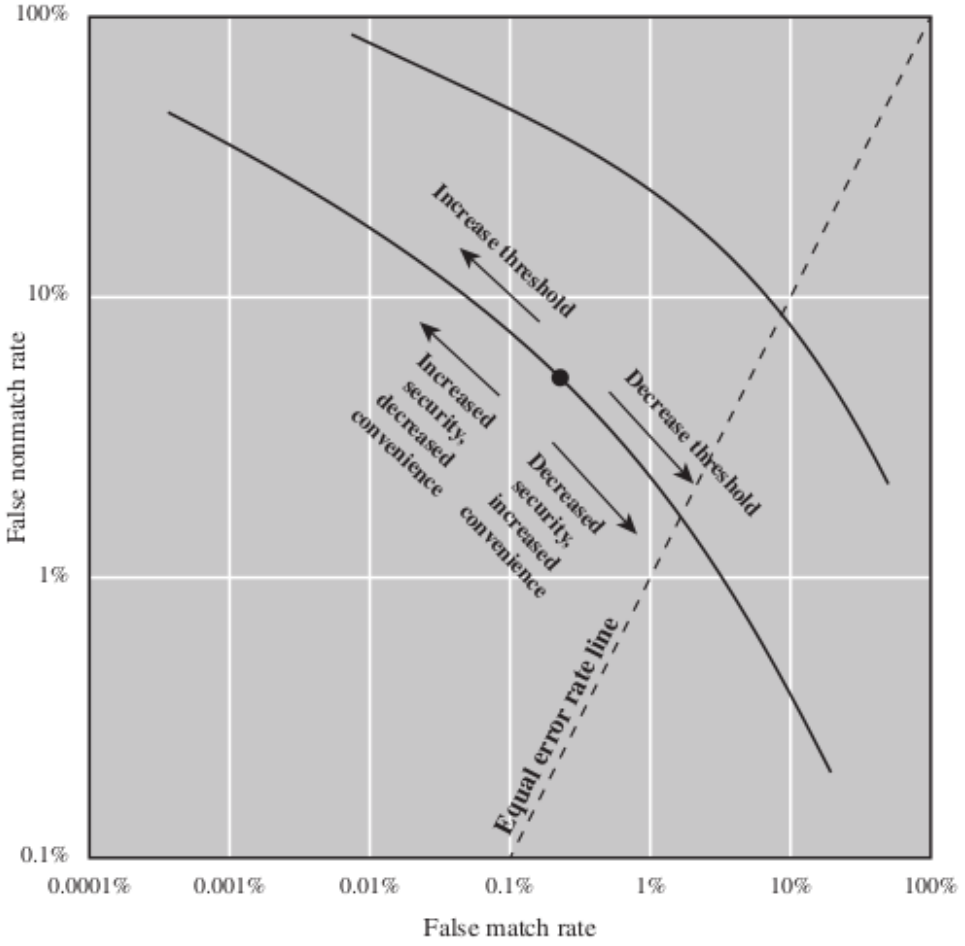


Figure 3.11 **Idealized Biometric Measurement Operating Characteristic Curves (log-log scale)**

Esempio nel caso di un'impronta digitale, i risultati possono variare a causa del rumore del sensore, dei cambiamenti nell'impronta dovuti al gonfiore o alla secchezza, del posizionamento del dito e così via. In media, qualsiasi altro individuo dovrebbe avere un punteggio di corrispondenza molto più basso, ma ancora una volta mostrerà una funzione di densità di probabilità a campana. La difficoltà è che la gamma di punteggi di corrispondenza prodotti da due individui, uno autentico e uno impostore, rispetto a un dato modello di riferimento, è probabile che si sovrappongano. Nella figura 3.10, un valore di soglia è selezionato in modo che se il valore presentato s >= t si assume una corrispondenza, e per s < t, si assume una mancata corrispondenza. La parte ombreggiata a destra di t indica una gamma di valori per cui è possibile una falsa corrispondenza, e la parte ombreggiata a sinistra indica una gamma di valori per cui è possibile una falsa non corrispondenza. Una falsa corrispondenza comporta l'accettazione di un utente che non

dovrebbe essere accettato, e una falsa mancata corrispondenza provoca il rifiuto di un utente valido. L'area di ogni parte ombreggiata rappresenta la probabilità di una falsa corrispondenza o non corrispondenza, rispettivamente. Spostando la soglia, a sinistra o a destra, le probabilità possono essere alterate, ma si noti che una diminuzione del tasso di falsi riscontri si traduce in un aumento del tasso di falsi non riscontri, e viceversa.

1.6 Autenticazione Remota dell'utente

La forma più semplice di autenticazione dell'utente è l'autenticazione locale, in cui un utente tenta di accedere a un sistema che è presente localmente, come un PC da ufficio stand-alone o un bancomat. Il caso più complesso è quello dell'autenticazione remota dell'utente, che avviene su Internet, una rete o un collegamento di comunicazione. L'autenticazione remota dell'utente solleva ulteriori minacce alla sicurezza, come un intercettatore in grado di catturare una password, o un avversario che riproduce una sequenza di autenticazione che è stata osservata.

1.6.1 Protocollo delle password

In questo esempio, un utente trasmette prima la sua identità a all'host remoto. L'host genera un numero casuale r, spesso chiamato nonce, restituisce questo nonce all'utente.

Inoltre, l'host specifica due funzioni, h() e f(), da utilizzare nella risposta. Questa trasmissione dall'host all'utente è la sfida. La risposta dell'utente è la quantità f(r', h(P')), dove r' = r e P' è la password dell'utente.

La funzione h è una funzione hash, quindi la risposta consiste nella funzione hash della password dell'utente combinata con il numero casuale utilizzando la funzione.

L'host memorizza la funzione hash della password di ogni utente registrato, rappresentata come h(P(U)) per l'utente U. Quando arriva la risposta, l'host confronta f(r', h(P')) con la f(r, h(P(U)) calcolata.) Se le quantità corrispondono, l'utente è autenticato. Questo schema difende da diverse forme di attacco. L'host memorizza non la password ma un codice hash della password. Questo protegge la password dagli intrusi nel sistema host. Inoltre, nemmeno l'hash della password viene trasmesso direttamente, ma piuttosto una funzione in cui l'hash della password è uno degli argomenti. Così, per una funzione f adatta, l'hash della password non può essere catturato durante la trasmissione.

Infine, l'uso di un numero casuale tenta di difendere da un attacco di replay, in cui un avversario cattura la trasmissione dell'utente e tenta di accedere a un sistema ritrasmettendo i messaggi.

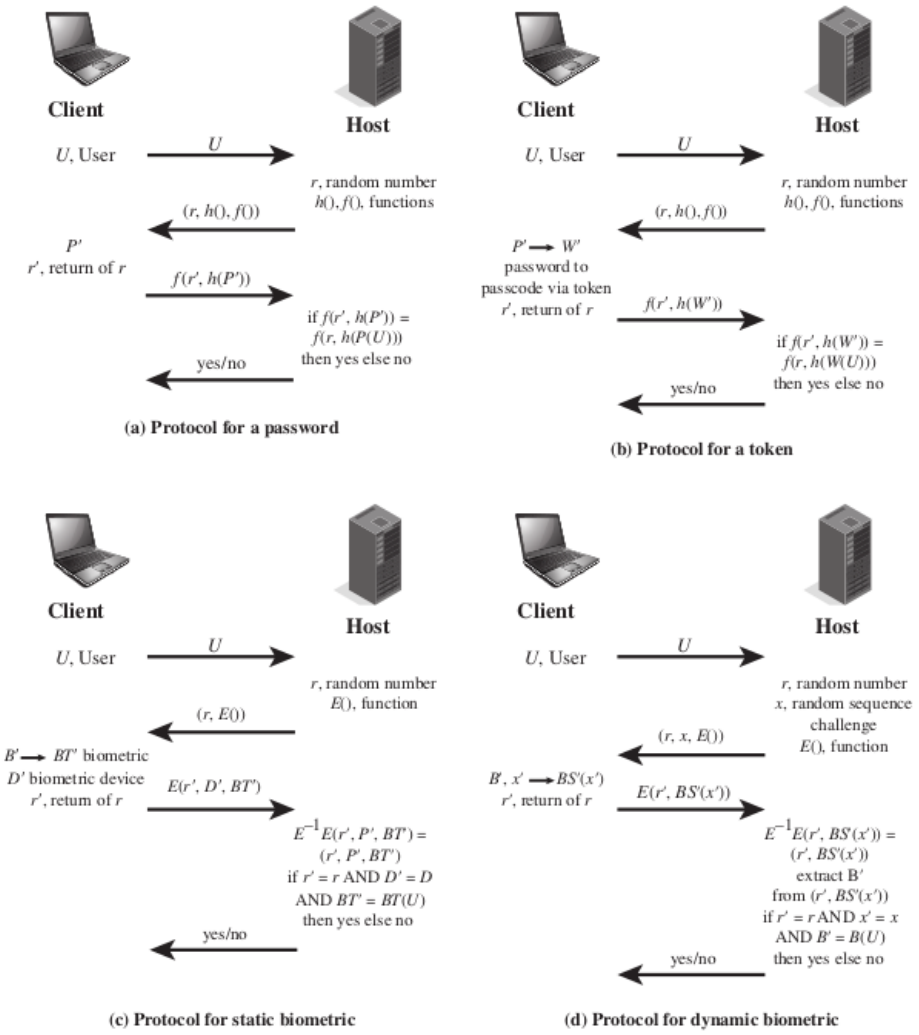


Figure 3.13 **Basic Challenge-Response Protocols for Remote User Authentication**
Source: Based on [OGOR03].

1.6.2 Protocollo di Token

Come prima, un utente trasmette prima la sua identità all'host remoto. L'host restituisce un numero casuale e gli identificatori delle funzioni f() e h() da utilizzare nella risposta. Alla fine dell'utente, il token fornisce un codice di accesso W'. Il token memorizza un codice statico statico o genera un codice casuale una tantum. Per un codice casuale una tantum, il token deve essere sincronizzato. Per un codice casuale una tantum, il token deve essere sincronizzato in qualche modo con l'host. In entrambi i casi, l'utente attiva il codice inserendo una password P'. Questa password è condivisa solo tra l'utente e il token e non coinvolge l'host remoto. Il token risponde all'host con la quantità f(r', h(W')). Per un codice di accesso statico, l host memorizza il valore hashed h(W(U)); per un passcode dinamico, l'host genera un passcode una tantum (sincronizzato con quello generato dal

token) e prende il suo hash. L'autenticazione procede poi nello stesso modo del protocollo della password.

1.6.3 Protocollo biometrico statico

Come prima cosa, l'utente trasmette un ID all'host, che risponde con un numero casuale r e, in questo caso, l'identificatore di una crittografia E(). Sul lato utente c'è un sistema client che controlla un dispositivo biometrico. Il sistema genera un template biometrico BT' dal biometrico dell'utente B' e restituisce il testo cifrato E(r', D', BT'), dove D' identifica questo particolare dispositivo biometrico. L'host decifra il messaggio in arrivo per recuperare i tre parametri trasmessi e li confronta con i valori memorizzati localmente.

Per una corrispondenza, l'host deve trovare r' = r. Inoltre, il punteggio di corrispondenza tra BT' e il modello memorizzato deve superare una soglia predefinita. Infine, l'host fornisce una semplice autenticazione del dispositivo di cattura biometrica confrontando l'ID del dispositivo in entrata con un elenco di dispositivi registrati nel database dell'host.

1.6.4 Protocollo Biometrico Dinamico

La principale differenza rispetto al caso di una biometria stabile è che l'host fornisce una sequenza casuale fornisce una sequenza casuale e un numero casuale come sfida. La sfida è una sequenza di numeri, caratteri o parole. L'utente umano all'estremità del client deve quindi vocalizzare (verifica con altoparlante), digitare (verifica dinamica della tastiera) o scrivere (verifica a mano) o scrivere (verifica della scrittura) la sequenza per generare un segnale biometrico BS'(x'). Il lato client cripta il segnale biometrico e il numero casuale. All'indirizzo lato host, il messaggio in arrivo viene decifrato. Il numero casuale in arrivo r' deve essere una corrispondenza esatta con il numero casuale che è stato originariamente utilizzato come sfida (r). Inoltre, l'host genera un confronto basato sul segnale biometrico in entrata biometrico BS'(x'), il template memorizzato BT(U) per questo utente e il segnale originale x. Se il valore di confronto supera una soglia predefinita, l'utente viene autenticato.

Capitolo4

1.7 Principi di controllo dell'accesso

Due definizioni di controllo dell'accesso sono utili per capire la sua portata.

1. **NISTIR 7298** (Glossario dei termini chiave della sicurezza delle informazioni, maggio 2013), definisce il controllo dell'accesso come il processo di concessione o rifiuto di richieste specifiche a:

   - Ottenere e utilizzare le informazioni e i relativi servizi di elaborazione delle informazioni
   - Entrare in specifiche strutture fisiche.

2. **RFC 4949**, Internet Security Glossary, definisce il controllo dell'accesso come un processo con cui l'uso delle risorse del sistema è regolato secondo una politica di sicurezza è permesso solo alle entità autorizzate (utenti, programmi, processi o altri sistemi) secondo tale politica.

   Possiamo considerare il controllo degli accessi come un elemento centrale della sicurezza informatica. Gli obiettivi principali della sicurezza informatica sono di impedire agli utenti non autorizzati di accesso alle risorse, impedire agli utenti legittimi di accedere alle risorse in modo non in modo non autorizzato, e permettere agli utenti legittimi di accedere alle risorse in modo autorizzato.

Table 4.1 **Access Control Security Requirements (SP 800-171)**

	Basic Security Requirements
1	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).
2	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.
	Derived Security Requirements
3	Control the flow of CUI in accordance with approved authorizations.
4	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.
5	Employ the principle of least privilege, including for specific security functions and privileged accounts.
6	Use non-privileged accounts or roles when accessing nonsecurity functions.
7	Prevent non-privileged users from executing privileged functions and audit the execution of such functions.
8	Limit unsuccessful logon attempts.
9	Provide privacy and security notices consistent with applicable CUI rules.
10	Use session lock with pattern-hiding displays to prevent access and viewing of data after period of inactivity.
11	Terminate (automatically) a user session after a defined condition.
12	Monitor and control remote access sessions.
13	Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.
14	Route remote access via managed access control points.
15	Authorize remote execution of privileged commands and remote access to security-relevant information.
16	Authorize wireless access prior to allowing such connections.
17	Protect wireless access using authentication and encryption.
18	Control connection of mobile devices.
19	Encrypt CUI on mobile devices.
20	Verify and control/limit connections to and use of external information systems.
21	Limit use of organizational portable storage devices on external information systems.
22	Control CUI posted or processed on publicly accessible information systems.

CUI = controlled unclassified information

Source: From NIST SP 800-171 Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations, December 2016 National Institute of Standards and Technology (NIST), United States Department of Commerce.

In senso lato, tutta la sicurezza informatica riguarda il controllo degli accessi. Infatti, RFC 4949 definisce la sicurezza informatica come segue:

Misure che implementano e assicurano servizi di sicurezza in un sistema informatico, in particolare quelle che assicurano il servizio di controllo degli accessi.

1.7.1 Contesto del controllo dell'accesso

Oltre al controllo d'accesso, questo contesto coinvolge le seguenti entità e funzioni:

- **Autenticazione**

  Verifica che le credenziali di un utente o di un'altra entità del sistema siano valide.

- **Autorizzazione**

  La concessione di un diritto o di un permesso ad un'entità di sistema per accedere una risorsa del sistema. Questa funzione determina chi è affidabile per un determinato scopo.

- **Audit**

  Una revisione ed esame indipendente delle registrazioni e delle attività del sistema al fine di verificare l'adeguatezza dei controlli del sistema, di assicurare la conformità con con la politica stabilita e le procedure operative, per rilevare le violazioni della sicurezza, e per raccomandare qualsiasi cambiamento indicato nel controllo, nella politica e nelle procedure.

Un meccanismo di controllo dell'accesso media tra un utente (o un processo che esegue per conto di un utente) e le risorse di sistema, come applicazioni, sistemi operativi, firewall, router, file e database. Il sistema deve prima autenticare un'entità che cerca l'accesso. Tipicamente, la funzione di autenticazione determina se l'utente è permesso di accedere al sistema. Poi la funzione di controllo dell'accesso determina se l'accesso specifico richiesto da questo utente è permesso. Un amministratore di sicurezza mantiene un database un database di autorizzazioni che specifica quale tipo di accesso a quali risorse è permesso a questo utente. La funzione di controllo degli accessi consulta questo database per se concedere l'accesso. Una funzione di auditing monitora e tiene un registro degli accessi degli utenti alle risorse del sistema.

In pratica, un certo numero di componenti può cooperare per condividere la funzione di controllo la funzione di controllo degli accessi. Tutti i sistemi operativi hanno almeno un rudimentale, e in molti casi un componente di controllo degli accessi abbastanza robusto. I pacchetti di sicurezza aggiuntivi possono integrare le capacità di controllo d'accesso native del sistema operativo. Applicazioni particolari o utilità, come un sistema di gestione di database, incorporano anche funzioni di controllo degli accessi funzioni di controllo degli accessi. Dispositivi esterni, come i firewall, possono anche fornire servizi di controllo dell'accesso.

1.7.2 Politiche di controllo dell'accesso

Una politica di controllo degli accessi, che può essere incorporata in un database di autorizzazioni, quali tipi di accesso sono permessi, in quali circostanze e da chi.

Le politiche di controllo dell'accesso sono generalmente raggruppate nelle seguenti categorie:

- **Controllo dell'accesso discrezionale (DAC)**

  Controlla l'accesso in base all'identità del richiedente e su regole di accesso (autorizzazioni) che stabiliscono cosa i richiedenti sono (o non sono)autorizzati a fare. Questa politica è definita discrezionale perché un'entità può avere diritti di accesso che permettono all'entità, di sua spontanea volontà, di un'altra entità di accedere a qualche risorsa.

- **Controllo di accesso obbligatorio (MAC)**

  Controlla l'accesso basandosi sul confronto delle etichette di sicurezza (che indicano quanto sono sensibili o critiche le risorse del sistema) con le autorizzazioni di sicurezza (che indicano le entità del sistema). con le autorizzazioni di sicurezza (che indicano che le entità del sistema sono autorizzate ad accedere a certe risorse). risorse). Questa politica è definita obbligatoria perché un'entità che ha l'autorizzazione di accedere a una risorsa non può, solo per sua volontà, permettere a un'altra entità di accedere a quella risorsa.

- **Controllo di accesso basato sui ruoli (RBAC)**

  Controlla l'accesso in base ai ruoli che gli utenti hanno all'interno del sistema e su regole che stabiliscono quali accessi sono permessi agli utenti in determinati ruoli.

- **Controllo di accesso basato sugli attributi (ABAC)**

  Controlla l'accesso in base agli attributi dell'utente, della risorsa a cui accedere e delle condizioni ambientali correnti.

Queste quattro politiche non si escludono a vicenda. Un meccanismo di controllo degli accessi può impiegare due o anche tutte e tre queste politiche per coprire diverse classi di risorse di sistema.

1.7.3 Soggetti oggetti e diritti d'accesso

Gli elementi di base del controllo d'accesso sono: soggetto, oggetto e diritto d'accesso.

Un soggetto è un'entità capace di accedere agli oggetti. In generale, il concetto di soggetto equivale a quello di processo. Qualsiasi utente o applicazione ottiene effettivamente l'accesso a un oggetto per mezzo di un processo che rappresenta quell'utente o applicazione. Il processo assume gli attributi dell'utente, come i diritti di accesso.

Un soggetto è tipicamente ritenuto responsabile delle azioni che ha iniziato, e un audit trail può essere usato per registrare l'associazione di un soggetto con azioni rilevanti per la sicurezza eseguite su un oggetto dal soggetto. I sistemi di controllo dell'accesso di base definiscono tipicamente tre classi di soggetti, con diritti di accesso diversi per ogni classe:

- **Propietario:** può essere il creatore di una risorsa, come un file. Per le risorse di sistema, la proprietà può appartenere ad un amministratore di sistema. Per le risorse del progetto, l'amministratore o il un amministratore di progetto o un leader può essere assegnato la proprietà.
- **Gruppo:** In aggiunta ai privilegi assegnati ad un proprietario, ad un gruppo nominato di utenti possono anche essere concessi diritti di accesso, in modo tale che l'appartenenza al gruppo sufficiente per esercitare questi diritti di accesso. Nella maggior parte degli schemi, un utente può appartenere a più gruppi.
- **Mondo:** Il minimo di accesso è concesso agli utenti che sono in grado di accedere al sistema ma non sono inclusi nelle categorie proprietario e gruppo per questa risorsa.

Un oggetto è una risorsa il cui accesso è controllato. In generale, un oggetto è un'entità usata per contenere e/o ricevere informazioni.

Il numero e i tipi di oggetti da proteggere con un sistema di controllo degli accessi dipende dall'ambiente in cui opera il controllo degli accessi e dal compromesso tra sicurezza da un lato e complessità, carico di lavoro e facilità d'uso dall'altro.

Un diritto di accesso descrive il modo in cui un soggetto può accedere a un oggetto.

I diritti di accesso potrebbero includere quanto segue:

- **Leggere:** L'utente può visualizzare le informazioni in una risorsa di sistema (ad esempio, un file, record selezionati record in un file, campi selezionati all'interno di un record, o qualche combinazione). Lettura l'accesso include la possibilità di copiare o stampare.
- **Scrittura:** L'utente può aggiungere, modificare o cancellare dati in una risorsa di sistema (ad esempio, file, record, programmi). L'accesso in scrittura include l'accesso in lettura.

- **Eseguire:** L'utente può eseguire programmi specifici.
- **Cancellare:** L'utente può cancellare certe risorse di sistema, come file o record.
- **Creare:** L'utente può creare nuovi file, record o campi.
- **Cercare:** L'utente può elencare i file in una directory o altrimenti cercare nella directory.

1.7.4 Controllo dell'accesso discrezionale

Come si è detto in precedenza, uno schema di controllo di accesso discrezionale è uno schema in cui un'entità può ricevere diritti di accesso che le permettono, per sua volontà, di permettere a un'altra entità di accedere a qualche risorsa. Un approccio generale al DAC, come esercitato da un sistema operativo o da un sistema di gestione di database, è quello di una matrice di accesso.

Una dimensione della matrice consiste in soggetti identificati che possono tentare l'accesso alle risorse.

Tipicamente, questa lista consisterà di singoli utenti o gruppi di utenti anche se l'accesso potrebbe essere controllato per terminali, apparecchiature di rete, host, o applicazioni invece di o in aggiunta agli utenti. L'altra dimensione elenca gli oggetti a cui si può accedere. Al massimo livello di dettaglio, gli oggetti possono essere singoli dati campi di dati. Raggruppamenti più aggregati, come record, file o anche l'intero database, possono anche essere oggetti nella matrice. Ogni voce nella matrice indica i diritti di accesso di un particolare soggetto per un particolare oggetto.

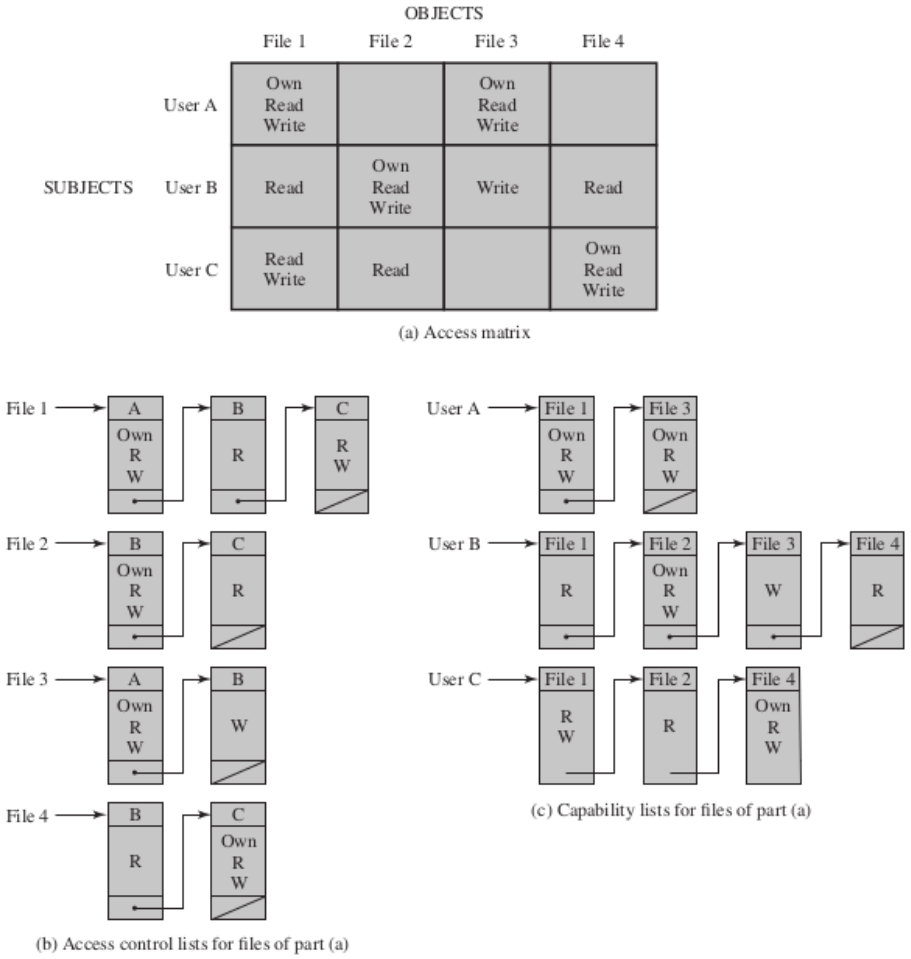


Figure 4.2 **Example of Access Control Structures**

Così, l'utente A possiede i file 1 e 3 e ha diritti di accesso in lettura e scrittura a questi file. L'utente B ha diritti di accesso in lettura al file 1, e così via.

In pratica, una matrice di accesso è di solito sparsa e viene implementata con la decomposizione in uno dei due modi. La matrice può essere decomposta per colonne, ottenendo liste di controllo degli accessi (ACL) (vedi Figura 4.2b). Per ogni oggetto, una ACL elenca gli utenti e i loro diritti di accesso consentiti. L'ACL può contenere una voce di default, o pubblica. Questo permette agli utenti che non sono esplicitamente elencati come aventi diritti speciali di avere un set di diritti. L'insieme predefinito di diritti dovrebbe sempre seguire la regola del minimo privilegio o accesso in sola lettura, a seconda del caso. Gli elementi della lista possono includere singoli utenti così come gruppi di utenti.

Quando si vuole determinare quali soggetti hanno quali diritti di accesso ad una particolare risorsa, le ACL sono convenienti, perché ogni ACL fornisce le informazioni per

una data risorsa. Tuttavia, questa struttura di dati non è conveniente per determinare i diritti di accesso disponibili per uno specifico utente.

La decomposizione per righe produce i capability ticket (vedi Figura 4.2c).

Un capability è un ticket di capacità specifica gli oggetti e le operazioni autorizzate per un particolare utente. Ogni utente ha un certo numero di ticket e può essere autorizzato a prestarli o darli ad altri. Poiché i ticket possono essere dispersi nel sistema, presentano un problema di sicurezza maggiore rispetto alle liste di controllo degli accessi. L'integrità del ticket deve essere protetta e garantita (di solito dal sistema operativo). In particolare, il ticket deve essere non falsificabile. Un modo per ottenere ciò è quello di avere il sistema operativo che tiene tutti i ticket per conto degli utenti. Questi biglietti dovrebbero essere tenuti in una regione di memoria inaccessibile agli utenti. Un'altra alternativa è includere un token non falsificabile nella capacità. Questo potrebbe essere una grande password casuale, o un codice crittografico di autenticazione del messaggio. Questo valore è verificato dalla risorsa ogni volta che viene richiesto l'accesso. Questa forma di capability ticket è appropriata per Questa forma di capability ticket è appropriata per l'uso in un ambiente distribuito, quando la sicurezza del suo contenuto non può essere garantita. Gli aspetti convenienti e scomodi dei capability ticket sono l'opposto di quelli delle ACL. È facile determinare l'insieme dei diritti di accesso che un dato utente ha, ma è più difficile determinare l'elenco degli utenti con diritti di accesso specifici per una risorsa specifica.

Una tabella di autorizzazione contiene una riga per un diritto di accesso di un soggetto ad una risorsa. Ordinare o accedere alla tabella per soggetto è equivalente a una lista di capacità. Ordinare o l'accesso alla tabella per oggetto è equivalente ad una ACL. Un database relazionale può facilmente implementare una tabella di autorizzazione di questo tipo.

Table 4.2 **Authorization Table for Files in Figure 4.2**

Subject	Access Mode	Object
A	Own	File 1
A	Read	File 1
A	Write	File 1
A	Own	File 3
A	Read	File 3
A	Write	File 3
B	Read	File 1
B	Own	File 2
B	Read	File 2
B	Write	File 2
B	Write	File 3
B	Read	File 4
C	Read	File 1
C	Write	File 1
C	Read	File 2
C	Own	File 4
C	Read	File 4
C	Write	File 4

1.7.5 Un modello di controllo d'accesso

Questa sezione introduce un modello generale per DAC sviluppato da Lampson, Graham, e Denning. Il modello presuppone un insieme di soggetti, un insieme di oggetti e un insieme di regole che governano l'accesso dei soggetti agli oggetti. Definiamo lo stato di protezione di un sistema come l'insieme di informazioni, in un dato momento, che specifica i diritti di accesso per ogni soggetto rispetto a ogni oggetto.

Noi Possiamo identificare tre requisiti: rappresentare lo stato di protezione, far rispettare i diritti di accesso e permettere ai soggetti di alterare lo stato di protezione in certi modi. Il modello affronta tutti e tre i requisiti, dando una descrizione generale e logica di un sistema DAC.

Per rappresentare lo stato di protezione, estendiamo l'universo di oggetti nella matrice di controllo degli accessi per includere quanto segue:

- **Processi:** I diritti di accesso includono la capacità di cancellare un processo, fermare (bloccare) e svegliare un processo.
- **Dispositivi:** I diritti di accesso includono la capacità di leggere/scrivere il dispositivo, di controllare il suo funzionamento (ad esempio, una ricerca su disco), e di bloccare/sbloccare il dispositivo per l'uso.
- **Luoghi o regioni di memoria:** I diritti di accesso includono la capacità di leggere/scrivere certe regioni di memoria che sono protette in modo tale che il default è di disabilitare l'accesso.
- **Soggetti:** I diritti di accesso rispetto ad un soggetto hanno a che fare con la capacità di concedere o cancellare i diritti di accesso di quel soggetto ad altri oggetti, come spiegato successivamente.

La figura 4.3 è un esempio. Per una matrice di controllo di accesso A, ogni voce A[S, X] contiene stringhe, chiamate attributi di accesso, che specificano i diritti di accesso del soggetto S all per l'oggetto X. Per esempio, nella figura 4.3, S1 può leggere il file F1, perché 'read' appare in A[S1, F1]. Da un punto di vista logico o funzionale, un modulo di controllo degli accessi separato è associato ad ogni tipo di oggetto (vedi figura 4.4). Il modulo valuta ogni Il modulo valuta ogni richiesta di un soggetto di accedere a un oggetto per determinare se il diritto di accesso esiste. Un tentativo di accesso innesca i seguenti passi:

1. Un soggetto S0 emette una richiesta di tipo a per l'oggetto X.
2. La richiesta fa sì che il sistema (il sistema operativo o un modulo di interfaccia di controllo degli accessi di qualche tipo) a generare un messaggio della forma (S0, a, X) al controllore per X.
3. Il controllore interroga la matrice di accesso A per determinare se a è in A[S0, X].

		OBJECTS								
		Subjects			Files		Processes		Disk drives	
		S_1	S_2	S_3	F_1	F_2	P_1	P_2	D_1	D_2
SUBJECTS	S_1	control	owner	owner control	read*	read owner	wakeup	wakeup	seek	owner
	S_2		control		write*	execute			owner	seek*
	S_3			control		write	stop			

* = copy flag set

Figure 4.3 **Extended Access Control Matrix**

In caso affermativo, l'accesso è permesso; in caso contrario, l'accesso è negato e si verifica una violazione della protezione si verifica una violazione della protezione. La violazione dovrebbe innescare un avvertimento e un'azione appropriata.

La figura 4.4 suggerisce che ogni accesso di un soggetto ad un oggetto è mediato dal controllore per quell'oggetto, e che la decisione del controllore è basata sul contenuto attuale della matrice. Inoltre, alcuni soggetti hanno l'autorità di apportare modifiche specifiche alla matrice di accesso. Una richiesta di modifica della matrice di accesso è trattata come un accesso alla matrice, con le singole voci della matrice trattate come oggetti.

Tali accessi sono mediati da un controllore della matrice di accesso, che controlla gli aggiornamenti alla matrice. Il modello include anche un insieme di regole che governano le modifiche alla matrice di accesso come mostrato nella tabella 4.3. A questo scopo, introduciamo i diritti di accesso "proprietario e 'controllo' e il concetto di flag di copia, come spiegato nei paragrafi successivi.

Le prime tre regole riguardano il trasferimento, la concessione e la cancellazione dei diritti di accesso. Supponiamo che la voce a* esista in A[S0, X]. Questo significa che S0 ha il diritto di accesso a al soggetto X e, a causa della presenza del flag di copia, può trasferire questo diritto, con o senza con o senza flag di copia, ad un altro soggetto. La regola R1 esprime questa capacità. Un soggetto potrebbe trasferire il diritto di accesso senza il flag di copia se ci fosse la preoccupazione che il nuovo soggetto potrebbe trasferire maliziosamente il diritto ad un altro soggetto che non dovrebbe avere quel diritto di accesso. Per esempio, S1 può mettere 'read' o 'read*' in qualsiasi voce della matrice in nella colonna F1. La regola R2 afferma che se S0 è designato come proprietario dell'oggetto X, allora S0 può concedere un diritto di accesso a quell'oggetto per qualsiasi altro soggetto. La regola R2

afferma che che se S0 è designato come proprietario dell'oggetto X, allora S0 può concedere un diritto di accesso a quell'oggetto per qualsiasi altro soggetto.

La regola R2 afferma che S0 può aggiungere qualsiasi diritto di accesso ad A[S, X] per qualsiasi S, se S0 ha accesso "proprietario" a X. La regola R3 permette a S0 di cancellare qualsiasi diritto di accesso da qualsiasi voce della matrice in una riga per la quale S0 controlla il soggetto, e per qualsiasi voce della matrice in una colonna per la quale S0 possiede l'oggetto.

La regola R4 permette ad un soggetto di leggere quella porzione di matrice che possiede o controlla.

Le restanti regole della tabella 4.3 regolano la creazione e la cancellazione di soggetti e oggetti.

La regola R5 afferma che ogni soggetto può creare un nuovo oggetto, che possiede, e può quindi concedere e cancellare l'accesso all'oggetto. Secondo la regola R6, il proprietario di un oggetto può distruggere l'oggetto, con la conseguente cancellazione della colonna corrispondente della matrice di accesso.

La regola R7 permette a qualsiasi soggetto di creare un nuovo soggetto; il creatore è proprietario del nuovo soggetto e il nuovo soggetto ha accesso di controllo su se stesso.

La regola R8 permette al proprietario di un soggetto di cancellare la riga e la colonna (se ci sono colonne di soggetti) della matrice di accesso designata da quel soggetto.

L'insieme di regole nella Tabella 4.3 è un esempio dell'insieme di regole che potrebbero essere definite per un sistema di controllo degli accessi. I seguenti sono esempi di regole aggiuntive o alternative

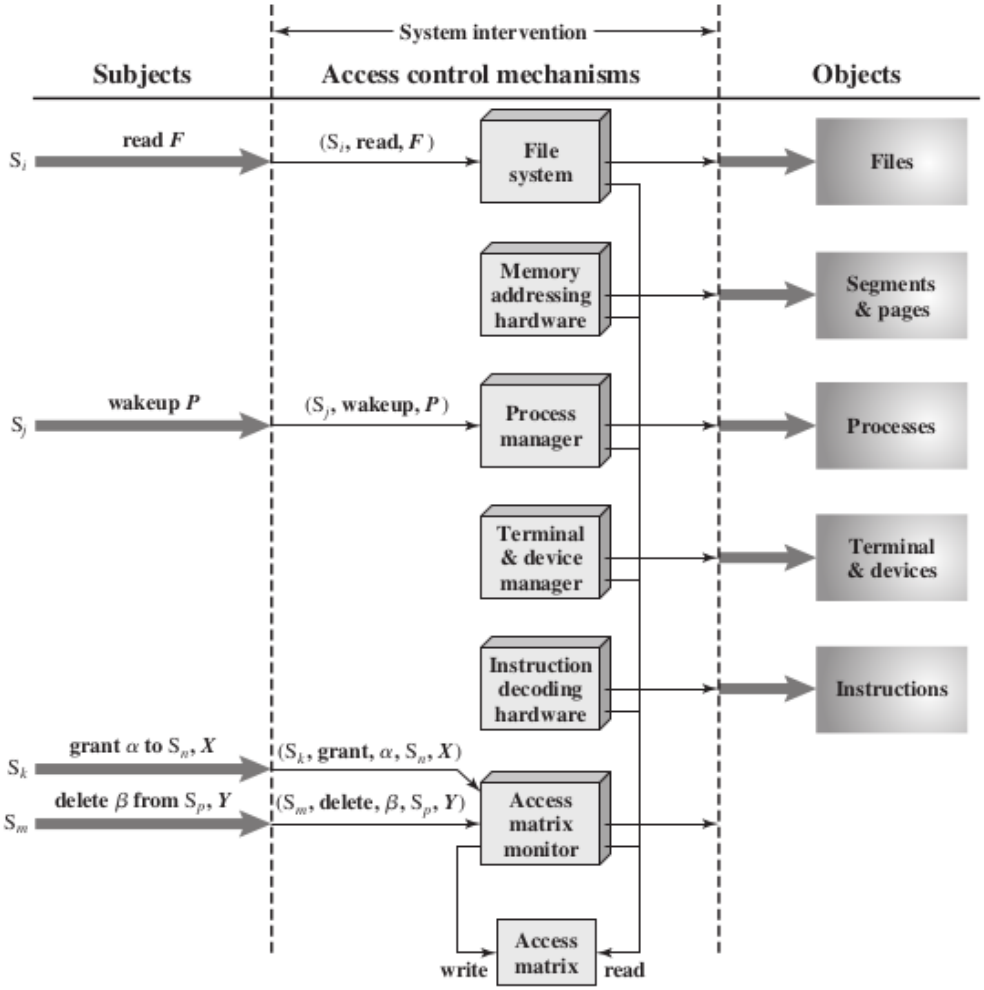


Figure 4.4 **An Organization of the Access Control Function**

Table 4.3 **Access Control System Commands**

Rule	Command (by S_0)	Authorization	Operation
R1	**transfer** $\left\{ \begin{matrix} \alpha^* \\ \alpha \end{matrix} \right\}$ **to** S, X	"α^*" in $A[S_0, X]$	store $\left\{ \begin{matrix} \alpha^* \\ \alpha \end{matrix} \right\}$ in $A[S, X]$
R2	**grant** $\left\{ \begin{matrix} \alpha^* \\ \alpha \end{matrix} \right\}$ **to** S, X	'owner' in $A[S_0, X]$å	store $\left\{ \begin{matrix} \alpha^* \\ \alpha \end{matrix} \right\}$ in $A[S, X]$
R3	**delete** α **from** S, X	'control' in $A[S_0, S]$ or 'owner' in $A[S_0, X]$	delete α from $A[S, X]$
R4	$w \leftarrow$ **read** S, X	'control' in $A[S_0, S]$ or 'owner' in $A[S_0, X]$	copy $A[S, X]$ into w
R5	**create object** X	None	add column for X to A; store 'owner' in $A[S_0, X]$
R6	**destroy object** X	'owner' in $A[S_0, X]$	delete column for X from A
R7	**create subject** S	none	add row for S to A; execute **create object** S; store 'control' in $A[S, S]$
R8	**destroy subject** S	'owner' in $A[S_0, S]$	delete row for S from A; execute **destroy object** S

1.8 Esempio: Controllo di accesso ai file Unix

Tutti i tipi di file UNIX sono amministrati dal sistema operativo per mezzo di inode.

Un inode (nodo indice) è una struttura di controllo che contiene le informazioni chiave necessarie al sistema operativo per un particolare file. Diversi nomi di file possono essere associati ad un singolo inode, ma un inode attivo è associato esattamente ad un file, e ogni file è controllato esattamente da un inode. Gli attributi del file così come i suoi permessi e altre informazioni di controllo sono memorizzati nell'inode. Sul disco, c'è una tabella di inode, o lista di inode, che contiene gli inode di tutti i file nel file sistema. Quando un file viene aperto, il suo inode viene portato nella memoria principale e memorizzato in una tabella di inode residente in memoria.

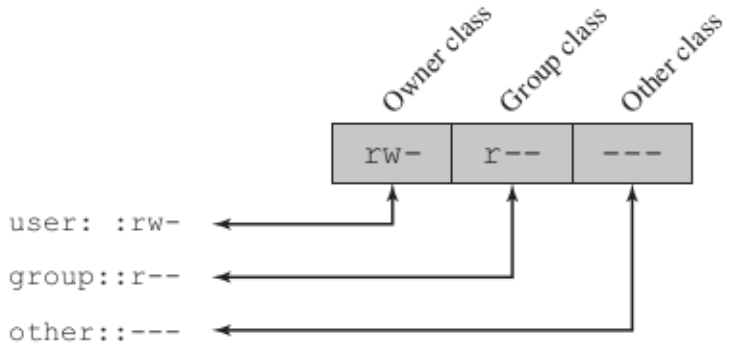
Le directory sono strutturate in un albero gerarchico. Ogni directory può contenere file e/o altre directory. Una directory che si trova all'interno di un'altra directory viene una sottodirectory. Una directory è semplicemente un file che contiene una lista di nomi di file più puntatori agli inode associati. Così, associato ad ogni directory c'è il proprio inode.

1.8.1 Controllo di accesso ai file UNIX tradizionale

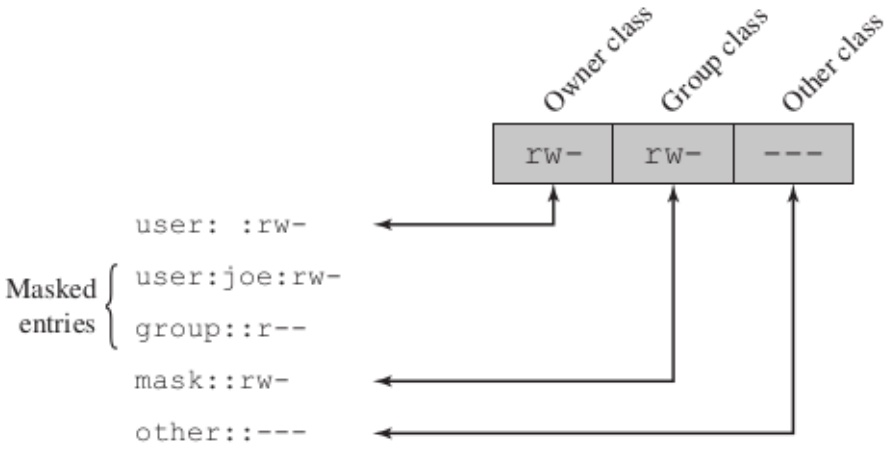
La maggior parte dei sistemi UNIX dipende, o almeno si basa, sullo schema di controllo dell'accesso ai file introdotto con le prime versioni di UNIX. Ad ogni utente UNIX viene assegnato un unico numero di identificazione utente (ID utente). Un utente è anche membro di un gruppo primario, e possibilmente di un certo numero di altri gruppi, ciascuno identificato da un ID di gruppo. Quando un file viene creato, è designato come di proprietà di un particolare utente e contrassegnato dall'ID di quell'utente **ID DI QUELL'UTENTE**.

Appartiene anche a un gruppo specifico, che inizialmente è o il gruppo primario del suo creatore, o il gruppo della sua directory madre se questa ha il permesso SetGID impostato. Associato ad ogni file c'è un insieme di 12 bit di protezione. L'ID del proprietario, l'ID del gruppo e i bit di protezione fanno parte dell'inode del file.

Nove dei bit di protezione specificano i permessi di lettura, scrittura ed esecuzione per il proprietario del file, gli altri membri del gruppo a cui questo file appartiene e tutti gli altri utenti. Questi formano una gerarchia di proprietario, gruppo e tutti gli altri, con l'insieme di permessi più alto che viene usato. La figura 4.5a mostra un esempio in cui il proprietario del file ha accesso in lettura e scrittura; tutti gli altri membri del gruppo del file hanno accesso in lettura; e gli utenti esterni al gruppo non hanno diritti di accesso al file. Quando sono applicati ad una directory, i bit di lettura e scrittura garantiscono il diritto di elencare e creare/rinominare/cancellare file nella directory. Il bit di esecuzione garantisce il diritto di scendere nella directory o di cercare un nome di file.



(a) Traditional UNIX approach (minimal access control list)



(b) Extended access control list

Figure 4.5 **UNIX File Access Control**

I tre bit rimanenti definiscono uno speciale comportamento aggiuntivo per i file o le directory. Due di questi sono i permessi "set user ID" (SetUID) e "set group ID" (SetGID) permessi. Se questi sono impostati su un file eseguibile, il sistema operativo funziona come segue.

Quando un utente (con privilegi di esecuzione per questo file) esegue il file, il sistema alloca temporaneamente i diritti dell'ID dell'utente del creatore del file, o del gruppo del file, rispettivamente, a quelli dell'utente che esegue il file. Questi sono conosciuti come "ID utente effettivo" e "ID gruppo effettivo" e sono usati in aggiunta all'"ID utente reale" e all'"ID gruppo reale". "ID" e "ID gruppo reale" dell'utente in esecuzione quando si prendono decisioni di controllo dell'accesso per questo programma. Questa modifica è efficace solo mentre il programma è in esecuzione.

Questa caratteristica permette la creazione e l'uso di programmi privilegiati che possono utilizzare file normalmente inaccessibili agli altri utenti. Permette agli utenti di accedere a certi file in modo con controllato. In alternativa, quando applicato ad una directory, il permesso SetGID indica che i file appena creati erediteranno il gruppo di questa directory. Il permesso SetUID viene ignorata.

L'ultimo bit di permesso è il bit "appiccicoso". Quando è impostato su un file, originariamente indica che il sistema dovrebbe mantenere il contenuto del file in memoria dopo l'esecuzione. Questo non è più usato. Quando è applicato ad una directory, però, specifica che solo il proprietario di qualsiasi file nella directory può rinominare, spostare o cancellare quel file. Questo è utile per gestire i file nelle directory temporanee condivise.

Un particolare ID utente è designato come "superutente". Il superutente è esente dai soliti vincoli di controllo dell'accesso ai file e ha accesso a tutto il sistema. Qualsiasi programma che è posseduto da, e SetUID a, il "superutente" garantisce potenzialmente un accesso illimitato al sistema accesso al sistema a qualsiasi utente che esegua quel programma. Quindi è necessaria una grande attenzione quando si scrivono tali programmi.

Questo schema di accesso è adeguato quando i requisiti di accesso ai file si allineano con gli utenti e un numero modesto di gruppi di utenti. Per esempio, supponiamo che un utente voglia dare l'accesso in lettura per il file X agli utenti A e B, e l'accesso in lettura per il file Y agli utenti B e C.

Avremmo bisogno di almeno due gruppi di utenti, e l'utente B dovrebbe appartenere ad entrambi gruppi per poter accedere ai due file. Tuttavia, se c'è un gran numero di diversi raggruppamenti di utenti che richiedono una serie di diritti di accesso a diversi file, allora potrebbe essere necessario un numero molto grande di gruppi può essere necessario per fornire questo. Questo diventa rapidamente ingombrante e difficile da gestire, se possibile.

Un modo per superare questo problema è usare le liste di controllo degli accessi, che sono fornite nella maggior parte dei moderni sistemi UNIX. Un ultimo punto da notare è che il tradizionale schema di controllo di accesso ai file UNIX implementa una semplice struttura di dominio di protezione. Un dominio è associato con l'utente, e cambiare il dominio corrisponde a cambiare temporaneamente l'ID dell'utente.

1.8.2 Liste di controllo d'accesso in UNIX

Molti moderni sistemi operativi UNIX e basati su UNIX supportano le liste di controllo degli accessi, inclusi FreeBSD, OpenBSD, Linux e Solaris. In questa sezione, descriviamo FreeBSD, ma altre implementazioni hanno essenzialmente le stesse caratteristiche e la stessa interfaccia. La caratteristica è indicata come lista di controllo di accesso estesa, mentre il tradizionale approccio UNIX UNIX tradizionale è indicato come lista di controllo dell'accesso minima.

FreeBSD permette all'amministratore di assegnare una lista di ID utente UNIX e ad un file usando il comando setfacl. Qualsiasi numero di utenti e gruppi può essere associato ad un file, ognuno con tre bit di protezione (lettura, scrittura, esecuzione), offrendo un meccanismo flessibile per l'assegnazione dei diritti di accesso. Un file non ha bisogno di avere un ACL ma può essere protetto solo dal tradizionale meccanismo di accesso ai file UNIX. I file FreeBSD includono un ulteriore bit di protezione che indica se il file ha una ACL estesa.
FreeBSD e la maggior parte delle implementazioni UNIX che supportano le ACL estese usano la seguente strategia (ad esempio, Figura 4.5b):

1. La classe del proprietario e le altre voci di classe nel campo dei permessi a 9 bit hanno lo stesso stesso significato che nel caso dell'ACL minima.

2. La voce group class specifica i permessi per il gruppo proprietario di questo file.

   Questi permessi rappresentano i permessi massimi che possono essere assegnati a utenti nominati o gruppi nominati, diversi dall'utente proprietario. In quest'ultimo ruolo, la voce classe di gruppo funziona come una maschera.

3. Altri utenti e gruppi nominati possono essere associati al file

   Ognuno con un campo di autorizzazione a 3 bit. I permessi elencati per un utente o un gruppo gruppo sono confrontati con il campo della maschera. Qualsiasi permesso per l'utente o il gruppo gruppo che non è presente nel campo della maschera non è permesso.

Quando un processo richiede l'accesso ad un oggetto del file system, vengono eseguiti due passi.

1. **Passo seleziona la voce ACL che più si avvicina al processo richiedente.**

   Il sito ACL vengono esaminate nel seguente ordine: proprietario, utenti nominati, gruppi (proprietari o con nome) gruppi, altri. Solo una singola voce determina l'accesso.

2. **Passo controlla se la voce voce corrispondente contiene sufficienti permessi.**

   Un processo può essere membro di più di un gruppo; quindi più di una voce di gruppo può corrispondere. Se una di queste voci di gruppo corrispondenti gruppo corrispondente contiene i permessi richiesti, ne viene scelto uno che contiene i permessi richiesti

(il risultato è lo stesso indipendentemente dalla voce scelta). Se nessuna delle delle voci di gruppo corrispondenti contiene i permessi richiesti, l'accesso sarà negato indipendentemente dalla voce scelta.

1.9 Controllo d'accesso basato sul ruolo

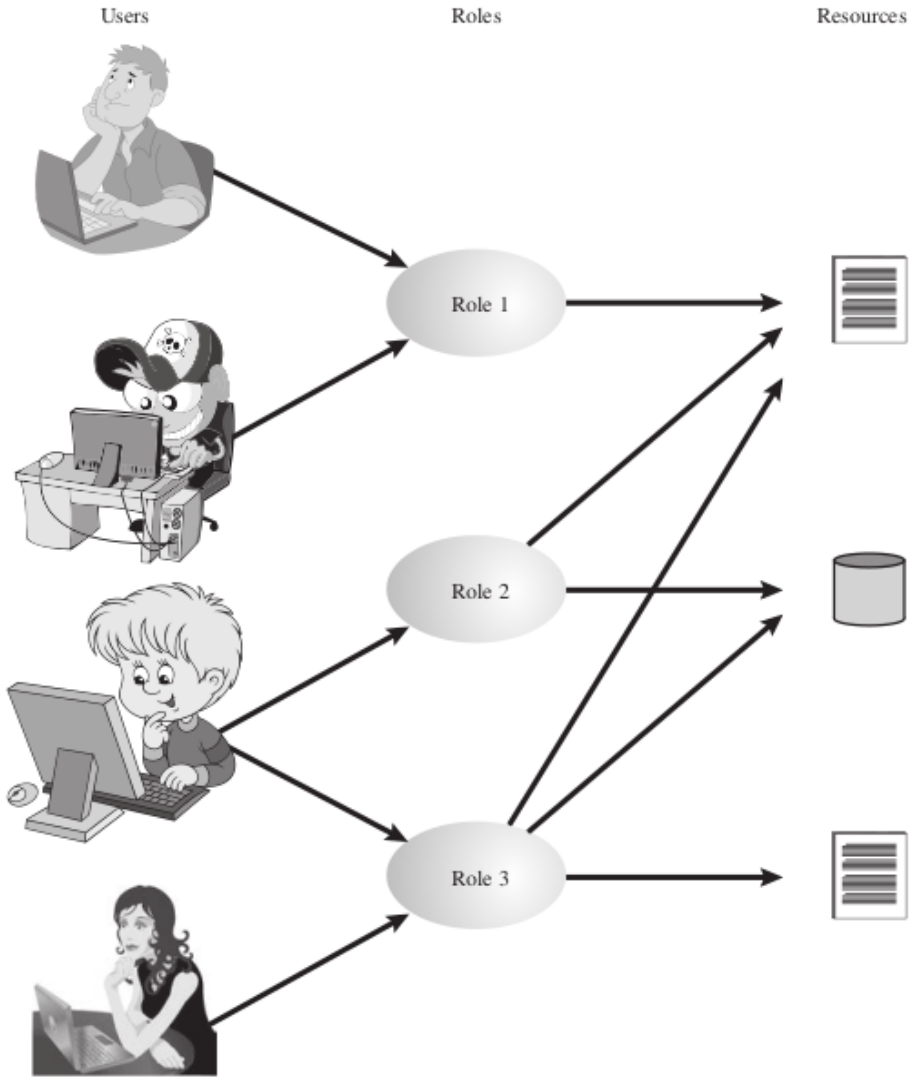
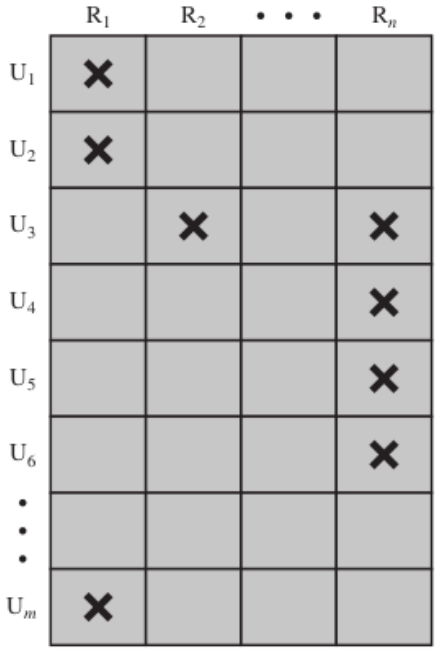


Figure 4.6 **Users, Roles, and Resources**



OBJECTS

ROLES	R_1	R_2	R_n	F_1	F_2	P_1	P_2	D_1	D_2
R_1	control	owner	owner control	read *	read owner	wakeup	wakeup	seek	owner
R_2		control		write *	execute			owner	seek *
•									
•									
•									
R_n			control		write	stop			

Figure 4.7 **Access Control Matrix Representation of RBAC**

I sistemi DAC tradizionali definiscono i diritti di accesso dei singoli utenti e dei gruppi di utenti. Al contrario, RBAC si basa sui ruoli che gli utenti assumono in un sistema piuttosto che sull'identità dell'utente. Tipicamente, i modelli RBAC definiscono un ruolo come una funzione lavorativa all'interno un'organizzazione. I sistemi RBAC assegnano i diritti di accesso ai ruoli invece che ai singoli utenti. A loro volta, gli utenti sono assegnati a diversi ruoli, sia staticamente che dinamicamente, secondo le loro responsabilità.

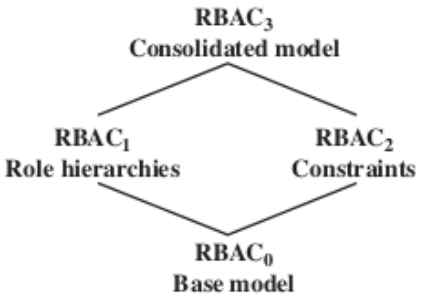
RBAC ora gode di un ampio uso commerciale e rimane un'area di ricerca attiva. Il National Institute of Standards and Technology (NIST) ha emesso uno standard, FIPS PUB 140-3 (Security Requirements for Cryptographic Modules, settembre 2009), che

richiede il supporto per il controllo degli accessi e l'amministrazione attraverso i ruoli. La relazione degli utenti con i ruoli è molti a molti, così come la relazione dei ruoli alle risorse o agli oggetti del sistema (vedi Figura 4.6). L'insieme degli utenti cambia, in alcuni ambienti frequentemente, e l'assegnazione di un utente a uno o più ruoli può anche essere dinamico. L'insieme dei ruoli nel sistema nella maggior parte degli ambienti è relativamente statico, con solo occasionali aggiunte o cancellazioni. Ogni ruolo avrà diritti di accesso specifici a una o più risorse. L'insieme delle risorse e i diritti di accesso specifici associati con un particolare ruolo è probabile che cambino raramente.

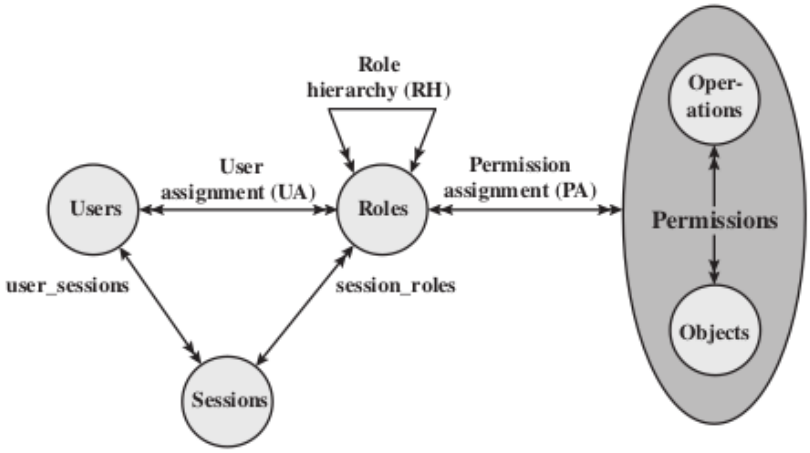
Possiamo usare la rappresentazione della matrice di accesso per rappresentare gli elementi chiave di un sistema RBAC in termini semplici, come mostrato nella figura 4.7. La matrice superiore mette in relazione i singoli utenti ai ruoli. Tipicamente ci sono molti più utenti che ruoli. Ogni matrice voce della matrice è vuota o marcata, quest'ultima indica che l'utente è assegnato a questo ruolo. Si noti che un singolo utente può essere assegnato a più ruoli (più di un segno in una riga) e più utenti possono essere assegnati a un singolo ruolo (più di un segno in una colonna). La matrice inferiore ha la stessa struttura della matrice di controllo degli accessi DAC, con i ruoli come soggetti. Tipicamente, ci sono pochi ruoli e molti oggetti, o risorse. In questa matrice, le voci sono i diritti di accesso specifici dei ruoli. Si noti che un ruolo può essere trattato come un oggetto, permettendo la definizione di gerarchie di ruoli.

RBAC si presta ad un'efficace implementazione del principio del minimo privilegio, a cui si fa riferimento nel capitolo 1. Ogni ruolo dovrebbe contenere l'insieme minimo di diritti di accesso necessari per quel ruolo. Un utente viene assegnato ad un ruolo che gli permette di eseguire solo ciò che è richiesto per quel ruolo. Più utenti assegnati allo stesso ruolo godono dello stesso insieme minimo di diritti di accesso.

1.9.1 Modelli di riferimento RBAC



(a) Relationship among RBAC models



(b) RBAC models

Figure 4.8 **A Family of Role-Based Access Control Models** RBAC_0 **is the minimum requirement for an RBAC system.** RBAC_1 **adds role hierarchies and** RBAC_2 **adds constraints.** RBAC_3 **includes** RBAC_1 **and** RBAC_2.

Table 4.4 **Scope RBAC Models**

Models	Hierarchies	Constraints
RBAC_0	No	No
RBAC_1	Yes	No
RBAC_2	No	Yes
RBAC_3	Yes	Yes

Una varietà di funzioni e servizi possono essere inclusi sotto l'approccio generale RBAC approccio. Per chiarire i vari aspetti di RBAC, è utile definire un insieme di modelli astratti modelli astratti di funzionalità RBAC.

Definisce una famiglia di modelli di riferimento che è servita come base per gli sforzi di standardizzazione in corso. Questa famiglia consiste di quattro modelli che sono correlati tra loro, come mostrato nella Figura 4.8a e nella Tabella 4.4. RBAC 0 contiene la funzionalità minima per un sistema RBAC.

RBAC 1 include le funzionalità di RBAC 0 e aggiunge le gerarchie dei ruoli, che permettono a un ruolo di ereditare i permessi da un altro ruolo. RBAC 2 include RBAC 0 e aggiunge vincoli, che limitano i modi in cui i componenti di un sistema RBAC possono essere configurati. RBAC 3 contiene la funzionalità di RBAC 0, RBAC1 e RBAC2.

Modello base-RBAC0 Figura 4.8b, senza la gerarchia dei ruoli e i vincoli, contiene i quattro tipi di entità in un sistema RBAC 0:

- **Utente:** un individuo che ha accesso a questo sistema informatico. Ogni individuo ha un ID utente associato.
- **Ruolo:** Una funzione di lavoro nominata all'interno dell'organizzazione che controlla questo sistema informatico. Tipicamente, associato ad ogni ruolo c'è una descrizione dell'autorità e della responsabilità conferite a questo ruolo, e a qualsiasi utente che assume questo ruolo.
- **Permesso:** Un'approvazione di una particolare modalità di accesso a uno o più oggetti. Termini equivalenti sono diritto di accesso, privilegio e autorizzazione.
- **Sessione:** Una mappatura tra un utente e un sottoinsieme attivato dell'insieme di ruoli a cui l'utente è assegnato.

Le linee con le frecce nella figura 4.8b indicano relazioni, o mappature, con una freccia singola che ne indica una e una doppia che ne indica molte. Quindi, c'è una relazione molti-a-molti tra utenti e ruoli: Un utente può avere più ruoli, e più utenti possono essere assegnati a un singolo ruolo. Allo stesso modo, c'è una relazione molti a molti tra ruoli e permessi. Una sessione è usata per definire una relazione temporanea uno-a-molti tra un utente e uno o più ruoli a cui l'utente è stato assegnato. L'utente stabilisce una sessione con solo i ruoli necessari per un particolare compito; questo è un esempio del concetto di minimo privilegio. Le relazioni molti-a-molti tra utenti e ruoli e tra ruoli e permessi forniscono una flessibilità e granularità di assegnazione che non si trova negli schemi DAC convenzionali. Senza questa flessibilità e granularità, c'è un rischio maggiore che ad un utente possa essere concesso più accesso alle risorse di quanto sia necessario a causa del controllo limitato sui tipi di accesso che possono essere permessi.

Gerarchie di ruolo-RBAC1

Le gerarchie di ruolo forniscono un mezzo per riflettere la struttura gerarchica dei ruoli in un'organizzazione. Tipicamente, le funzioni lavorative con maggiore responsabilità hanno maggiore autorità per accedere alle risorse. Una funzione lavorativa subordinata può avere un sottoinsieme dei diritti di accesso della funzione lavorativa superiore. Le gerarchie di ruolo fanno uso del concetto di ereditarietà per permettere ad un ruolo di includere implicitamente i diritti di accesso associati ad un ruolo subordinato. La figura 4.9 è un esempio di diagramma di una gerarchia di ruoli. Per convenzione, i ruoli subordinati sono più in basso nel diagramma. Una linea tra due ruoli implica che il ruolo superiore include tutti i diritti di accesso del ruolo inferiore, così come altri diritti di accesso non disponibili al ruolo inferiore. Un ruolo può ereditare diritti di accesso da più ruoli subordinati. Per esempio, nella figura 4.9, il ruolo Project Lead include tutti i diritti di accesso del ruolo Production Engineer e del ruolo Quality Engineer. Più di un ruolo può ereditare dallo stesso ruolo subordinato. Per esempio, sia il ruolo Production Engineer che il ruolo Quality Engineer includono tutti i diritti di accesso del ruolo Engineer. Ulteriori diritti di accesso sono anche assegnati al ruolo Production Engineer, e un diverso insieme di diritti di accesso aggiuntivi sono assegnati al ruolo Quality ingegnere di qualità. Quindi, questi due ruoli hanno diritti di accesso che si sovrappongono, vale a dire i diritti di accesso diritti di accesso che condividono con il ruolo Engineer.

Vincoli-RBAC2

I vincoli forniscono un mezzo per adattare RBAC alle specifiche delle politiche amministrative e di sicurezza in un'organizzazione. Un vincolo è una relazione definita tra i ruoli o una condizione relativa ai ruoli. Esistono i seguenti tipi di vincoli: ruoli mutuamente esclusivi, cardinalità e ruoli prerequisiti. I ruoli mutuamente esclusivi sono ruoli tali che un utente può essere assegnato ad un solo ruolo nell'insieme. Questa limitazione potrebbe essere statica, o potrebbe essere dinamica, nel senso che ad un utente potrebbe essere assegnato solo uno dei ruoli nell'insieme per una sessione. Il vincolo reciprocamente esclusivo supporta una separazione di doveri e capacità all'interno un'organizzazione. Questa separazione può essere rafforzata o migliorata dall'uso di assegnazioni di permessi reciprocamente esclusivi. Con questo vincolo aggiuntivo, un insieme di ruoli mutuamente esclusivi ha le seguenti proprietà:

Un utente può essere assegnato ad un solo ruolo nell'insieme (sia durante una sessione staticamente). Qualsiasi permesso (diritto di accesso) può essere concesso ad un solo ruolo dell'insieme.

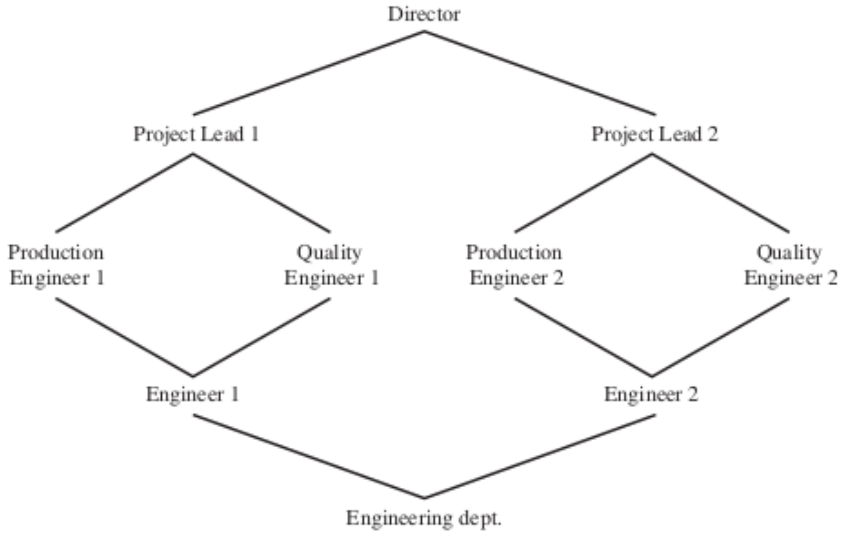


Figure 4.9 **Example of Role Hierarchy**

Così, l'insieme dei ruoli reciprocamente esclusivi hanno permessi non sovrapposti. Se due utenti sono assegnati a ruoli diversi nell'insieme, allora gli utenti hanno permessi non sovrapposti permessi mentre assumono quei ruoli. Lo scopo dei ruoli mutuamente esclusivi è quello di aumentare la difficoltà di collusione tra individui con competenze diverse o funzioni funzioni lavorative divergenti per contrastare le politiche di sicurezza. La cardinalità si riferisce all'impostazione di un numero massimo rispetto ai ruoli. Uno di questi vincolo è quello di impostare un numero massimo di utenti che possono essere assegnati ad un dato ruolo.
Per esempio, un ruolo di capo progetto o un ruolo di capo reparto potrebbe essere limitato ad un singolo utente. Il sistema potrebbe anche imporre un vincolo sul numero di ruoli che un utente è assegnato, o il numero di ruoli che un utente può attivare per una singola sessione. Un'altra forma di vincolo è quella di impostare un numero massimo di ruoli che possono essere concessi un particolare permesso; questa potrebbe essere una tecnica desiderabile di mitigazione del rischio per un permesso sensitiva o potente.

Un sistema potrebbe essere in grado di specificare un ruolo prerequisito, che impone che un utente possa essere assegnato a un particolare ruolo solo se è già assegnato a qualche altro ruolo specificato.

Un prerequisito può essere usato per strutturare l'implementazione del concetto di minimo privilegio. In una gerarchia, potrebbe essere richiesto che un utente possa essere assegnato ad un ruolo (superiore) solo se gli è già stato assegnato un ruolo immediatamente inferiore. Per esempio, nella figura 4.9 un utente assegnato a un ruolo di Project Lead deve essere assegnato anche a ai ruoli subordinati Production Engineer e Quality Engineer. Quindi, se l'utente non ha bisogno di tutti i permessi del ruolo Project Lead per un dato compito,

l'utente può invocare una sessione usando solo il ruolo subordinato richiesto. Si noti l'uso di prerequisiti legati al concetto di gerarchia richiede il modello RBAC 3.

1.10 Controllo degli accessi basato su attributi

Uno sviluppo relativamente recente nella tecnologia di controllo dell'accesso è il modello di controllo dell'accesso basato sugli attributi (ABAC). Un modello ABAC può definire autorizzazioni che esprimono condizioni su proprietà sia della risorsa che del soggetto. Per esempio, consideriamo una configurazione in cui ogni risorsa ha un attributo che identifica il soggetto che ha creato la risorsa. Quindi, una singola regola di accesso può specificare il privilegio del proprietario per tutti i creatori di ogni risorsa. La forza dell'approccio ABAC è la sua flessibilità e potenza espressiva. Sottolinea che il principale ostacolo alla sua adozione in sistemi reali è stata la preoccupazione per l'impatto della valutazione dei predicati su entrambe le proprietà della risorsa e dell'utente per ogni accesso.

Tuttavia, per applicazioni come i servizi Web cooperanti e il cloud computing questo aumento del costo delle prestazioni è meno evidente perché c'è già un costo di prestazione relativamente alto per ogni accesso. Così, i servizi Web sono stati tecnologie innovative per l'implementazione di modelli ABAC, specialmente attraverso l'introduzione dell'eXtensible Access Control Markup Language (XAMCL) e c'è un notevole interesse nell'applicare il modello ABAC ai servizi cloud.

Ci sono tre elementi chiave in un modello ABAC: gli attributi, che sono definiti per le entità in una configurazione; un modello di policy, che definisce le politiche ABAC; e il modello di architettura, che si applica alle politiche che impongono il controllo degli accessi.

1.10.1 Attributi

Gli attributi sono caratteristiche che definiscono aspetti specifici del soggetto, dell'oggetto, delle condizioni ambientali e/o delle operazioni richieste che sono predefinite e preassegnate da un'autorità. Gli attributi contengono informazioni che indicano la classe di informa un nome e un valore (ad esempio, Class = HospitalRecordsAccess, Name = PatientInformationAccess, Value = MFBusinessHoursOnly).

I seguenti sono i tre tipi di attributi nel modello ABAC:

- **Attributi soggetto**

  Un soggetto è un'entità attiva (ad esempio, un utente, un'applicazione, un processo o un dispositivo) che causa il flusso di informazioni tra gli oggetti o cambia lo stato del sistema. Ogni soggetto ha degli attributi associati che definiscono l'identità e le caratteristiche del soggetto. Tali attributi possono includere l'identificatore del soggetto identificatore, nome, organizzazione, titolo di lavoro e così via. Anche il ruolo di un soggetto può essere visto come un attributo.

- **Attributi dell'oggetto**

  Un oggetto, chiamato anche risorsa, è un oggetto passivo (nel contesto della richiesta data) un'entità legata al sistema informativo (ad esempio, dispositivi, file, record, tabelle, processi, programmi, reti, domini) che contengono o ricevere informazioni. Come per i soggetti, gli oggetti hanno attributi che possono essere per prendere decisioni di controllo dell'accesso.

- **Attributi ambientali**

  Questi attributi sono stati finora largamente ignorati nella maggior parte delle politiche di controllo degli accessi. Essi descrivono l'ambiente operativo, tecnico e anche ambiente o contesto situazionale in cui avviene l'accesso alle informazioni. Per esempio, attributi come la data e l'ora correnti, le attività correnti di virus/hacker e il livello di sicurezza della rete (ad esempio, Internet o intranet), non sono associati ad un particolare soggetto o ad una risorsa, ma possono comunque essere rilevanti nell'applicazione di una politica di controllo degli accessi. ABAC è un modello di controllo dell'accesso logico che si distingue perché controlla l'accesso agli oggetti valutando le regole contro gli attributi delle entità (soggetto e oggetto), le operazioni e oggetto), delle operazioni e dell'ambiente rilevanti per una richiesta. ABAC si basa sulla valutazione degli attributi del soggetto, degli attributi dell'oggetto e di una relazione forzata o una regola di controllo dell'accesso che definisce le operazioni consentite per le combinazioni di attributi di soggetto e oggetto in un dato ambiente.

Tutte le soluzioni ABAC contengono queste capacità di base per valutare gli attributi e applicare regole o relazioni tra questi attributi. I sistemi ABAC sono in grado di applicare i concetti DAC, RBAC e concetti MAC. ABAC consente un controllo dell'accesso a grana fine, che permette un numero numero di input discreti in una decisione di controllo

dell'accesso, fornendo un più grande insieme di possibili combinazioni di quelle variabili per riflettere un insieme più ampio e definitivo di possibili regole, politiche o restrizioni di accesso. Così, ABAC permette un numero illimitato numero illimitato di attributi da combinare per soddisfare qualsiasi regola di controllo dell'accesso. Inoltre, i sistemi ABAC possono essere implementati per soddisfare una vasta gamma di requisiti da dalle liste di controllo degli accessi di base a modelli di policy avanzati ed espressivi che sfruttano appieno la flessibilità dell'ABAC.

1.10.2 Architettura locìgica ABAC

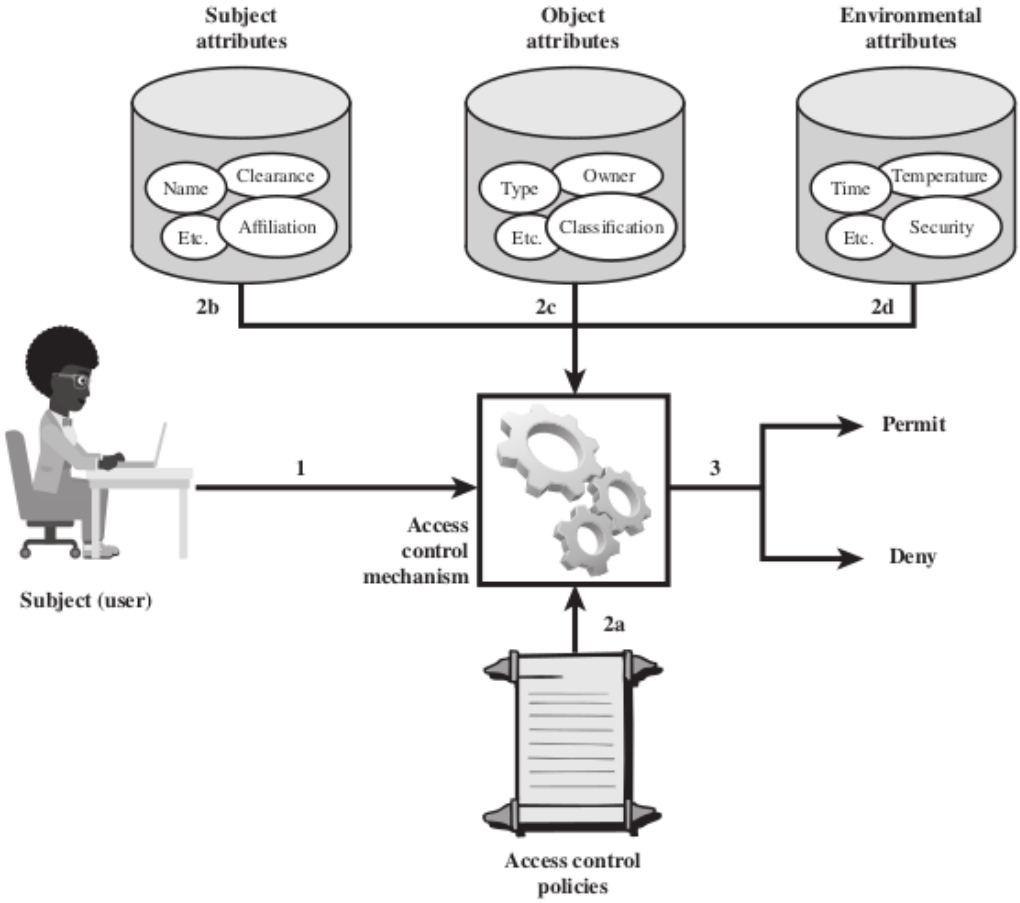


Figure 4.10 **ABAC Scenario**

La figura 4.10 illustra in un'architettura logica i componenti essenziali di un sistema ABAC.

Un accesso di un soggetto a un oggetto procede secondo i seguenti passi:

1. Un soggetto richiede l'accesso ad un oggetto. Questa richiesta viene inoltrata ad un meccanismo di controllo meccanismo di controllo dell'accesso.

2. Il meccanismo di controllo degli accessi è governato da un insieme di regole (2a) che sono definite da una politica di controllo dell'accesso preconfigurata. Sulla base di queste regole, il meccanismo di controllo dell'accesso valuta gli attributi del soggetto (2b), dell'oggetto (2c) e le condizioni ambientali (2d) per determinare l'autorizzazione.

3. Il meccanismo di controllo dell'accesso concede al soggetto l'accesso all'oggetto se l'accesso è autorizzato, e nega l'accesso se non è autorizzato. È chiaro dall'architettura logica che ci sono quattro fonti indipendenti di informazioni utilizzate per la decisione di controllo dell'accesso.

Il progettista del sistema può decidere quali attributi sono importanti per il controllo dell'accesso rispetto a soggetti, oggetti e condizioni ambientali. Il progettista del sistema o altra autorità può quindi definire politiche di controllo dell'accesso, sotto forma di regole, per qualsiasi combinazione desiderata di attri di soggetti, oggetti e condizioni ambientali.

Dovrebbe essere evidente che questo approccio è molto potente e flessibile. Tuttavia, il costo, sia in termini di complessità della progettazione e dell'implementazione, e in termini di impatto sulle prestazioni, è probabile che superi quello di altri approcci di controllo dell'accesso. Questo è un compromesso che autorità di sistema deve fare.

Rispetto a un modello DAC che usa liste di controllo degli accessi (ACL). Questa figura non solo illustra la complessità relativa dei due modelli, ma chiarisce anche i requisiti di fiducia dei due modelli. Un confronto delle relazioni di fiducia rappresentative (indicate dalle linee con la freccia) per l'uso di ACL e ABAC mostra che ci sono molte relazioni di fiducia più complesse richieste per ABAC per funzionare correttamente. Ignorando i punti in comune in entrambe le parti della Figura 4.11, si può osservare che con le ACL la radice della fiducia è con il proprietario dell'oggetto, il quale applica in che fa rispettare le regole di accesso all'oggetto fornendo l'accesso all'oggetto attraverso l'aggiunta di un utente ad una ACL.

L'aggiunta di un utente ad una ACL. In ABAC, la radice della fiducia deriva da molte fonti di cui il proprietario dell'oggetto non ha controllo, come le Subject Attribute Authorities, sviluppatori di policy e emittenti di credenziali. Di conseguenza, SP 800-162 raccomandava che un organismo di governance aziendale sia formato per gestire tutte le identità, le credenziali, di gestione delle identità, delle credenziali e degli accessi e che ogni organizzazione sub-ordinata mantenga un organismo simile per garantire la coerenza nella gestione l'implementazione e il cambiamento di paradigma associati all'implementazione di ABAC a livello aziendale.

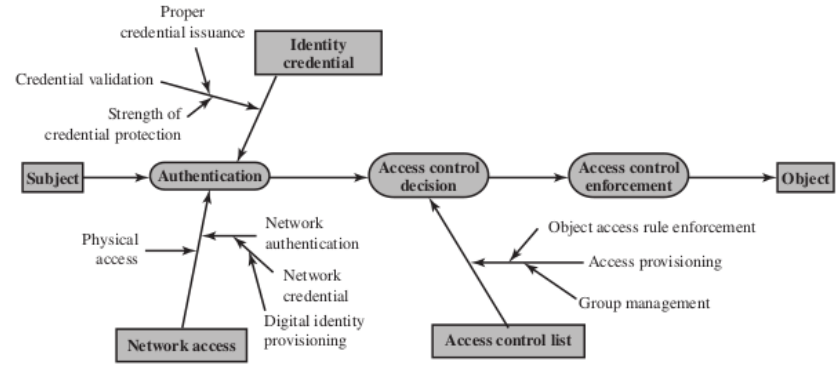
Inoltre, si raccomanda che un'impresa sviluppi un modello di fiducia che può essere usato per illustrare le relazioni di fiducia e aiutare a determinare la proprietà e la responsabilità delle informazioni e dei servizi, le esigenze di ulteriori politiche e di governance e i requisiti per soluzioni tecniche per convalidare o applicare le relazioni di fiducia. Il modello di fiducia di modello di fiducia può essere usato per influenzare le organizzazioni a condividere le loro informazioni con chiare aspettative su come queste informazioni saranno usate e protette e per essere in grado di fidarsi delle informazioni e delle asserzioni di attributi e autorizzazioni provenienti da altre organizzazioni.

1.10.3 Politiche ABAC

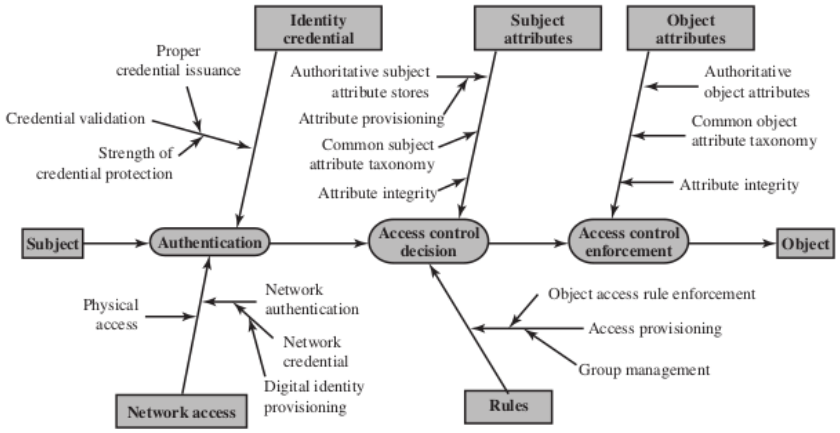
Una politica è un insieme di regole e relazioni che governano il comportamento consentito all'interno di un'organizzazione. Basato sui privilegi dei soggetti e su come le risorse o gli oggetti devono essere protetti in quali condizioni ambientali. A loro volta, i privilegi rappresentano il comportamento autorizzato di un soggetto; sono definiti da un'autorità e incorporati in una politica. Altri termini comunemente usati al posto di privilegi sono autorizzazioni e diritti. La politica è tipicamente scritta dal punto di vista dell'oggetto da proteggere e dei privilegi disponibili ai soggetti. Ora definiamo un modello di policy ABAC. Sono utilizzate le seguenti convenzioni

S, O ed E sono rispettivamente soggetti, oggetti e ambienti

SAk (1 <= k <= K), OAm (1 <= m <= M), e EAn (1 <= n <= N) sono gli attributi predefiniti per soggetti, oggetti e ambienti, rispettivamente



(a) ACL Trust Chain



(b) ABAC Trust Chain

Figure 4.11 **ACL and ABAC Trust Relationships**

ATTR(s), ATTR(o), e ATTR(e) sono relazioni di assegnazione di attributi per il soggetto s, oggetto o, e ambiente e, rispettivamente:

$$ATTR(s) \subseteq SA_1 \times SA_2 \times \ldots \times SA_K$$
$$ATTR(r) \subseteq OA_1 \times OA_2 \times \ldots \times OA_M$$
$$ATTR(o) \subseteq EA_1 \times EA_2 \times \ldots \times EA_N$$

Usiamo anche la notazione di funzione per l'assegnazione del valore dei singoli attributi. Per esempio:

$$Role(s) = \text{"Service Consumer"}$$
$$ServiceOwner(o) = \text{"XYZ, Inc."}$$
$$CurrentDate(e) = \text{"01-23-2005"}$$

Nella forma più generale, una Policy Rule, che decide se un soggetto s può accedere ad un oggetto o in un particolare ambiente e, è una funzione booleana degli attributi di s, o ed e:
Inserire immagine
Una base di regole di policy o policy store può consistere in un certo numero di regole di policy, che coprono molti soggetti e oggetti all'interno di un dominio di sicurezza. Il controllo dell'accesso Il processo decisionale del controllo d'accesso equivale essenzialmente alla valutazione delle regole di nell'archivio delle politiche.
Ora considerate l'esempio di un negozio di intrattenimento online che trasmette film agli utenti per una tariffa mensile fissa. Useremo questo esempio per contrastare gli approcci RBAC e ABAC approcci. Il negozio deve applicare la seguente politica di controllo degli accessi basata sull'età all'età dell'utente e alla classificazione del contenuto del film:

Movie Rating	Users Allowed Access
R	Age 17 and older
PG-13	Age 13 and older
G	Everyone

In un modello RBAC, ad ogni utente verrebbe assegnato uno dei tre ruoli: Adulto, Juvenile, o Child, possibilmente durante la registrazione. Ci sarebbero tre permessi creati: Può vedere film vietati ai minori, Può vedere film vietati ai minori, e Può vedere i film vietati ai minori. Il ruolo Adulto viene assegnato con tutti e tre i permessi.

Il ruolo Juvenile ottiene le autorizzazioni Can view PG-13-rated movies e Can view G-rated movies e il ruolo Bambino ottiene solo il permesso di visualizzare i film vietati ai minori. Entrambe le assegnazioni utente-ruolo e permesso-ruolo sono compiti amministrativi manuali. L'approccio ABAC a questa applicazione non ha bisogno di definire esplicitamente i ruoli. Invece, se un utente u può accedere o vedere un film m (in un ambiente di sicurezza e che qui viene ignorato) verrebbe risolto valutando una regola di policy come la seguente:

```
R1:can_access(u, m, e) ←
   (Age(u) ≥ 17 ∧ Rating(m) ∈ {R, PG-13, G}) ∨
   (Age(u) ≥ 13 ∧ Age(u) < 17 ∧ Rating(m) ∈ {PG-13, G}) ∨
   (Age(u) < 13 ∧ Rating(m) ∈ {G})
```

dove Age e Rating sono rispettivamente l'attributo soggetto e l'attributo oggetto. Il vantaggio del modello ABAC mostrato qui è che elimina la definizione e la gestione di ruoli statici, eliminando così la necessità di compiti amministrativi per l'assegnazione da utente a ruolo e da permesso a ruolo.
Il vantaggio di ABAC si vede più chiaramente quando imponiamo politiche a grana più fine. Per esempio, supponiamo che i film siano classificati come New Release o Old Release, in base alla data di rilascio rispetto alla data corrente, e che gli utenti siano classificati come classificati come Utente Premium e Utente Regolare, in base alla tariffa che pagano. Vorremmo applicare una politica per cui solo gli utenti premium possono vedere i nuovi film. Per il modello RBAC, dovremmo raddoppiare il numero di ruoli, per distinguere ogni utente per età e tariffa, e dovremmo raddoppiare il numero di permessi separati pure.
In generale, se ci sono K attributi soggetto e M attributi oggetto, e se per ogni attributo, Range() denota l'intervallo di valori possibili che può assumere, allora il rispettivo numero di ruoli e permessi richiesti per un modello RBAC sono:

$$\prod_{k=1}^{K} Range\,(SA_k) \text{ and } \prod_{m=1}^{M} Range\,(SA_m)$$

Così, possiamo vedere che quando il numero di attributi aumenta per ospitare politiche a grana più fine, il numero di ruoli e permessi cresce esponenzialmente.
Al contrario, il modello ABAC tratta gli attributi aggiuntivi in modo efficiente. Per questo esempio, la policy R1 definita in precedenza è ancora valida. Abbiamo bisogno di due nuove regole:

```
R2:can_access(u,  m,  e) ←
   (MembershipType(u) = Premium) ∨
   (MembershipType(u) = Regular ∧ MovieType(m) = OldRelease)
R3:can_access(u,  m,  e) ← R1 ∧ R2
```

Con il modello ABAC, è anche facile aggiungere attributi ambientali. Supponiamo che che vogliamo aggiungere una nuova regola di policy che è espressa in parole come segue: Gli utenti regolari sono autorizzati a vedere le nuove release nei periodi promozionali. Questo sarebbe difficile da esprimere in un modello RBAC. In un modello ABAC, abbiamo solo bisogno di aggiungere una regola congiuntiva (AND) che controlla per vedere se l'attributo ambientale la data di oggi cade in un periodo promozionale.

1.11 Gestione dell'entità, delle credenziali e dell'accesso

L'ICAM è un approccio completo alla gestione e all'implementazione delle identità digitali identità digitali (e gli attributi associati), le credenziali e il controllo degli accessi. ICAM è stato sviluppato dal governo degli Stati Uniti, ma è applicabile non solo alle agenzie governative, ma può anche essere distribuito da imprese che cercano un approccio unificato al controllo degli accessi. ICAM è progettato per:

- Creare rappresentazioni fidate di identità digitali di individui e di ciò che i documenti ICAM si riferiscono a entità non personali (NPE). Queste ultime includono processi, applicazioni e dispositivi automatici che cercano di accedere a una risorsa.
- Legare queste identità a credenziali che possono servire come proxy per l'individuo o NPE nelle transazioni di accesso. Una credenziale è un oggetto o una struttura di dati che lega autorevolmente un'identità (e opzionalmente, attributi aggiuntivi) a un token posseduto e controllato da un sottoscrittore.
- Utilizza le credenziali per fornire un accesso autorizzato alle risorse di un'agenzia.

1.11.1 Gestione dell'identità

La gestione dell'identità si occupa di assegnare attributi a un'identità digitale e di collegare tale identità digitale a un individuo o a una NPE. L'obiettivo è quello di stabilire un'identità digitale affidabile che sia indipendente da una specifica applicazione o contesto.

L'approccio tradizionale, e ancora più comune, al controllo dell'accesso per applicazioni e programmi è quello di creare una rappresentazione digitale di un'identità per l'uso specifico di l'applicazione o il programma. Di conseguenza, il mantenimento e la protezione dell'identità stessa è trattata come secondaria rispetto alla missione associata all'applicazione. Inoltre, c'è una considerevole sovrapposizione di sforzi nello stabilire queste identità specifiche dell'applicazione.

A differenza degli account usati per accedere a reti, sistemi o applicazioni, i record di identità aziendali non sono legati al titolo di lavoro, alle mansioni lavorative, all'ubicazione o al fatto che sia necessario l'accesso a un sistema specifico. Questi elementi possono diventare attributi legati ad un record di identità e possono anche diventare parte di ciò che identifica in modo univoco un individuo in una specifica applicazione. Le decisioni sul controllo degli accessi saranno basate sul contesto e sugli attributi rilevanti di un utente non solo sulla sua identità. Il concetto di un'identità aziendale è che gli individui avranno una singola rappresentazione digitale di se stessi che può essere sfruttata in tutti i dipartimenti e le agenzie per molteplici scopi, compreso il controllo degli accessi.

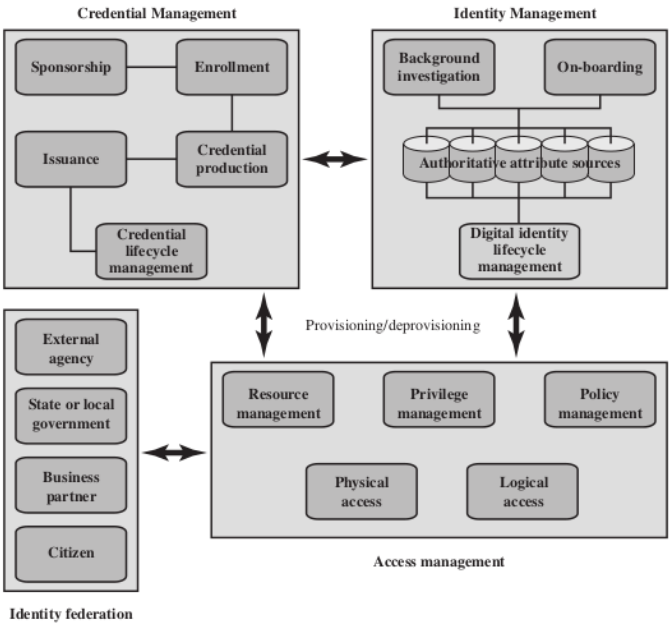


Figure 4.12 **Identity, Credential, and Access Management (ICAM)**

La figura 4.12 illustra le funzioni chiave coinvolte nella gestione delle identità. Un'identità digitale inizia tipicamente con la raccolta di dati di identità come parte di un processo di iscrizione. Un'identità digitale è spesso composta da un insieme di attributi che aggregati identificano in modo univoco un utente all'interno di un sistema o di un'azienda. Al fine di stabilire la fiducia nell'individuo rappresentato da un'identità digitale, un'agenzia può anche condurre un'indagine di fondo.

Gli attributi di un individuo possono essere memorizzati in varie fonti autorevoli all'interno di un'agenzia e collegati per formare una visione aziendale dell'identità digitale. Questa identità digitale può quindi essere fornita in applicazioni per supportare l'accesso fisico e logico (parte della gestione degli accessi) e de-provisionata quando l'accesso non è più richiesto.

Un elemento finale della gestione delle identità è la gestione del ciclo di vita, include quanto segue:

- Meccanismi, politiche e procedure per proteggere l'identità personale informazioni
- Controllo dell'accesso ai dati di identità
- Tecniche per condividere dati di identità autorevoli con le applicazioni che ne hanno bisogno
- Revoca di un'identità aziendale

1.11.2 Gestione delle credenziali

Come detto, una credenziale è un oggetto o una struttura di dati che lega autorevolmente un'identità (e opzionalmente, attributi aggiuntivi) ad un token posseduto e controllato da un sottoscrittore. Esempi di credenziali sono le smart card, le chiavi crittografiche private/pubbliche crittografiche private/pubbliche e i certificati digitali. La gestione delle credenziali è la gestione del ciclo di vita ciclo di vita della credenziale.

La gestione delle credenziali comprende i seguenti cinque componenti logistici:

1. Un individuo autorizzato sponsorizza un individuo o un'entità per una credenziale per stabilire la necessità della credenziale. Per esempio, un supervisore di reparto sponsorizza un dipendente del dipartimento.

2. L'individuo sponsorizzato si iscrive per la credenziale, un processo che tipicamente consiste in una prova d'identità e nella cattura di dati biografici e di dati di sicurezza.

   un processo che tipicamente consiste nella prova dell'identità e nell'acquisizione di dati biografici e biometrici. Questo passo può anche comportare l'incorporazione di dati di attributo autorevoli, mantenuti dal dal componente di gestione dell'identità.

3. Viene prodotta una credenziale. A seconda del tipo di credenziale, la produzione può coinvolgere la crittografia, l'uso di una firma digitale, la produzione di una smartcard, o altre funzioni.

4. La credenziale viene rilasciata all'individuo o alla NPE.

5. Una credenziale deve essere mantenuta durante il suo ciclo di vita, che potrebbe includere la revoca, la riemissione/sostituzione, la reiscrizione, la scadenza, la reimpostazione del numero di identificazione personale (PIN), sospensione o reintegrazione.

1.11.3 Gestione degli accessi

Il componente di gestione degli accessi si occupa della gestione e del controllo delle modalità di accesso alle risorse da parte delle entità. Copre sia l'accesso logico che fisiologico e può essere interno ad un sistema o un elemento esterno. Lo scopo della gestione degli accessi è quello di garantire che venga fatta la corretta verifica dell'identità quando un individuo tenta di accedere a edifici, sistemi informatici o dati sensibili alla sicurezza. La funzione di controllo degli accessi fa uso delle credenziali presentate da chi richiede l'accesso e l'identità digitale del richiedente.

Sono necessari tre elementi di supporto per una struttura di controllo degli accessi a livello aziendale:

- **Gestione delle risorse**

  Questo elemento riguarda la definizione di regole per una risorsa che richiede il controllo dell'accesso. Le regole includeranno le credenziali requisiti delle credenziali e quali attributi dell'utente, attributi della risorsa e condizioni ambientali sono richieste per l'accesso ad una data risorsa per una data funzione.

- **Gestione dei privilegi**

  Questo elemento si occupa di stabilire e mantenere di diritti o attributi di privilegio che comprendono il profilo di accesso di un individuo. Questi attributi rappresentano caratteristiche di un individuo che possono essere utilizzati come base per determinare le decisioni di accesso alle risorse fisiche e logiche. I privilegi sono considerati attributi che possono essere collegati a un'identità digitale. identità digitale.

- **Gestione delle politiche**

  Questo elemento governa ciò che è permesso e non permesso in una transazione di accesso. Cioè, dati l'identità e gli attributi del richiedente, gli attributi della risorsa o dell'oggetto e le condizioni ambientali, una politica specifica quali azioni questo utente può eseguire su questo oggetto.

1.11.4 Federazione delle identità

La federazione di identità affronta due questioni:

1. Come vi fidate delle identità di individui di organizzazioni esterne che hanno bisogno di accesso ai vostri sistemi?

2. Come garantisci le identità degli individui della tua organizzazione quando hanno hanno bisogno di collaborare con organizzazioni esterne?

La federazione delle identità è un termine usato per descrivere la tecnologia, gli standard, le politiche e processi che permettono a un'organizzazione di fidarsi di identità digitali, attributi di identità e credenziali create ed emesse da un'altra organizzazione.

1.12 Strutte di fiducia

I concetti interconnessi di fiducia, identità e attributi sono diventati preoccupazioni fondamentali delle imprese Internet, dei fornitori di servizi di rete e delle grandi imprese. Queste preoccupazioni possono essere viste chiaramente nell'ambiente del commercio elettronico. Per l'efficienza, la privacy e la semplicità legale, le parti delle transazioni generalmente applicano il principio del need-to-know: cosa si deve sapere di qualcuno per trattare con lui? La risposta varia da caso a caso, e include attributi come il numero di registrazione professionale o di licenza, l'organizzazione e il dipartimento, l'ID del personale, il nulla osta di sicurezza, il numero di riferimento del cliente, il numero di carta di credito, l'identificatore unico della salute, le allergie, il gruppo sanguigno, il numero di previdenza sociale, l'indirizzo, lo stato di cittadino, il nickname dei social network, lo pseudonimo e così via. Gli attributi di un individuo che devono essere conosciuti e verificati per permettere una transazione dipendono dal contesto. Per esempio, un'impresa può bisogno di fornire accesso alle risorse per clienti, utenti, fornitori e partner. A seconda del contesto, l'accesso sarà determinato non solo dall'identità, ma dagli attributi del richiedente e della risorsa.

1.12.1 Approccio tradizionale allo scambio di identità

Le transazioni online o in rete che coinvolgono parti di diverse organizzazioni, o tra un'organizzazione e un utente individuale come un cliente online, richiedono generalmente la condivisione di informazioni di identità. Queste informazioni possono includere una serie di attributi associati oltre a un semplice nome o identificatore numerico. Sia la parte che divulga le informazioni che quella che le riceve devono avere un livello di fiducia sulle questioni di sicurezza e di privacy relative a tali informazioni. La figura 4.13a mostra la tecnica tradizionale per lo scambio di informazioni sull'identità. Questo comporta che gli utenti sviluppino accordi con un fornitore di servizi di identità per procurarsi identità e credenziali digitali, e accordi con le parti che forniscono servizi e applicazioni per gli utenti finali e che sono disposti a fare affidamento sull'identità e sulle informazioni sull'identità e le credenziali generate dal fornitore di servizi d'identità. L'accordo della Figura 4.13a deve soddisfare una serie di requisiti. La parte fidata richiede che l'utente sia stato autenticato con un certo grado di sicurezza, che gli attributi imputati all'utente dal fornitore di servizi d'identità siano accurati, e che il fornitore di servizi d'identità sia autorevole per quegli attributi. Il fornitore di servizi d'identità richiede l'assicurazione di avere informazioni accurate sull'utente e che, se condivide le informazioni, la parte che si affida le userà in accordo con i termini e le condizioni contrattuali e la legge. L'utente richiede l'assicurazione che al fornitore di servizi d'identità e alla parte fidata possano essere affidate informazioni sensibili e che si attengano alle preferenze dell'utente e rispettino la sua privacy. Soprattutto, tutte le parti vogliono sapere se le pratiche descritte dalle altre parti sono effettivamente quelle attuate dalle parti, e quanto sono affidabili quelle parti.

1.12.2 Approccio di fiducia per l'identità aperta

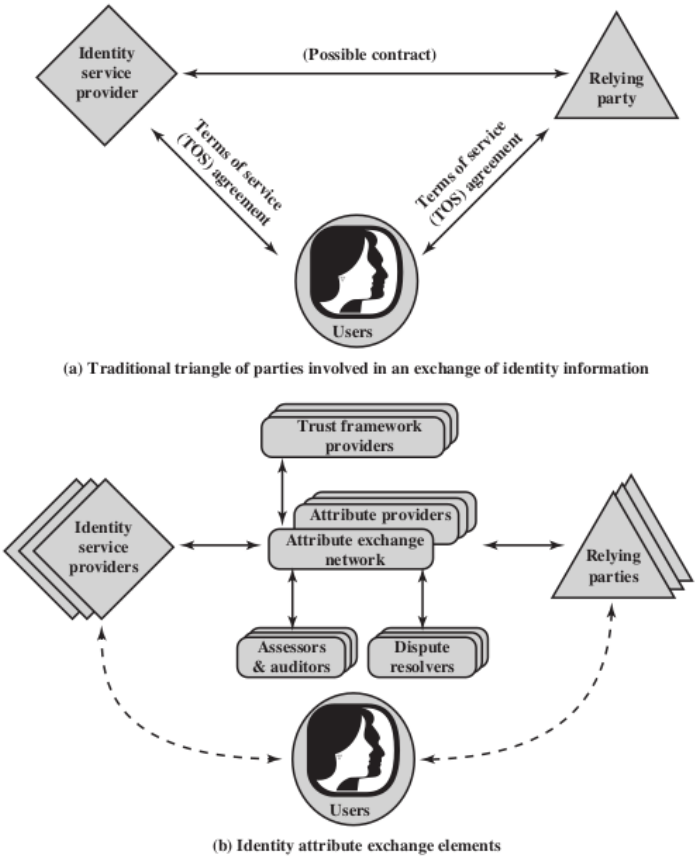


Figure 4.13 **Identity Information Exchange Approaches**

Senza qualche standard e quadro universale, la disposizione della Figura 4.13a deve essere replicata in molteplici contesti. Un approccio di gran lunga preferibile è quello di sviluppare un approccio aperto e standardizzato per lo scambio di identità e attributi affidabili. Nel resto di questa sezione, esaminiamo un tale approccio che sta guadagnando sempre più consenso. Sfortunatamente, questo argomento è gravato da numerosi acronimi, quindi è meglio iniziare con una definizione del più importante di questi:

- **OpenId**

  Questo è uno standard aperto che permette agli utenti di essere autenticati da alcuni siti cooperanti (noti come Relying Parties) utilizzando un servizio di terze parti, eliminando la necessità per i webmaster di fornire i propri sistemi ad hoc e permettendo agli utenti di consolidare le loro identità digitali. Gli utenti possono creare account con i loro fornitori di identità OpenID preferiti, quindi utilizzare tali account come base per accedere a qualsiasi sito web che accetti l'autenticazione OpenID.

- **OIDF**

  La OpenID Foundation è un'organizzazione internazionale senza scopo di lucro di persone e aziende impegnate ad abilitare, promuovere e proteggere le tecnologie OpenID. OIDF assiste la comunità fornendo l'infrastruttura necessaria struttura e aiuto nel promuovere e sostenere l'adozione estesa di OpenID.

- **ICF**

  La Information Card Foundation è una comunità senza scopo di lucro di aziende e individui che lavorano insieme per far evolvere l'ecosistema Information Card. Le carte d'informazione sono identità digitali personali che le persone possono usare online, e la componente chiave dei metasistemi di identità. Visivamente, ogni Information Card ha un'immagine a forma di carta e un nome di carta associato ad essa che permette alle persone di organizzare le loro identità digitali e di selezionare facilmente quella che vogliono usare per qualsiasi interazione.

- **OITF**

  La Information Card Foundation è una comunità senza scopo di lucro di aziende e individui che lavorano insieme per far evolvere l'ecosistema Information Card. Le carte d'informazione sono identità digitali personali che le persone possono usare online, e la componente chiave dei metasistemi di identità. Visivamente, ogni Information Card ha un'immagine a forma di carta e un nome di carta associato ad essa che permette alle persone di organizzare le loro identità digitali e di selezionare facilmente quella che vogliono usare per qualsiasi interazione.

- **OIX**

  L'Open Identity Exchange Corporation è un fornitore internazionale indipendente e neutrale internazionale di strutture di fiducia per la certificazione conformi al modello Open Identity Trust Frameworks.

- **AXN**

  Un Attribute Exchange Network (AXN) è un gateway online su scala Internet per i fornitori di servizi d'identità e per le parti che si affidano a loro per accedere in modo efficiente agli attributi di identità online affermati dall'utente, autorizzati e verificati in volumi a costi accessibili.

I gestori del sistema devono potersi fidare del fatto che gli attributi associati a un soggetto o un oggetto siano autorevoli e vengano scambiati in modo sicuro. Un approccio per fornire tale fiducia all'interno di un'organizzazione è il modello ICAM, in particolare i componenti ICAM (vedi figura 4.12). Combinato con una funzionalità di federazione di identità che è condivisa con altre organizzazioni, gli attributi possono essere scambiati in modo degno di fiducia, supportando un controllo di accesso sicuro. Nei sistemi d'identità digitale, una struttura di fiducia funziona come un programma di certificazione. Permette ad una parte che accetta una credenziale di identità digitale (chiamata parte fidata) di fidarsi delle politiche di identità, sicurezza e privacy della parte che emette la credenziale (chiamato fornitore di servizi di identità) e viceversa.

Più formalmente, OIX definisce un quadro di fiducia come un insieme di impegni verificabili da ciascuna delle varie parti di una transazione verso le loro controparti.

Questi impegni includono:

1. Controlli (compresi gli obblighi normativi e contrattuali) per aiutare a garantire che gli impegni siano
2. Rimedi per il mancato rispetto di tali impegni.

Un quadro di fiducia è sviluppato da una comunità i cui membri hanno obiettivi e prospettive simili. Esso definisce i diritti e le responsabilità dei partecipanti di quella comunità; specifica le politiche e gli standard specifici della comunità e definisce i processi e le processi e procedure specifiche della comunità che forniscono garanzie. Possono esistere diversi quadri di fiducia, e i gruppi di partecipanti possono personalizzare le strutture di fiducia per soddisfare le loro particolari esigenze. La figura 4.13b mostra gli elementi coinvolti nell'OITF.

All'interno di una data organizzazione o agenzia, i seguenti ruoli sono parte del quadro generale:

- **Relying parties (RPs):** Chiamati anche fornitori di servizi, sono entità che forniscono servizi a specifici utenti. Le RP devono avere fiducia nelle identità e/o negli attributi dei loro utenti, e devono fare affidamento sulle varie credenziali presentate per dimostrare tali attributi e identità.
- **Soggetti:** Questi sono gli utenti dei servizi di una RP, compresi i clienti, gli impiegati, partner commerciali e abbonati.
- **Fornitori di attributi (AP):** Gli AP sono entità riconosciute dalla comunità di interesse come in grado di verificare determinati attributi come presentati dai soggetti e che sono attrezzati attraverso l'AXN per creare credenziali di attributo conformi secondo le regole e gli accordi dell'AXN. Alcuni AP saranno fonti di autorità per certe informazioni; più comunemente gli AP saranno broker di attributi derivati.
- **Fornitori di identità (IDP):** Queste sono entità in grado di autenticare le credenziali degli utenti e di garantire i nomi (o pseudonimi o handle) dei soggetti, e che sono attrezzati attraverso l'AXN o qualche altro sistema compatibile di Identità e (IDAM) compatibile per creare identità digitali che possono essere utilizzate per indicizzare gli attributi degli utenti.

Ci sono anche i seguenti importanti elementi di supporto come parte di un AXN:

- **Valutatori:** I valutatori valutano i fornitori di servizi di identità e gli RP e certificano che sono in grado di seguire il progetto del fornitore OITF.
- **Revisori:** Queste entità possono essere chiamate a controllare che le pratiche delle parti siano state in linea con quanto concordato per l'OITF.

- **Risolutori di controversie:** Queste entità forniscono arbitrato e risoluzione delle controversie secondo le linee guida dell'OIX.
- **Fornitori di strutture di fiducia:** Un fornitore di strutture di fiducia è un'organizzazione che traduce i requisiti dei politici in un proprio progetto per una struttura di fiducia quadro di fiducia che poi procede a costruire, facendolo in un modo che è coerente con i requisiti minimi stabiliti nella specifica OITF.

In quasi tutti i casi, ci sarà un'organizzazione candidata ragionevolmente ovvia ad assumere questo ruolo, per ogni settore industriale o grande organizzazione che decide che è appropriato interoperare con un AXN.

Le linee solide con le frecce nella Figura 4.13b indicano gli accordi con il fornitore del quadro fiduciario per l'implementazione dei requisiti tecnici, operativi e legali. Le linee tratteggiate indicano altri accordi potenzialmente interessati da questi requisiti. In termini generali, il modello illustrato nella Figura 4.13b funzionerebbe nel modo seguente. Le persone responsabili all'interno delle organizzazioni partecipanti determinano i requisiti tecnici, operativi e legali per gli scambi di informazioni sull'identità che ricadono sotto la loro autorità. Quindi selezionano i fornitori dell'OITF per implementare questi requisiti. Questi fornitori dell'OITF traducono i requisiti in un progetto per un quadro di fiducia che può includere ulteriori condizioni del fornitore dell'OITF. Il fornitore dell'OITF esamina i fornitori di servizi d'identità e gli RP e stipula con loro dei contratti per seguire i requisiti del suo quadro di fiducia quando conduce scambi di informazioni sull'identità. I contratti contengono disposizioni relative ai risolutori di controversie e ai revisori per l'interpretazione e l'applicazione del contratto.

1.13 Caso di studio: Sistema RBAC per una banca

La Dresdner Bank ha implementato un sistema RBAC che serve come utile esempio pratico.

Esempio pratico La banca usa una varietà di applicazioni informatiche. Molte di queste sono state inizialmente sviluppate per un ambiente mainframe; alcune di queste vecchie applicazioni sono ora supportate su una rete client-server, mentre altre rimangono su mainframe. Ci sono anche applicazioni più recenti su server. Prima del 1990, un semplice sistema DAC era usato su ogni server e mainframe. Gli amministratori mantenevano un file di controllo dell'accesso locale su ogni host e definivano i diritti di accesso per ogni dipendente su ogni applicazione su ogni host. Questo sistema era ingombrante, dispendioso in termini di tempo e soggetto a errori. Per migliorare il sistema, la banca ha introdotto uno schema RBAC, che è a livello di sistema e in cui la determinazione dei diritti di accesso è compartimentata in tre diverse unità amministrative per una maggiore sicurezza. I ruoli all'interno dell'organizzazione sono definiti da una combinazione di posizione ufficiale e funzione lavorativa. La tabella 4.5a fornisce degli esempi. Questo differisce un po' dal concetto di ruolo nello standard NIST, in cui un ruolo è definito da una funzione lavorativa. In una certa misura, la differenza è una questione di terminologia. In ogni caso, la strutturazione dei ruoli della banca porta a un mezzo naturale per sviluppare una gerarchia di eredità basata sulla posizione ufficiale. All'interno della banca, c'è un rigido ordine parziale delle posizioni ufficiali all'interno di ogni organizzazione, che riflette una gerarchia di responsabilità e potere. Per esempio, le posizioni di capo divisione, direttore di gruppo e impiegato sono in ordine decrescente. Quando la posizione ufficiale è combinata con la funzione lavorativa, c'è un conseguente un ordinamento dei diritti di accesso, come indicato nella tabella 4.5b. Così, l'analista finanziario/Group Manager (ruolo B) ha più diritti di accesso rispetto al ruolo analista finanziario/commesso (ruolo A). La tabella indica che il ruolo B ha altrettanti o più diritti di accesso del ruolo A in tre applicazioni e ha diritti di accesso a una quarta applicazione. D'altra parte, non c'è una relazione gerarchica tra office banking/Group Manager e l'analista finanziario/commesso perché lavorano in aree funzionali diverse. Possiamo definire una gerarchia di ruoli in cui un ruolo è superiore ad un altro se la sua posizione è superiore e le loro funzioni sono identiche. La gerarchia dei ruoli permette di risparmiare sulle definizioni dei diritti di accesso, come suggerito nella tabella 4.5c.

Table 4.5 **Functions and Roles for Banking Example**

(a) Functions and Official Positions

Role	Function	Official Position
A	financial analyst	Clerk
B	financial analyst	Group Manager
C	financial analyst	Head of Division
D	financial analyst	Junior
E	financial analyst	Senior
F	financial analyst	Specialist
G	financial analyst	Assistant
...	...	...
X	share technician	Clerk
Y	support e-commerce	Junior
Z	office banking	Head of Division

(b) Permission Assignments

Role	Application	Access Right
A	money market instruments	1, 2, 3, 4
	derivatives trading	1, 2, 3, 7, 10, 12
	interest instruments	1, 4, 8, 12, 14, 16
B	money market instruments	1, 2, 3, 4, 7
	derivatives trading	1, 2, 3, 7, 10, 12, 14
	interest instruments	1, 4, 8, 12, 14, 16
	private consumer instruments	1, 2, 4, 7
...	...	...

(c) Permission Assignment with Inheritance

Role	Application	Access Right
A	money market instruments	1, 2, 3, 4
	derivatives trading	1, 2, 3, 7, 10, 12
	interest instruments	1, 4, 8, 12, 14, 16
B	money market instruments	7
	derivatives trading	14
	private consumer instruments	1, 2, 4, 7
...	...	...

Nello schema originale, l'assegnazione diretta dei diritti di accesso al singolo utente avveniva a livello di applicazione ed era associata alla singola applicazione. Nel nuovo schema, un'amministrazione dell'applicazione determina l'insieme dei diritti di accesso associati ad ogni singola applicazione. Tuttavia, un dato utente che esegue un dato compito potrebbe non avere tutti i diritti di accesso associati all'applicazione. applicazione. Quando un utente invoca un'applicazione, l'applicazione concede l'accesso sulla sulla base di un profilo di sicurezza fornito a livello centrale. Un'amministrazione separata delle autorizzazioni associa i diritti di accesso ai ruoli e crea il profilo di sicurezza per un uso sulla sulla base del ruolo dell'utente. Ad un utente viene assegnato staticamente un ruolo. In linea di principio (in questo esempio), ogni utente può essere assegnato staticamente fino a quattro ruoli e selezionare un dato ruolo da usare per invocare una particolare applicazione. Questo corrisponde al concetto NIST di sessione. In pratica, la maggior parte utenti sono assegnati staticamente a un singolo ruolo in base alla posizione dell'utente e alla sua funzione lavorativa. Tutti questi ingredienti sono rappresentati nella Figura 4.14. Il Dipartimento Risorse Umane assegna un ID utente

unico ad ogni dipendente che userà il sistema.

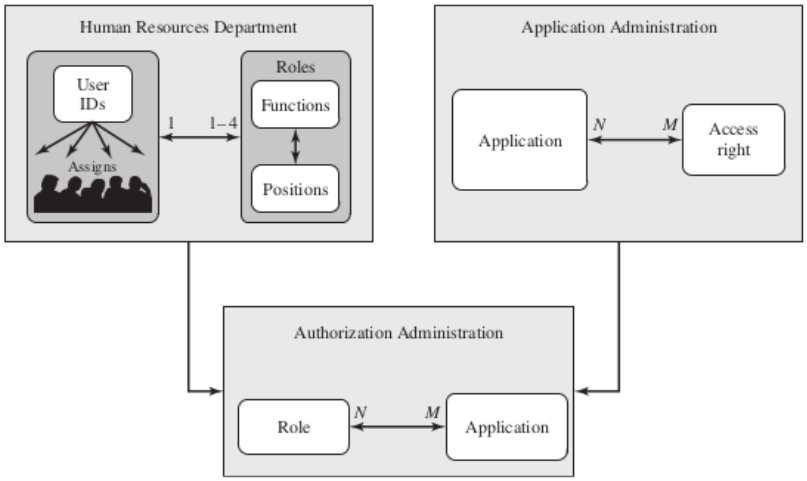


Figure 4.14 **Example of Access Control Administration**

In base alla posizione e alla funzione lavorativa dell'utente, il dipartimento assegna anche uno o ruoli all'utente. Le informazioni sull'utente/ruolo sono fornite all'Amministrazione delle autorizzazioni Amministrazione, che crea un profilo di sicurezza per ogni utente che associa l' ID utente e il ruolo a un insieme di diritti di accesso. Quando un utente invoca un'applicazione, l'applicazione consulta il profilo di sicurezza per quell'utente per determinare quale sottoinsieme dei diritti di accesso dell'applicazione sono in vigore per questo utente in questo ruolo. Un ruolo può essere usato per accedere a diverse applicazioni. Così, l'insieme dei diritti di accesso associati a un ruolo possono includere diritti di accesso che non sono associati a una delle applicazioni che l'utente invoca. Questo è illustrato nella tabella 4.5b. Il ruolo A ha numerosi diritti di accesso, ma solo un sottoinsieme di questi diritti è applicabile a ciascuna delle tre applicazioni che il ruolo A può invocare.

Alcune cifre su questo sistema sono interessanti. All'interno della banca, ci sono 65 posizioni ufficiali, che vanno da un impiegato in una filiale, attraverso il direttore di filiale, a un membro del consiglio di amministrazione. Queste posizioni sono combinate con 368 diverse funzioni lavorative fornite dal database delle risorse umane. Potenzialmente, ci sono 23.920 ruoli diversi, ma il numero di ruoli attualmente in uso è di circa 1.300. Questo è in linea con l'esperienza di altre implementazioni RBAC. In media, 42.000 profili di sicurezza sono distribuiti alle applicazioni ogni giorno dal modulo di amministrazione delle autorizzazioni.

Capitolo 27

1.14 Il modello Bell-LaPadula per la sicurezza informatica

1.14.1 Modelli di sicurezza informatica

In primo luogo, tutti i sistemi software complessi alla fine hanno rivelato difetti o bug che successivamente hanno dovuto essere corretti. Una buona discussione di questo può essere trovato nel classico The Mythical Man-Month. Secondo cui è straordinariamente difficile, se non impossibile, costruire un sistema hardware/software che non sia vulnerabile ad una varietà di attacchi alla sicurezza.

I problemi per fornire una forte sicurezza del computer hanno coinvolto sia il design che l'implementazione. È difficile, progettare qualsiasi hardware o software, ed essere sicuri che il progetto fornisca di fatto il livello di sicurezza che è stato previsto. Questa difficoltà si traduce in molte vulnerabilità di sicurezza non previste. Anche se il progetto è in un certo senso corretto, è difficile, se non impossibile, implementare il progetto senza errori o bug, fornendo un'altra serie di vulnerabilità. Questi problemi hanno portato al desiderio di sviluppare un metodo per dimostrare, logicamente o matematicamente, che un particolare progetto soddisfa un insieme dichiarato di requisiti di sicurezza e che l'implementazione di quel progetto è fedelmente conforme alle specifiche del progetto.

A tal fine, i ricercatori di sicurezza hanno cercato di sviluppare modelli formali di sicurezza del computer che possono essere utilizzati per verificare i progetti e le implementazioni di sicurezza.

Inizialmente, la ricerca in questo settore è stata finanziata dal Dipartimento della Difesa degli Stati Uniti e sono stati fatti notevoli progressi nello sviluppo di modelli e nella loro applicazione a sistemi prototipo. Quel finanziamento è notevolmente diminuito così come i tentativi di costruire modelli formali di sistemi complessi. Il modello di sicurezza informatica più influente il modello Bell-LaPadula (BLP).

1.14.2 Descrizione Generale

Il modello BLP è stato sviluppato negli anni '70 come modello formale per il controllo degli accessi. Il modello modello si basava sul concetto di controllo dell'accesso. Nel modello, ad ogni soggetto e ad ogni oggetto viene assegnata una classe di sicurezza. Nella formulazione più semplice formulazione, le classi di sicurezza formano una rigida gerarchia e sono chiamate livelli di sicurezza.

Un esempio è lo schema di classificazione militare degli Stati Uniti:

top secret > **secret** > **confidential** > **restricted** > **unclassified**

È possibile anche aggiungere un insieme di compartimenti, o categorie, ad ogni livello di sicurezza, così che un soggetto deve essere assegnato sia al livello appropriato che al compartimento per accedere ad un oggetto. Questo concetto è ugualmente applicabile in altre aree, dove le informazioni possono essere organizzate in livelli lordi e compartimenti, e agli utenti possono essere concesse autorizzazioni per accedere a certi compartimenti di dati. Per esempio, il livello più alto di sicurezza potrebbe essere per i documenti ed i dati strategici di pianificazione aziendale, accessibili solo ai funzionari aziendali e al loro staff; poi potrebbero venire i dati finanziari e dei dati sensibili del personale, accessibili solo dal personale amministrativo, ai funzionari aziendali, e così via.

Questo suggerisce uno schema di classificazione:

strategic > **sensitive** > **confidential** > **public**

- Un soggetto ha un nulla osta di sicurezza di un determinato livello
- Un oggetto deve avere una classificazione di sicurezza di un determinato livello.

Le classi di sicurezza controllano il modo con cui un soggetto può accedere ad un oggetto. Il modello ha definito quattro modalità di accesso.

I modi sono i seguenti:

1. **Lettura:** Al soggetto è permesso solo l'accesso in lettura all'oggetto.
2. **Append:** Al soggetto è permesso solo l'accesso in scrittura all'oggetto.
3. **Scrittura:** Il soggetto è autorizzato ad accedere sia in lettura che in scrittura all'oggetto.
4. **Esecuzione:** Il soggetto non è autorizzato né a leggere né a scrivere sull'oggetto ma può invocare l'oggetto per l'esecuzione.

Quando vengono definite più categorie o livelli di dati, il requisito viene definito sicurezza multilivello (MLS). La dichiarazione generale del requisito per la sicurezza multilivello incentrata sulla riservatezza è che un soggetto ad un livello alto non può trasmettere informazioni ad un soggetto ad un livello inferiore a meno che quel flusso rifletta accuratamente la volontà di un utente autorizzato come rivelato da una declassificazione autorizzata. Ai fini dell'implementazione, questo requisito è in due parti ed è dichiarato semplicemente.

Un sistema sicuro multilivello per la riservatezza deve far rispettare quanto segue:

- **Nessuna lettura:** Un soggetto può leggere solo un oggetto di livello di sicurezza inferiore o uguale. Questo è indicato in letteratura come la proprietà di sicurezza semplice (ss-property).
- **Nessuna scrittura:** Un soggetto può solo scrivere in un oggetto di livello di sicurezza maggiore o uguale. Questo è indicato in letteratura come la proprietà1 (pronunciato star property).

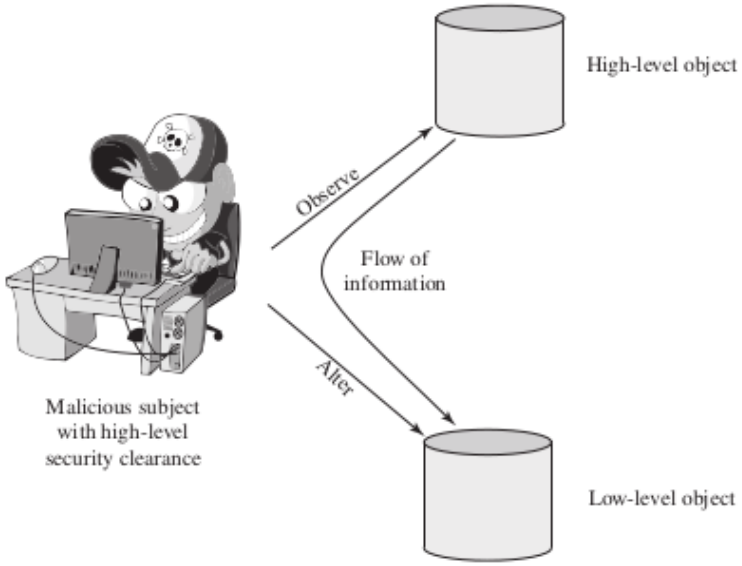


Figure 27.1 **Information Flow Showing the Need for the *-Property**

Qui, un soggetto malintenzionato passa informazioni classificate mettendole in un contenitore di informazioni etichettato con una classificazione di sicurezza inferiore a quella delle informazioni stesse. Questo permetterà un successivo accesso in lettura a queste informazioni da parte di un soggetto con un livello di autorizzazione inferiore. Queste due proprietà forniscono la forma di riservatezza di ciò che è noto come controllo obbligatorio dell'accesso (MAC). Sotto il MAC, non è permesso alcun accesso che non soddisfi queste due proprietà. Inoltre, il modello BLP prevede un controllo di accesso discrezionale (DAC).

- **DS-propietà**

  Un individuo (o ruolo) può concedere a un altro individuo (o ruolo) l'accesso a un documento in base alla discrezione del proprietario, limitato dalle regole MAC regole.

  Così, un soggetto può esercitare solo gli accessi per i quali ha la necessaria autorizzazione e che soddisfano le regole del MAC.

1.14.3 Descrizione formale del modello

Il modello si basa sul concetto di uno stato attuale del sistema. Lo stato è descritto dalla 4-tupla (b, M, f, H), definita come segue:

- **Insieme di accesso corrente b:**

  Questo è un insieme di triple della forma (soggetto, oggetto, accesso-modo). Una tripla (s, o, a) significa che il soggetto s ha accesso corrente a o nel modo di accesso a. Questo non significa semplicemente che s ha il diritto di accesso ad a o ad o. La tripla significa che s sta attualmente esercitando tripla significa che s sta attualmente esercitando quel diritto di accesso; cioè, s sta attualmente accedendo ad a o in modalità a.

- **Matrice di accesso M:**

  L'elemento della matrice Mij registra le modalità di accesso in cui il soggetto Si è autorizzato di accedere all'oggetto Oj.

- **Funzione di livello F:**

  Questa funzione assegna un livello di sicurezza ad ogni soggetto e oggetto. Consiste di tre mappature: fo(Oj) è il livello di classificazione dell'oggetto Oj; fs(Si) che è il nulla osta di sicurezza del soggetto Si; fc(Si) è il livello di sicurezza attuale del soggetto Si. Il nulla osta di sicurezza di un soggetto è il massimo livello di sicurezza del soggetto. Il soggetto può operare a questo livello o a un livello inferiore. Così, un utente può accedere al sistema ad un livello inferiore al nulla osta di sicurezza dell'utente. Questo è particolarmente utile in un sistema di controllo dell'accesso basato sui ruoli.

- **Gerarchia H:**

  Si tratta di un albero con radici dirette i cui nodi corrispondono agli oggetti del sistema. Il modello richiede che il livello di sicurezza di un oggetto domini il livello di sicurezza del suo genitore. Per la nostra discussione, possiamo equiparare questo, alla condizione che il livello di sicurezza di un oggetto deve essere maggiore o uguale al suo genitore.

Possiamo ora definire le tre proprietà di BLP in modo più formale. Per ogni soggetto Si e ogni oggetto Oj, i requisiti possono essere dichiarati come segue:

- **ss-property:** Tutte le triple della forma (Si, Oj, read) nell'insieme corrente di accesso b hanno la propietà fc(Si) >= fo(Oj).
- **property:** Tutte le triple della forma (Si, Oj, append) nell'insieme di accesso corrente b ha la propietà fc(Si) <= fo(Oj). Tutte le triple della forma (Si, Oj, write) nell'attuale set di accesso b hanno la propietà fc(Si) = fo(Oj).
- **ds-property:** Se (Si, Oj, Ax) è un'accesso corrente (in b), la modalità di accesso Ax è registarta in (Si, Oj) elemnti di M. Questo da (Si, Oj, Ax) ed implica che Ax $\in$ M

$$Si, Oj$$

.

Queste tre proprietà possono essere utilizzate per definire un sistema sicuro per la riservatezza.

In sostanza, un sistema sicuro è caratterizzato da quanto segue:

1. Lo stato di sicurezza attuale del sistema (b, M, f, H) è sicuro se e solo se ogni elemento di b soddisfa le tre proprietà.
2. Lo stato di sicurezza del sistema viene cambiato da qualsiasi operazione che causa un cambiamento uno qualsiasi dei quattro componenti del sistema, (b, M, f, H).
3. Un sistema sicuro rimane sicuro finché qualsiasi cambiamento di stato non viola le tre proprietà.

Questi tre punti possono essere espressi come teoremi usando il modello formale. Inoltre, dato un progetto o un'implementazione attuale, è teoricamente possibile dimostrare che il sistema è sicuro provando che ogni azione che influisce sullo stato del sistema soddisfa le tre proprietà. In pratica, per un sistema complesso, tale prova non è mai stata completamente sviluppata. Tuttavia, come menzionato prima, la dichiarazione formale dichiarazione formale dei requisiti può portare ad una progettazione e implementazione più sicura.

1.14.4 Operazioni Astratte

Il modello BLP include un insieme di regole basate su operazioni astratte che cambiano lo stato del sistema. Le regole sono le seguenti:

1. **Ottenere l'accesso**

   Aggiungere una tripla (soggetto, oggetto, modalità di accesso) al set di accesso corrente b. Utilizzato da un soggetto per avviare l'accesso a un oggetto nel modo richiesto

2. **Rilasciare l'accesso**

   Rimuove una tripla (soggetto, oggetto, modo di accesso) dal set di accesso corrente b. Usato per rilasciare un accesso precedentemente iniziato.

3. **Cambiare livello dell'oggetto**

   Cambia il valore di fo(Oj) per qualche oggetto Oj. Usato da un soggetto per modificare il livello di sicurezza di un oggetto

4. **Cambiare livello attuale**

   Cambia il valore di fc(Si) per qualche soggetto Si. Usato da un soggetto per alterare il livello di sicurezza di un oggetto.

5. **Dare il permesso di accesso**

   Aggiungere una modalità di accesso a qualche voce della permissione M. Usato da un soggetto per concedere un modo di accesso su un oggetto specificato a un altro soggetto.

6. **Rescindere il permesso di accesso**

   Cancella un modo di accesso da qualche voce di M. Usato da un soggetto per revocare un accesso precedentemente concesso.

7. **Creare oggetto**

   Attacca un oggetto alla struttura ad albero corrente H come foglia. Usato per creare un nuovo oggetto o attivare un oggetto che è stato precedentemente definito ma è inattivo perché non è stato inserito in H.

8. **Cancellare un gruppo di oggetti**

   Stacca da H un oggetto e tutti gli altri oggetti sotto di esso nella gerarchia. Questo rende il gruppo di oggetti inattivo. Questa operazione può anche modificare l'attuale set di accesso b perché tutti gli accessi all'oggetto vengono rilasciati.

Le regole 1 e 2 alterano l'accesso corrente. Le regole 3 e 4 alterano le funzioni di livello. Le regole 5 e 6 alterano il permesso di accesso e le regole 7 e 8 alterano la gerarchia. Ogni regola è governata dall'applicazione delle tre proprietà. Per esempio, per ottenere l'accesso per una lettura, dobbiamo avere fc(Si) >= fo(Oj) e Ax ∈ M

$$Si, Oj$$

.

1.14.5 Esempio di utilizzo Bella-Pabula

Questo esempio illustra il funzionamento del modello BLP ed evidenzia anche un problema pratico problema pratico che deve essere affrontato. Assumiamo un sistema di controllo degli accessi basato sui ruoli.

Carla e Dirk sono utenti del sistema. Carla è una studentessa (s) nel corso c1. Dirk è un insegnante (t) nel corso c1, ma può anche accedere al sistema come studente; così, due ruoli sono assegnati a Dirk:

$$Carla : (c1 - s)$$
$$Dirk : (c1 - t), (c1 - s)$$

Al ruolo di studente è assegnato un nulla osta di sicurezza inferiore e al ruolo di insegnante un autorizzazione di sicurezza più alta. Vediamo alcune possibili azioni:

1. **Dirk crea un nuovo file f1 come c1-t; Carla crea il file f2 come c1-s (vedi Figura 27.2a)**.

   Carla può leggere e scrivere su f2, ma non può leggere f1, perché è a un livello di classificazione più alto (livello insegnante).

2. **Nel ruolo c1-t, Dirk può leggere e scrivere f1 e può leggere f2 se Carla concede l'accesso a f2**.

   Tuttavia, in questo ruolo, Dirk non può scrivere f2 a causa della proprietà. Né Dirk né un cavallo di Troia per suo conto possono declassare i dati dal livello dell'insegnante al livello dello studente.

   Solo se Dirk si collega come studente può creare un file c1-s o scrivere su un file c1-s esistente, come f2. Nel ruolo di studente, Dirk può anche leggere f2.

3. **Dirk legge f2 e vuole creare un nuovo file con commenti a Carla come feedback**.

   Dirk deve firmare nel ruolo studente c1-s per creare f3 in modo che sia accessibile da Carla (vedi Figura 27.2b). In un ruolo di insegnante, Dirk non può creare un file a livello di classificazione studente.

4. **Dirk crea un esame basato su un file modello esistente memorizzato a livello c1-t**.

   Dirk deve accedere come c1-t per leggere il modello, e anche il file che crea (f4) deve essere a livello dell'insegnante (vedi Figura 27.2c).

5. **Dirk vuole che Carla faccia l'esame, e quindi deve fornirle un accesso in lettura**.

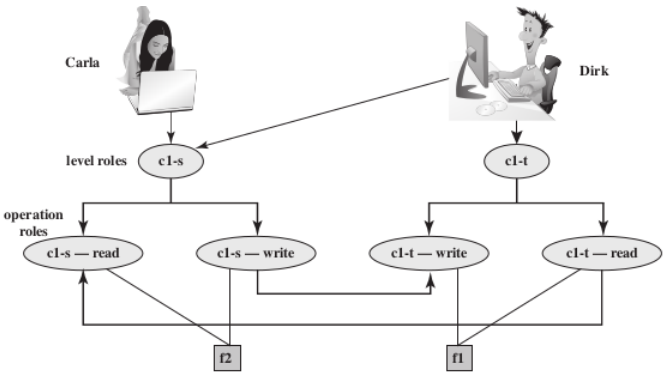
   Tuttavia, tale accesso violerebbe la proprietà ss. Dirk deve declassare la classificazione di f4 da c1-t a c1-s.

   Dirk non può farlo nel ruolo c1-t perché questo violerebbe la proprietà. Pertanto, un amministratore di sicurezza (possibilmente Dirk in questo ruolo) deve avere l'autorità di downgrade e deve essere in grado di eseguire il downgrade al di fuori del modello BLP. La linea tratteggiata nella Figura 27.2d che collega f4 con c1-s-read indica che questa connessione non è stata generata dalle regole predefinite di BLP ma da un'operazione di sistema.

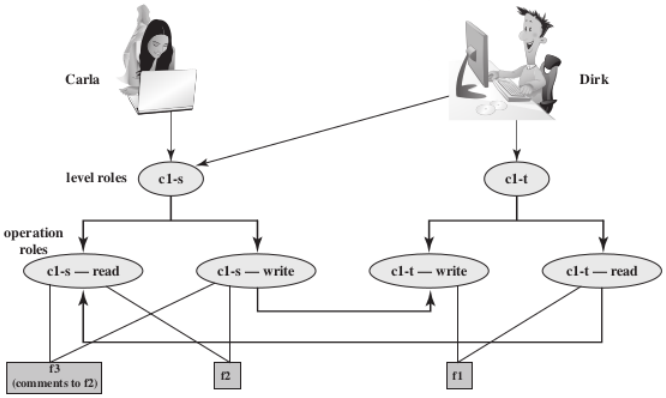
6. **Carla scrive le risposte all'esame in un file f5**.

   Crea il file a livello c1-t in modo che solo Dirk possa leggere il file.

   Questo è un esempio di scrittura, che non è vietato dalle regole BLP. Carla può ancora vedere le sue risposte alla sua stazione di lavoro, ma non può accedere a f5 per leggere.

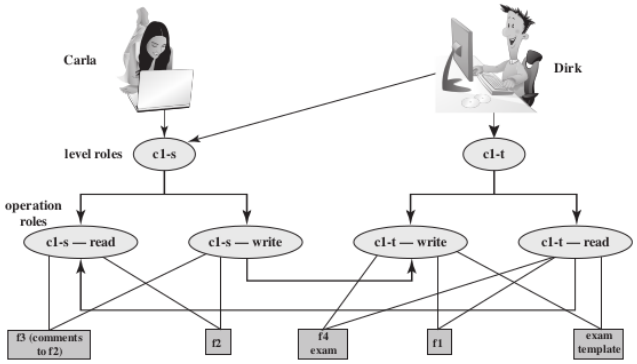


(a) Two new files are created: f1: c1-t; f2: c1-s

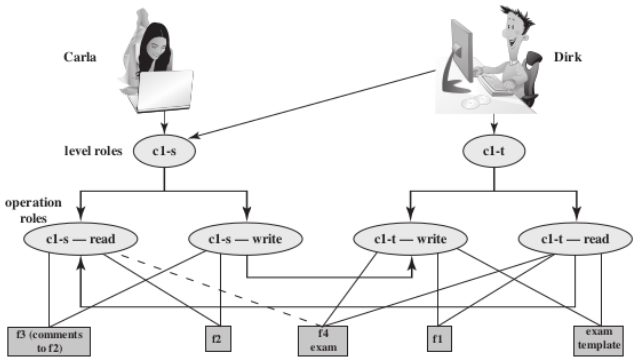


(b) A third file is added: f3: c1-s

Figure 27.2 **Example of Use of BLP Concepts**

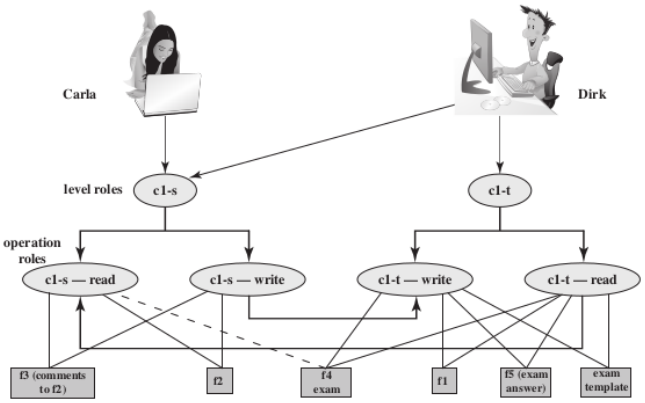


(c) An exam is created based on an existing template: f4: c1-t



(d) Carla, as student, is permitted acess to the exam: f4: c1-s

Figure 27.2 **Example of Use of BLP Concepts**



(e) The answers given by Carla are only accessible for the teacher: f5: c1-t

In primo luogo, come notato al punto 4, il modello BLP non ha alcuna disposizione per gestire il "downgrade" di oggetti, anche se i requisiti per la sicurezza multilivello riconoscono che tale un flusso di informazioni da un livello superiore a uno inferiore può essere richiesto, purché rifletta la volontà di un utente autorizzato. Quindi, qualsiasi implementazione pratica di un sistema multilivello deve supportare tale processo in modo controllato e monitorato. Collegato a questo c'è un'altra preoccupazione. Un soggetto

vincolato dal modello BLP può solo "editare" (leggere e scrivere) un file ad un livello di sicurezza mentre visualizza anche file allo stesso livello o a livelli inferiori. Se il nuovo documento consolida informazioni da una gamma di fonti e livelli, alcune di quelle informazioni sono ora classificate ad un livello rispetto a quello originale. Questo è noto come classification creep ed è un problema ben noto preoccupazione quando si gestiscono informazioni multilivello. Anche in questo caso, è necessario un processo di declassamento delle informazioni è necessario per ripristinare livelli di classificazione ragionevoli.

1.14.6 Esempio di implementazione Multics

Un'implementazione di MLS sul sistema operativo Multics.

Iniziamo con una breve descrizione degli aspetti rilevanti di Multics. Multics è un sistema operativo a tempo condiviso che fu sviluppato da un gruppo del MIT noto come Progetto MAC (computer ad accesso multiplo) negli anni '60. Multics era non solo anni, ma decenni in anticipo sui tempi. Anche a metà degli anni '80, quasi 20 anni dopo essere diventato operativo, Multics aveva caratteristiche di sicurezza superiori e una maggiore sofisticazione nell'interfaccia utente e in altre aree rispetto ad altri sistemi operativi per mainframe contemporanei. Sia la gestione della memoria che il file system in Multics sono basati sul concetto di segmenti. La memoria virtuale è segmentata. Ogni file nel file system è definito come un segmento. Così, il sistema operativo utilizza lo stesso meccanismo per caricare un segmento di dati dalla memoria virtuale nella memoria principale, e per caricare un file dalla memoria virtuale nella memoria principale. I segmenti sono organizzati gerarchicamente, da una directory principale fino ai singoli segmenti.

Multics gestisce lo spazio di indirizzamento virtuale per mezzo di un segmento descrittore, che è associato ad un processo e che ha una voce per ogni segmento nella memoria virtuale accessibile da questo processo. Il registro base del segmento del descrittore punta all'inizio del segmento descrittore per il processo attualmente in esecuzione. Per MLS, sono necessarie due caratteristiche aggiuntive. Una tabella a livello di processo include ed una voce per ogni processo attivo, e la voce indica l'autorizzazione di sicurezza del processo. Associato ad ogni segmento c'è un livello di sicurezza, che è memorizzato nel segmento del segmento in questione.

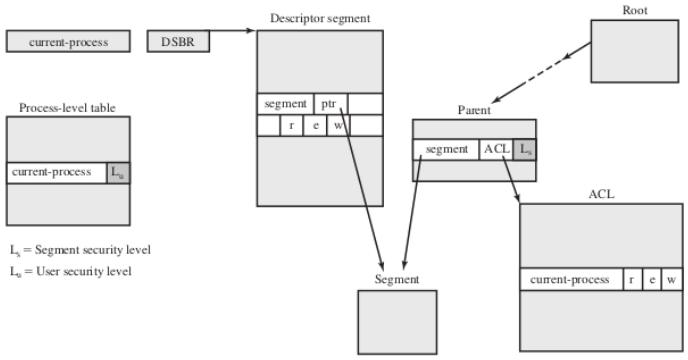


Figure 27.3 **Multics Data Structures for MLS**

Corrispondente allo stato di sicurezza del modello BLP (b, M, f, H) è un insieme di strutture dati Multics (vedi Figura 27.3).
La corrispondenza è la seguente:

- **b:** Segmento descrittore parola.

Il segmento descrittore identifica il soggetto (processo). Il puntatore di segmento nella parola descrittore di segmento identifica l'oggetto (segmento dati). I tre bit di controllo dell'accesso nel segmento descrittore di segmento identificano il modo di accesso.

- **M:** elenco di controllo dell'accesso
- **f:** Informazioni nel segmento directory e nella tabella a livello di processo.
- **H:** Struttura gerarchica del segmento.

Con queste strutture di dati, Multics può imporre il controllo di accesso discrezionale e obbligatorio. Quando un processo tenta un accesso ad un segmento, deve avere il permesso di accesso desiderato come specificato dalla lista di controllo degli accessi. Inoltre, la sua autorizzazione di sicurezza viene confrontata con la classificazione di sicurezza del segmento a cui accedere per determinare se la regola di sicurezza semplice e la regola di sicurezza sono soddisfatte.

1.14.7 Limitazioni modello BLP

Mentre il modello BLP potrebbe, in teoria, porre le basi per un calcolo sicuro all'interno di un ambiente di amministrazione singola, ci sono alcune importanti limitazioni alla sua usabilità e difficoltà di implementazione.

1. L'incompatibilità di riservatezza e integrità all'interno di un singolo sistema MLS.

   In termini generali, MLS può funzionare sia per i poteri che per i segreti, ma non prontamente per entrambi. Questa esclusione reciproca esclude alcune interessanti tecnologie centrate sulla potenza e sull'integrità di essere usate efficacemente in ambienti MLS in stile BLP.

2. Limitazione all'usabilità è il cosiddetto problema del cospiratore cooperante.

   In presenza di canali nascosti. In presenza di risorse condivise, la proprietà * può diventare inapplicabile. Questo è un problema specialmente nella presen contenuto attivo che è prevalente nell'attuale elaborazione di testi e in altri formati di documenti. Un documento maligno potrebbe contenere un soggetto che quando eseguito trasmette documenti classificati usando canali segreti a risorse condivise. In essenza, il modello BLP si rompe efficacemente quando i dati eseguibili (non fidati) a bassa classificazione dati eseguibili a bassa classificazione possono essere eseguiti da un soggetto ad alta autorizzazione (fidato).

1.15 Altri modelli per la sicurezza informatica

È importante notare che i modelli descritti in questo capitolo si concentrano sulla riservatezza o sull'integrità, con l'eccezione del Chinese Wall Model. L'incompatibilità delle preoccupazioni di riservatezza e integrità è riconosciuta come una grande limitazione all'usabilità di MLS in generale, e a MLS focalizzati sulla riservatezza in particolare.

1.15.1 Modello di integrità Biba

Il modello BLP si occupa della riservatezza ed è preoccupato della divulgazione non autorizzata delle informazioni. Il modello Biba si occupa dell'integrità e si occupa della modifica non autorizzata dei dati. Il modello Biba è destinato a trattare il caso in cui ci sono dati che devono essere visibili agli utenti a più o a tutti i livelli di sicurezza, ma devono essere modificati solo in modi controllati da agenti autorizzati.

Gli elementi di base del modello Biba hanno la stessa struttura del modello BLP. Come con BLP, il modello Biba si occupa di soggetti e oggetti. Ogni soggetto e oggetto è assegnato un livello di integrità, indicato come I(S) e I(O) per il soggetto S e l'oggetto O, rispettivamente. Si può usare una semplice classificazione gerarchica, in cui c'è un ordine rigoroso dei livelli dal più basso al più alto.

Come nel modello BLP, è anche possibile aggiungere un insieme di compartimenti allo schema di classificazione.

Il modello considera le seguenti modalità di accesso:

1. **Modificare:** Scrivere o aggiornare le informazioni in un oggetto
2. **Osservare:** Leggere le informazioni di un oggetto
3. **Eseguire:** Eseguire un oggetto
4. **Invocare:** Comunicazione da un oggetto all'altro

I primi tre modi sono analoghi ai modi di accesso BLP. Il modo invoke è nuovo. Biba propone poi una serie di politiche alternative che possono essere imposte a questo modello. La più rilevante è la politica di integrità rigorosa, basata sulle seguenti regole:

- **Integrità semplice:** Un soggetto può modificare un oggetto solo se il livello di integrità del soggetto domina il livello di integrità dell'oggetto: I(S) >= I(O).
- **Confinamento dell'integrità:** Un soggetto può leggere un oggetto solo se il livello di integrità del soggetto è dominato dal livello di integrità dell'oggetto: I(S) <= I(O).
- **Proprietà di invocazione:** Un soggetto può invocare un altro soggetto solo se il livello di integrità livello di integrità del primo soggetto domina il livello di integrità del secondo soggetto: I(S1) >= I(S2).

Le prime due regole sono analoghe a quelle del modello BLP ma riguardano dell'integrità e invertono il significato di lettura e scrittura. La semplice regola di integrità è la restrizione logica di scrittura che impedisce la contaminazione dei dati ad alta integrità. Un processo a bassa integrità può leggere dati a bassa integrità ma gli viene impedito di contaminare un file ad alta integrità con quei dati grazie alla semplice regola di integrità. Se solo questa regola è in vigore, un processo ad alta integrità potrebbe plausibilmente copiare dati a bassa integrità in un file ad alta integrità in un file ad alta integrità. Normalmente, ci si aspetterebbe che un processo ad alta integrità non contamini un file ad alta integrità, ma un errore nel codice del processo o un cavallo di Troia potrebbe risultare in tale contaminazione; da qui la necessità della regola di confinamento dell'integrità.
Inserire immagine 27.4

1.15.2 Modello di integrità Clark-Wilson

Un modello di integrità più elaborato e forse più pratico è stato proposto da Clark e Wilson. Il modello di integrità Clark-Wilson (CWM) è rivolto ad applicazioni commerciali piuttosto che militari e modella da vicino le reali operazioni commerciali. Il modello si basa su due concetti che sono tradizionalmente usati per applicare politiche di sicurezza commerciali:

- **Transazioni ben formate:** Un utente non dovrebbe manipolare i dati arbitrariamente, ma solo in modi limitati che preservano o assicurano l'integrità dei dati.
- **Separazione dei compiti tra gli utenti:** Ogni persona autorizzata a creare o certificare una transazione ben formata non può essere autorizzata ad eseguirla (almeno contro dati di produzione). Il modello impone controlli di integrità sui dati e sulle transazioni che manipolano i dati.

I componenti principali del modello sono i seguenti:

- **Elementi di dati vincolati (CDI):** Soggetti a severi controlli di integrità
- **Elementi di dati non vincolati (UDI):** Elementi di dati non controllati. Un esempio è un semplice file di testo
- **Procedure di verifica dell'integrità (IVP):** Destinate ad assicurare che tutte le CDI sono conformi a qualche modello di integrità e coerenza specifico dell'applicazione
- **Procedure di trasformazione (TP):** Transazioni di sistema che cambiano l'insieme delle CDI da uno stato coerente ad un altro Il CWM fa rispettare l'integrità per mezzo di regole di certificazione e applicazione sui TP. Le regole di certificazione sono restrizioni di politica di sicurezza sul comportamento di IVP e dei TP.

  Le regole di applicazione sono meccanismi di sicurezza integrati nel sistema che raggiungono gli obiettivi delle regole di certificazione.

Le regole sono le seguenti:

Cl: Tutti gli IVP devono garantire adeguatamente che tutti i CDI siano in uno stato valido nel momento in cui l'IVP viene eseguito.

C2: Tutti i TP devono essere certificati per essere validi. Cioè, devono portare un CDI ad uno stato finale valido, dato che è in uno stato valido per cominciare. Per ogni TP, ogni insieme di CDI che può manipolare, il responsabile della sicurezza deve specificare una relazione che definisce tale esecuzione. Una relazione è quindi della forma (TPi, (CDIa, CDIb, CDIc . . .)), dove la lista dei CDI definisce un particolare insieme di argomenti per i quali il TP è stato certificato.

El: Il sistema deve mantenere la lista di relazioni specificata nella regola C2 e deve assicurare che l'unica manipolazione di qualsiasi CDI sia da parte di un TP, dove il TP sta operando sul CDI come specificato in qualche relazione.

E2: Il sistema deve mantenere una lista di relazioni della forma (UserID, TPi,(CDIa, CDIb, CDIc, . . .)), che mette in relazione un utente, un TP e gli oggetti dati che il TP può referenziare per conto di quell'utente. Deve assicurare che solo esecuzioni descritte in una delle relazioni.

C3: L'elenco delle relazioni in E2 deve essere certificato per soddisfare il requisito di separazione dei compiti.

E3: Il sistema deve autenticare l'identità di ogni utente che tenta di eseguire un TP.

C4: Tutti i TP devono essere certificati per scrivere in un CDI di sola appendice (il log) tutte le informazioni necessarie per permettere di ricostruire la natura dell'operazione.

C5: Ogni TP che prende un UDI come valore di ingresso deve essere certificato per eseguire solo trasformazioni valide, oppure nessuna trasformazione, per ogni possibile valore dell'UDI. La trasformazione dovrebbe prendere l'input da un UDI, o l'UDI viene rifiutata. Tipicamente, questo è un programma di modifica.

E4: Solo l'agente autorizzato a certificare entità può cambiare la lista di tali entità associate ad altre entità: in particolare, la lista dei TP associati con un CDI e la lista degli utenti associati a un TP. Un agente che può certificare un'entità non può avere alcun diritto di esecuzione rispetto a tale entità.

Inserire figura 27.5

1.15.3 Modello Muraglia Cinese

Il Chinese Wall Model (CWM) ha un approccio abbastanza diverso per specificare integrità e riservatezza rispetto a qualsiasi approccio che abbiamo esaminato finora. Il modello è stato sviluppato per applicazioni commerciali in cui possono sorgere conflitti di interesse. Il modello fa uso di concetti di accesso sia discrezionali che obbligatori. L'idea principale dietro il CWM è un concetto che è comune nelle professioni e nelle professioni legali, che è quello di usare una cosiddetta muraglia cinese per prevenire un conflitto di interessi. Un esempio dal mondo finanziario è quello di un analista di mercato che lavora per un'istituzione finanziaria che fornisce servizi aziendali. Un analista non può essere autorizzato a fornire consigli a una società quando l'analista ha informazioni riservate (conoscenza privilegiata) sui piani o lo stato di un concorrente. Tuttavia l'analista è libero di consigliare più società che non sono in concorrenza tra loro e di attingere alle informazioni di mercato che sono aperte al pubblico.

Gli elementi del modello sono i seguenti:

- **Soggetti:** Entità attive che potrebbero voler accedere a oggetti protetti. include utenti e processi
- **Informazioni:** Informazioni aziendali organizzate in una gerarchia con tre livelli
  - **Oggetti:** Singoli elementi di informazione, ciascuno riguardante una singola società
  - **Set di dati (DS):** Tutti gli oggetti che riguardano la stessa società
  - **Classe di conflitto di interessi (CI):** Tutti i set di dati le cui società sono in concorrenza
- **Regole di accesso:** Regole per l'accesso in lettura e scrittura

A differenza dei modelli che abbiamo studiato finora, il CWM non assegna livelli di sicurezza a soggetti e oggetti e quindi non è un vero modello sicuro multi-livello. Invece, la storia del precedente accesso di un soggetto determina il controllo dell'accesso. La base della politica della muraglia cinese è che i soggetti possono accedere solo alle informazioni che non è ritenuto in conflitto con qualsiasi altra informazione che già possiedono. Una volta che un soggetto accede alle informazioni di un set di dati, una muraglia è impostata per proteggere le informazioni in altri insiemi di dati nello stesso CI. Il soggetto può accedere alle informazioni su un lato del del muro ma non dall'altro lato. Inoltre, le informazioni in altri CI non sono inizialmente Inoltre, le informazioni in altri IC non sono inizialmente considerate su un lato o l'altro del muro, ma all'aperto. Quando lo stesso soggetto effettua ulteriori accessi in altri IC, la forma del muro cambia per mantenere la protezione desiderata. Inoltre, ogni soggetto è controllato dal proprio pareti per i diversi soggetti che sono diverse.

Per far rispettare la politica della muraglia cinese, sono necessarie due regole. Per indicare la similarità con le due regole BLP, gli autori hanno dato loro gli stessi nomi.

La prima regola è la **semplice regola di sicurezza**

Regola di sicurezza semplice:

- O si trova nello stesso DS di un oggetto a cui S ha già avuto accesso
- O appartiene a un CI da cui S non ha ancora avuto accesso a nessuna informazione.

inserire figura 27.6
John ha fatto la sua prima richiesta di lettura a qualsiasi oggetto in questo set per un oggetto nella Banca A DS. Poiché John non ha precedentemente avuto accesso ad un oggetto in nessun altro DS in CI 1, l'accesso accesso è concesso. Inoltre, il sistema deve ricordare che l'accesso è stato concesso in modo che ogni successiva richiesta di accesso a un oggetto nella Banca B DS sarà negata. Qualsiasi richiesta di accesso ad altri oggetti nella Banca A DS è concessa. In un momento successivo, John richiede l'accesso ad un oggetto nella Banca A DS. Poiché non c'è conflitto, questo accesso viene concesso, ma viene creato un muro che proibisce il successivo accesso all'Oil B DS, come mostrato nella Figura 27.6b. Allo stesso modo, la Figura 27.6c riflette la storia di accesso alternativo di Jane. Nel nostro esempio, John ha accesso a Oil A DS e Bank A DS; Jane ha accesso a Oil B DS e Bank A DS. Se John è autorizzato a leggere dall'Oil A DS e scrivere nel Bank A DS, John può trasferire informazioni sull'olio A nel Bank A DS; ciò è indicato dal cambiamento del valore del primo oggetto sotto il Bank A DS a g. I dati possono poi essere letti da Jane. Così, Jane avrebbe accesso alle informazioni sia sul petrolio A che sul petrolio B, creando un conflitto di interessi.

Per prevenire questo, il CWM ha una **seconda regola**

Regola della proprietà: Un soggetto S può scrivere un oggetto O solo se:

- S può leggere O secondo la regola di sicurezza semplice, E
- Tutti gli oggetti che S può leggere sono nella stessa DS di O.

Detto altrimenti, o il soggetto non può scrivere affatto, o l'accesso di un soggetto (sia lettura e scrittura) è limitato ad un singolo set di dati. Così, nella figura 27.6, né John né Jane ha accesso in scrittura a qualsiasi oggetto nell'universo complessivo dei dati.

La regola proprietà è abbastanza restrittiva. Tuttavia, in molti casi, un utente ha solo ha bisogno dell'accesso in lettura perché l'utente sta eseguendo qualche ruolo di analisi.

Per facilitare in qualche modo la restrizione di scrittura, il modello include il concetto di dati sanificati. In sostanza, i dati sanificati sono dati che possono essere derivati dai dati aziendali ma che non possono essere usati per scoprire l'identità della società. Qualsiasi DS che consiste esclusivamente di dati sanificati non ha bisogno di essere protetto da un muro; quindi, le due regole CWM non si non si applicano a tali DS.

1.16 Il concetto di sitemi fidati

1.16.1 Applicazione sicurezza multilivello

Sicurezza multilivello (MLS) è un modo di funzionamento del sistema in cui:

- **Due o più livelli di sicurezza** delle informazioni possono essere gestiti simultaneamente all'interno dello stesso sistema quando alcuni utenti che hanno accesso al sistema non hanno né un nulla osta di sicurezza né la necessità di sapere per alcuni dei dati gestiti dal sistema.
- **La separazione degli utenti e del materiale classificato sulla base** dell'autorizzazione e del livello di classificazione dipendono dal controllo del sistema operativo.

La sicurezza multilivello è interessante quando c'è la necessità di mantenere una risorsa, come un file system o un database in cui sono definiti più livelli di sensibilità dei dati. La gerarchia potrebbe essere semplice come due livelli (ad esempio, pubblico e proprietario) o potrebbe avere molti livelli (ad esempio, il militare non classificato, riservato, confidenziale, segreto, top secret). Le tre sezioni precedenti ci hanno introdotto agli elementi essenziali della sicurezza multilivello.

In questa sezione, esaminiamo due applicazioni in cui sono stati applicati i concetti di MLS:

1. Sistema di controllo degli accessi basato sui ruoli.
2. La sicurezza dei database.

1.16.2 Sicurezza multilivello per il controllo dell'accesso basato sui ruoli

Mostra come un sistema di controllo degli accessi basato su regole (RBAC) può essere usato per implementare le regole di sicurezza multilivello BLP. Ricordiamo che la specifica ANSI standard RBAC ANSI includeva il concetto di funzioni amministrative, che forniscono la capacità di creare, cancellare e mantenere elementi e relazioni RBAC. È utile quindi assegnare ruoli amministrativi speciali a queste funzioni. Con questo in mente, La Tabella 27.2 riassume i componenti di un RBAC.

La seguente specifica formale indica come un sistema RBAC può essere usato per implementare l'accesso MLS:

- **Vincolo sugli utenti:**

  Per ogni utente u nell'insieme degli utenti U, viene assegnato un nulla osta di sicurezza L(u). Formalmente, qualsiasi u $\in$ U [$L(u)dato$].

- **Vincoli sui permessi:**

  Ogni permesso assegna un permesso di lettura o scrittura a un oggetto o, e ogni oggetto ha un permesso di lettura e uno di scrittura. Tutti gli oggetti hanno una classificazione di sicurezza. Formalmente, $P = \{(o, r), (o, w)$ o è un oggetto nel sistema$\}$ qualsiasi o $\in$ P[L(o) è dato].

- **Definizioni:**

  Il livello di lettura di un ruolo r, denotato r-level(r), è il minimo limite superiore dei livelli di sicurezza degli oggetti per i quali (o, r) è nelle autorizzazioni di r. Il livello w di un ruolo r (denotato w-level(r)) è il massimo limite inferiore (glb) dei livelli di sicurezza degli oggetti o per i quali (o, w) è nelle permessi di r, se tale glb esiste. Se il glb non esiste, il livello w è indefinito.

- **Vincoli su UA:**

  Ogni ruolo r ha un livello di scrittura definito, denotato w-level(r). Per ogni assegnazione dell'utente, l'autorizzazione dell'utente deve dominare il livello r del ruolo ed essere dominata dal livello w del ruolo. Formalmente, qualsiasi r $\in$ UA [w-level(r) è definito]; qualsiasi (u,r) $\in$ UA [L(u) >= r-livello(r)]; qualsiasi (u,r) $\in$ UA [L(u) <= w-livello(r)].

Le definizioni e i vincoli precedenti applicano il modello BLP. Un ruolo può includere permessi di accesso per più oggetti. Il livello r del ruolo indica la più alta classificazione di sicurezza per gli oggetti assegnati al ruolo. Così, la semplice proprietà di sicurezza (nessuna lettura) richiede che un utente possa essere assegnato a un ruolo solo se l'autorizzazione dell'utente è almeno pari al livello r del ruolo. Allo stesso modo, il livello w del ruolo indica la classificazione di sicurezza più bassa dei suoi oggetti. La proprietà sicurezza (no write down) richiede che un utente sia assegnato a un ruolo solo se il suo non è superiore al livello w del ruolo.

Inserire Tabella 27.2

1.16.3 Sicurezza dei database e sicurezza multilivello

L'aggiunta della sicurezza multilivello a un sistema di database aumenta la complessità della funzione di controllo dell'accesso e del design del database stesso. Una questione chiave è la granularità della classificazione. I seguenti sono possibili metodi per imporre la sicurezza multilivello su un database relazionale, in termini di granularità di classificazione (vedi Figura 27.9):

- **Intero database:** Questo semplice approccio è facilmente realizzabile su una piattaforma MLS. Un intero database, come un database finanziario o personale, potrebbe essere classificato come confidenziale o riservato e mantenuto su un server con altri file.
- **Tabelle individuali (relazioni):** Per alcune applicazioni, è appropriato assegnare classificazione a livello di tabella. Nell'esempio della Figura 27.9a, sono definiti due livelli di classificazione:
  - Unrestricted (U)
  - Restricted (R)

La tabella Employee contiene informazioni sensibili sullo stipendio ed è classificata ristretta, mentre la tabella tabella Department è illimitata. Questo livello di granularità è relativamente facile da implementare e applicare.

- **Colonne individuali (attributi):** Un amministratore della sicurezza può scegliere di determinare la classificazione sulla base degli attributi, in modo che le colonne selezionate sono classificate. Nell'esempio della Figura 27.9b, l'amministratore determina che le informazioni sullo stipendio e l'identità dei responsabili di reparto sono informazioni riservate.
- **Righe individuali (tuple):** altre circostanze, può avere senso assegnare livelli di classificazione sulla base di singole righe che corrispondono a certe proprietà. Nell'esempio della figura 27.9c, tutte le righe della tabella Department che contengono informazioni relative al dipartimento di contabilità (Dept. ID = 4), e tutte le righe nella tabella Employee per le quali lo stipendio è maggiore di 50K sono limitate.
- **Elementi individuali:** Lo schema più difficile da implementare e gestire è uno in cui i singoli elementi possono essere classificati selettivamente. Nell'esame Figura 27.9d, le informazioni sullo stipendio e l'identità del manager del eparto contabilità sono limitate

La granularità dello schema di classificazione influisce sul modo in cui il controllo dell'accesso viene applicato. In particolare, gli sforzi per prevenire l'inferenza dipendono dalla granularità della classificazione.
Inserire figura 27.9

1.17 Trusted Computing e il Trusted Platform Module

Il trusted platform module (TPM) è un concetto standardizzato da un consorzio industriale consorzio industriale, il Trusted Computing Group. Il TPM è un modulo hardware che è al il cuore di un approccio hardware/software all'informatica di fiducia. Infatti, il termine trusted computing (TC) è ora usato nell'industria per riferirsi a questo tipo di approccio hardware/approccio hardware/software. L'approccio TC impiega un chip TPM nella scheda madre del personal computer o una smart card o integrato nel processore principale, insieme all'hardware e al software che in qualche modo è stato approvato o certificato per lavorare con il TPM.

Il TPM genera chiavi che condivide con i componenti vulnerabili che passano dati all'interno del sistema, come i dispositivi di archiviazione, i componenti di memoria e l'hardware audio/visivo. hardware audio/video. Le chiavi possono essere usate per crittografare i dati che fluiscono attraverso la macchina. Il TPM funziona anche con il software abilitato a TC, incluso il sistema operativo e le applicazioni.

Il software può essere sicuro che i dati che riceve sono affidabili, e il sistema può essere sicuro che il software stesso sia affidabile.

Per ottenere queste caratteristiche, TC fornisce tre servizi di base: avvio autenticato, certificazione e crittografia.

1.17.1 Servizio di avvio autenticato

Il servizio di avvio autenticato è responsabile dell'avvio dell'intero sistema operativo in fasi e assicurando che ogni porzione del sistema operativo, quando viene caricata, sia una versione che è approvato per l'uso. Tipicamente, l'avvio di un sistema operativo inizia con un piccolo pezzo di codice nella ROM. Questo pezzo porta altro codice dal blocco di avvio sul disco rigido e trasferisce l'esecuzione a quel codice. Questo processo continua con blocchi sempre più grandi del codice del sistema operativo fino a quando l'intera procedura di avvio del sistema operativo è completa e il sistema operativo residente è avviato. Ad ogni stadio, l'hardware del TC controlla che il software valido sia stato portato dentro. Questo può essere fatto verificando una firma digitale associata al software.

Il TPM tiene un registro a prova di manomissione del processo di caricamento, usando una funzione di hash crittografica per rilevare qualsiasi manomissione del registro. Quando il processo è completato, il registro a prova di manomissione contiene un record che stabilisce esattamente quale versione del sistema operativo e i suoi vari moduli sono in esecuzione. È ora possibile espandere il confine di fiducia per includere ulteriore hardware e applicazioni e software di utilità. Il sistema abilitato TC mantiene una lista approvata di componenti hardware e software approvati. Per configurare un pezzo di hardware o caricare un software, il sistema controlla se il componente è nella lista approvata, se è firmato digitalmente (dove applicabile), e se il suo numero di serie non è stato revocato. Il risultato è una configurazione di hardware, software di sistema e applicazioni che è in uno stato ben definito con componenti approvati.

1.17.2 Servizio di certificazione

Una volta che una configurazione è raggiunta e registrata dal TPM, il TPM può certificare la configurazione ad altre parti. Il TPM può produrre un certificato digitale firmando una descrizione formattata delle informazioni di configurazione usando la chiave privata del TPM. Così, un altro utente, sia un utente locale che un sistema remoto, può avere fiducia che una configurazione inalterata è in uso perché:

1. Il TPM è considerato affidabile. Non abbiamo bisogno di un'ulteriore certificazione del TPM stesso.

2. Solo il TPM possiede la chiave privata di questo TPM. Un destinatario della configurazione può usare la chiave pubblica del TPM per verificare la firma (vedi Figura 2.7b).

Per assicurare che la configurazione sia puntuale, un richiedente emette una "sfida" sotto forma di un numero casuale quando richiede un certificato firmato dal TPM.

Il TPM firma un blocco di dati che consiste nelle informazioni di configurazione con il numero casuale aggiunto ad esso. Il richiedente può quindi verificare che il certificato sia valido e aggiornato.

Lo schema TC prevede un approccio gerarchico alla certificazione. Il TPM certifica la configurazione hardware/OS. Poi il sistema operativo può certificare la presenza e la configurazione dei programmi applicativi. Se un utente si fida del TPM e si fida della versione certificata del sistema operativo, allora l'utente può avere fiducia nella configurazione dell'applicazione.

1.17.3 Servizio di crittografia

Il servizio di crittografia permette la crittografia dei dati in modo tale che i dati possano essere decifrati solo da una certa macchina, e solo se questa macchina è in una certa configurazione. Ci sono diversi aspetti di questo servizio.

In primo luogo, il TPM mantiene una chiave segreta principale unica per questa macchina. Da questa chiave, il TPM genera una chiave di crittografia segreta per ogni possibile configurazione di quella macchina. Se i dati sono criptati mentre la macchina è in una configurazione, i dati possono essere decifrati solo usando quella stessa configurazione. Se una configurazione diversa viene creata sulla macchina, la nuova configurazione non sarà in grado di decifrare i dati crittografati da una configurazione diversa.

Questo schema può essere esteso verso l'alto, come si fa con la certificazione. Così, è possibile fornire una chiave di crittografia ad un'applicazione in modo che l'applicazione possa criptare i dati, e la decriptazione possa essere fatta solo dalla versione desiderata dell'applicazione desiderata che gira sulla versione desiderata del sistema operativo desiderato. Questi dati crittografati possono essere memorizzati localmente, recuperabili solo dall'applicazione che li ha memorizzati, o trasmessi a un'applicazione peer su una macchina remota. L'applicazione peer dovrebbe essere nella stessa configurazione per decifrare i dati.

1.17.4 Funzioni TPM

Per dare un'idea del funzionamento di un sistema TC/TPM, guardiamo la funzione di memorizzazione protetta. Il TPM genera e memorizza un certo numero di chiavi crittografia in una gerarchia di fiducia. Alla radice della gerarchia c'è una chiave radice di memorizzazione generata dal TPM e accessibile solo per l'uso del TPM. Da questa chiave, altre chiavi possono essere generate e protette dalla crittografia con chiavi più vicine alla radice della gerarchia.
Una caratteristica importante delle Trusted Platforms è che un oggetto protetto dal TPM può essere "sigillato" ad un particolare stato del software in una piattaforma. Quando l'oggetto protetto TPM viene creato, il creatore indica lo stato del software che deve esistere se il segreto deve essere rivelato. Quando un TPM scarta l'oggetto protetto TPM (all'interno del TPM e nascosto alla vista), il TPM controlla che lo stato attuale del software corrisponda allo stato del software indicato. Se corrispondono, il TPM permette l'accesso al segreto. Se non non corrispondono, il TPM nega l'accesso al segreto.

La figura 27.12 fornisce un esempio di questa protezione. In questo caso, c'è un file criptato sulla memoria locale a cui un'applicazione utente desidera accedere. I seguenti passi da compiere:

1. La chiave simmetrica che è stata usata per criptare il file è memorizzata con il file. La chiave stessa è criptata con un'altra chiave a cui il TPM ha accesso. La chiave protetta è presentata al TPM con una richiesta di rivelare la chiave all'applicazione.

2. Associata alla chiave protetta è una specifica della configurazione hardware/software che può avere accesso alla chiave. Il TPM verifica che la configurazione corrente corrisponda alla configurazione richiesta per rivelare la chiave. Inoltre, l'applicazione richiedente deve essere specificamente autorizzata ad accedere alla chiave. Il TPM usa un protocollo di autorizzazione per verificare l'autorizzazione.

3. Se la configurazione corrente permette l'accesso alla chiave protetta, allora il TPM decifra la chiave e la passa all'applicazione.

4. L'applicazione usa la chiave per decifrare il file. L'applicazione è affidabile per poi scartare la chiave in modo sicuro.

La crittografia di un file procede in modo analogo. In quest'ultimo caso, un processo richiede una chiave simmetrica per cifrare il file. Il TPM fornisce quindi una versione criptata della chiave da memorizzare con il file.
Inserire foto27.12

1.18 Criteri comuni per la valutazione della sicurezza informatica

Il lavoro svolto dalla National Security Agency e da altre agenzie governative statunitensi per sviluppare requisiti e criteri di valutazione per i sistemi affidabili ha portato alla

pubblicazione del Trusted Computer System Evaluation Criteria (TCSEC), informalmente noto come Orange Book, nei primi anni '80. Questo si concentrava principalmente per proteggere la riservatezza delle informazioni. Successivamente, altri paesi hanno iniziato a lavorare per sviluppare criteri basati sul TCSEC che fossero più flessibili e adattabili alla natura in evoluzione dell'informatica. Il processo di fusione, estensione e consolidamento di questi vari sforzi alla fine è sfociato nello sviluppo dei Criteri Comuni alla fine degli anni '90. I Common Criteria (CC) per l'Information Technology e la valutazione della sicurezza sono standard ISO per specificare i requisiti di sicurezza e definire i criteri di valutazione.

Lo scopo di questi standard è quello di fornire una maggiore fiducia nella sicurezza dei prodotti IT come risultato di azioni formali prese durante il processo di sviluppo, valutazione e funzionamento di questi prodotti. Nella fase di sviluppo, il CC definisce insiemi di requisiti IT di validità nota che possono essere usati per stabilire i i requisiti di sicurezza di futuri prodotti e sistemi. Poi il CC dettagli come un prodotto specifico può essere valutato rispetto a questi requisiti noti, per fornire la conferma che esso li soddisfi davvero, con un adeguato livello di fiducia. Infine, quando è in funzione, l'ambiente IT in evoluzione può rivelare nuove vulnerabilità o preoccupazioni. Il CC dettaglia un processo per rispondere a tali cambiamenti, e possibilmente per rivalutare il prodotto. A seguito di una valutazione positiva, un particolare prodotto può essere elencato come certificato CC o convalidato dall'appropriata agenzia nazionale, come il NIST/NSA negli Stati Uniti. Tale agenzia pubblica elenchi dei prodotti valutati, che sono usati dagli acquirenti del governo e dell'industria che hanno bisogno di usare tali prodotti.

1.18.1 Requisiti

Il CC definisce un insieme comune di potenziali requisiti di sicurezza da usare nella valutazione. Il termine obiettivo della valutazione (TOE) si riferisce a quella parte del prodotto o sistema che è soggetto alla valutazione. I requisiti rientrano in due categorie:

1. **Requisiti funzionali**

   Definiscono il comportamento di sicurezza desiderato. I documenti CC stabiliscono un insieme di componenti funzionali di sicurezza che forniscono un modo standard di esprimere i requisiti funzionali di sicurezza per un TOE.

2. **Requisiti di sicurezza**

   La base per ottenere la fiducia che le misure di sicurezza dichiarate misure di sicurezza dichiarate siano efficaci e implementate correttamente. I documenti CC stabiliscono un insieme di componenti di garanzia che forniscono un modo standard di esprimere i requisiti di garanzia per un TOE.

Sia i requisiti funzionali che quelli di garanzia sono organizzati in classi:

Una classe è una collezione di requisiti che condividono un obiettivo o un intento comune.

Le tabelle 27.3 e 27.4 definiscono brevemente le classi per i requisiti funzionali e di garanzia. Ciascuna di queste classi contiene un certo numero di famiglie. I requisiti all'interno di ogni famiglia condividono obiettivi di sicurezza, ma differiscono per enfasi o rigore. Per esempio, la classe di audit contiene sei famiglie che si occupano di vari aspetti dell'auditing (ad es, generazione di dati di audit, analisi di audit e memorizzazione di eventi di audit). Ogni famiglia, a sua volta, contiene uno o più componenti. Un componente descrive un insieme specifico di requisiti di sicurezza requisiti di sicurezza ed è il più piccolo insieme selezionabile di requisiti di sicurezza da includere nelle strutture definite nel CC.
Inserire tabella 27.3 e 27.4

1.18.2 Profili e Obiettivi

Il CC definisce anche due tipi di documenti che possono essere generati usando i requisiti definiti dal CC.

- **Profili di protezione (PP):** Definiscono un insieme indipendente dall'implementazionedi requisiti e obiettivi di sicurezza per una categoria di prodotti o sistemi che soddisfano esigenze simili dei consumatori per la sicurezza informatica.

  Un PP è inteso essere riutilizzabile e definire requisiti che sono noti per essere utili ed efficaci nel soddisfare gli obiettivi identificati. Il concetto di PP è stato sviluppato per supportare la definizione di standard funzionali e come aiuto alla formulazione di specifiche di approvvigionamento. Il PP riflette la sicurezza dell'utente esigenze degli utenti.

- **Obiettivi di sicuressa(ST):** Contengono gli obiettivi e i requisiti di sicurezza IT di uno specifico TOE identificato e definisce le misure funzionali e di garanzia offerte da quel TOE per soddisfare i requisiti dichiarati.

  La ST può dichiarare la conformità a uno o più PP e costituisce la base per una valutazione. La ST è fornito da un fornitore o sviluppatore. La figura 27.13 illustra la relazione tra i requisiti da un lato e i profili e gli obiettivi dall'altro. Per un PP, un utente può selezionare un numero di componenti per definire i requisiti del prodotto desiderato. L'utente può anche fare riferimento a pacchetti predefiniti che assemblano una serie di requisiti comunemente raggruppati insieme all'interno di un documento sui requisiti del prodotto. Allo stesso modo, un venditore o un progettista può selezionare una serie di componenti e pacchetti per definire un ST. La figura 27.14 mostra ciò a cui ci si riferisce nei documenti CC come paradigma dei requisiti funzionali di sicurezza. In sostanza, questa illustrazione si basa sul concetto di monitor di riferimento, ma fa uso della terminologia e della filosofia di progettazione del CC.

1.18.3 Esempio di protezione di un profilo

Il profilo di protezione per una smart card, sviluppato dallo Smart Card Security User Group, fornisce un semplice esempio di PP.

Questo PP descrive i requisiti di sicurezza IT per una smart card da usare in connessione con applicazioni sensibili, come i sistemi di pagamento finanziario dell'industria bancaria. Il livello di garanzia per questo PP è EAL 4, che è descritto nella seguente sottosezione. Il PP elenca le minacce che devono essere affrontate da un prodotto che dichiara di essere conforme a questo PP. Le minacce includono seguenti:

- **Sondaggio fisico:** Può comportare la lettura di dati dal TOE attraverso tecniche comunemente impiegate nell'analisi dei guasti IC e negli sforzi di reverse engineering IC.
- **Input non valido:** L'input non valido può assumere la forma di operazioni che non sono correttamente, richieste di informazioni oltre i limiti del registro, o tentativi di trovare ed eseguire comandi non documentati. Il risultato di un tale attacco può essere una compromissione delle funzioni di sicurezza, la generazione di errori sfruttabili nel funzionamento, o il rilascio di dati protetti.
- **Collegamento di più operazioni:** Un attaccante può osservare usi multipli di risorse o servizi e, collegando queste osservazioni, dedurre informazioni che possono rivelare dati sulla funzione di sicurezza.

Dopo un elenco di minacce, il PP passa alla descrizione degli obiettivi di sicurezza. Questi riflettono l'intento dichiarato di contrastare le minacce identificate e/o conformarsi a qualsiasi politiche di sicurezza organizzativa identificate. Sono elencati diciannove obiettivi, tra cui i seguenti:

- **Audit:** Il sistema deve fornire i mezzi per registrare determinati eventi rilevanti per la sicurezza eventi rilevanti per la sicurezza, in modo da assistere un amministratore nell'individuazione potenziali attacchi o configurazioni errate delle caratteristiche di sicurezza del sistema che lo lascerebbero suscettibile di attacco.
- **Inserimento dei guasti:** Il sistema deve essere resistente a sondaggi ripetuti attraverso inserimento di dati errati.
- **Perdita di informazioni:** Il sistema deve fornire i mezzi per controllare e limitare la perdita di informazioni nel sistema in modo che nessuna informazione utile sia rivelata attraverso le linee di alimentazione, terra, clock, reset o I/O.

I requisiti di sicurezza sono forniti per contrastare minacce specifiche e per supportare politiche specifiche sotto specifiche ipotesi. Il PP elenca requisiti specifici in tre aree generali: requisiti funzionali di sicurezza del TOE, requisiti di sicurezza del TOE, e requisiti di sicurezza per l'ambiente IT.

Nell'area dei requisiti funzionali di sicurezza, il PP definisce 42 requisiti delle classi disponibili di requisiti funzionali di sicurezza (vedi tabella 27.3).

Per esempio, per l'auditing di sicurezza, il PP stabilisce cosa deve controllare il sistema; quali informazioni devono essere registrate; quali sono le regole per monitorare, operare e proteggere i registri, e così via. I requisiti funzionali sono anche elencati da le altre classi di requisiti funzionali, con dettagli specifici per il funzionamento della smart card.

Il PP definisce 24 requisiti di garanzia della sicurezza dalle classi disponibili di requisiti di garanzia della sicurezza (vedi tabella 27.4). Questi requisiti sono stati scelti per dimostrare:

- La qualità della progettazione e della configurazione del prodotto
- Che viene fornita una protezione adeguata durante la progettazione e l'implementazione del prodotto
- Che il test del prodotto da parte del fornitore rispetta parametri specifici
- Che la funzionalità di sicurezza non è compromessa durante la consegna del prodotto
- che la guida per l'utente, compresi i manuali del prodotto relativi all'installazione, alla manutenzione e all'uso, siano di una qualità specifica, la manutenzione e l'uso, siano di una specifica qualità e adeguatezza

Il PP elenca anche i requisiti di sicurezza dell'ambiente IT. Questi coprono i seguenti argomenti:

- Distribuzione delle chiavi crittografiche
- Distruzione della chiave crittografica
- Ruoli di sicurezza

La sezione finale del PP (escluse le appendici) è una lunga motivazione per tutte delle selezioni e delle definizioni nel PP. Il PP è uno sforzo a livello industriale progettato per essere realistico nella sua capacità di essere soddisfatto da una varietà di prodotti con una varietà di meccanismi interni meccanismi interni e approcci di implementazione.

1.19 Assicurazione e valutazione

La garanzia può essere definita come una misura di fiducia che le caratteristiche di sicurezza e l'architettura di un sistema informativo (IS) mediano e applicano accuratamente la politica di sicurezza. Se si fa affidamento sulle caratteristiche di sicurezza di un IS per proteggere informazioni classificate o sensibili e limitare l'accesso degli utenti, le caratteristiche devono essere testate per assicurare che la politica di sicurezza sia applicata. Come per qualsiasi altro aspetto della sicurezza informatica, le risorse dedicate alla garanzia devono essere sottoposte a una sorta di analisi costi-benefici per determinare quale quantità di sforzo sia ragionevole per il livello di garanzia desiderato.

1.19.1 Destinatari

Il design delle misure di garanzia dipende in parte dal pubblico a cui queste misure. Cioè, nello sviluppare un grado di fiducia nelle misure di sicurezza, dobbiamo specificare quali individui o gruppi possiedono quel grado di fiducia. Il documento del CC sull'assicurazione elenca i seguenti destinatari:

- **Consumatori:** Selezionano le caratteristiche e le funzioni di sicurezza per un sistema e determinano i livelli richiesti di garanzia di sicurezza.
- **Sviluppatori:** Rispondono ai requisiti di sicurezza reali o percepiti dai consumatori; interpretare le dichiarazioni dei requisiti di sicurezza e determinare gli approcci e livello di sforzo.
- **Valutatori:** Usano i requisiti di garanzia come una dichiarazione obbligatoria di criteri di valutazione quando valutano le caratteristiche e i controlli di sicurezza.

I valutatori possono essere nella stessa organizzazione dei consumatori o un team di valutazione di terze parti.

1.19.2 Ambito di garanzia

La garanzia si occupa delle caratteristiche di sicurezza dei prodotti IT, come computer, database, sistemi operativi e sistemi completi. La garanzia si applica a i seguenti aspetti di un sistema:

- **Requisiti:** Questa categoria si riferisce ai requisiti di sicurezza di un prodotto
- **Politica di sicurezza:** Sulla base dei requisiti, può essere definita una politica di sicurezza
- **Progettazione del prodotto:** Sulla base dei requisiti e della politica di sicurezza
- **Implementazione del prodotto:** Basato sulla progettazione
- **Funzionamento del sistema:** Include l'uso ordinario più la manutenzione

In ogni area, si possono adottare diversi approcci per fornire garanzie.

I possibili approcci:

- Analisi e controllo dei processi e delle procedure
- Verifica dell'applicazione dei processi e delle procedure
- Analisi della corrispondenza tra le rappresentazioni del progetto TOE
- Analisi della rappresentazione del progetto TOE rispetto ai requisiti
- Verifica delle prove
- Analisi dei documenti di guida
- Analisi dei test funzionali sviluppati e dei risultati forniti
- Test funzionali indipendenti
- Analisi delle vulnerabilità (inclusa l'ipotesi di difetti)
- Penetration Testing

Siccome viene fornita una visione un po' diversa degli elementi di garanzia. Questa relazione è basata sull'esperienza con le valutazioni di Orange Book, ma è rilevante per gli attuali sforzi di sviluppo di prodotti affidabili. L'autore vede la garanzia come comprendente i seguenti requisiti:

- **Architettura del sistema**

  Riguarda sia la fase di sviluppo del sistema che la fase operativa del sistema. Esempi di tecniche per aumentare il livello di garanzia durante la fase di sviluppo includono la progettazione modulare del software, la stratificazione e l'astrazione dei dati/nascondere le informazioni.

- **Integritò del sistema**

  Riguarda il corretto funzionamento dell'hardware e del firmware ed è tipicamente soddisfatto dall'uso periodico di software diagnostico.

- **Test del sistema**

  Assicura che le caratteristiche di sicurezza siano state testate a fondo. Questo include il test delle operazioni funzionali, il test dei requisiti di sicurezza, e test di possibili penetrazioni.

- **Specifica e verifica del design**

  Affronta la correttezza del design e dell'implementazione del sistema progettazione e implementazione del sistema rispetto alla politica di sicurezza del sistema. Idealmente, possono essere usati metodi formali di verifica.

- **Gestione fidata della struttura**

  Si occupa dell'amministrazione del sistema. Un approccio è quello di separare i ruoli di operatore del sistema e di amministratore della sicurezza. Un altro approccio è la specificazione dettagliata di politiche e procedure con meccanismi per la revisione.

- **Recupero affidabile**

  Fornisce il corretto funzionamento delle funzioni di sicurezza dopo che un sistema si riprende da guasti, crash o incidenti di sicurezza.

- **Distribuzione fidata**

  Assicura che hardware, firmware e software protetti non subiscano modifiche non autorizzate durante il transito dal fornitore al cliente

- **Gestione della configurazione**

  I requisiti sono inclusi per la configurazione controllo, audit, gestione e contabilità

Così, vediamo che la garanzia si occupa della progettazione, dell'implementazione e del funzionamento delle risorse protette e delle loro funzioni e procedure di sicurezza. È importante notare che la garanzia è un processo, non un risultato. Cioè, la garanzia deve essere un'attività attività continua, che include test, verifiche e revisioni.

1.19.3 Processo di valutazione

Lo scopo della valutazione di un prodotto IT, un TOE, rispetto a uno standard informatico affidabile è quello di garantire che le caratteristiche di sicurezza nel TOE funzionino correttamente ed efficacemente, e non mostrino vulnerabilità sfruttabili. Il processo di valutazione viene eseguito sia in parallelamente o dopo lo sviluppo del TOE, a seconda del livello di garanzia richiesto.

Più alto è il livello, maggiore è il rigore richiesto dal processo, e più tempo e spese si dovranno sostenere.

I principali input per la valutazione sono l'obiettivo di sicurezza, un insieme di prove sul TOE e il TOE attuale. Il risultato desiderato del processo di valutazione è confermare che l'obiettivo di sicurezza è soddisfatto per il TOE, confermato da prove documentate nel rapporto di valutazione tecnica. Il processo di valutazione metterà in relazione l'obiettivo di sicurezza con uno o più dei seguenti elementi progettazione di alto livello, progettazione di basso livello, specifiche funzionali, implementazione del codice sorgente, codice oggetto e realizzazione hardware del TOE. Il grado di rigore utilizzato e la profondità dell'analisi sono determinati dal livello di garanzia desiderato per la valutazione. Ai livelli più alti, si usano modelli semiformali o formali per confermare che il TOE implementa effettivamente l'obiettivo di sicurezza desiderato. Il processo di valutazione comporta anche Il processo di valutazione implica anche un attento test del TOE per confermare le sue caratteristiche di sicurezza.

La valutazione coinvolge una serie di parti:

- **Sponsor:** Di solito o il cliente o il fornitore di un prodotto per il quale è richiesta la valutazione. Gli sponsor determinano l'obiettivo di sicurezza che il prodotto deve soddisfare.
- **Sviluppatore:** Deve fornire prove adeguate sui processi usati per progettare, implementare e testare il prodotto per permetterne la valutazione.
- **Valutatore:** Esegue il lavoro di valutazione tecnica, usando le prove fornite dagli sviluppatori, e ulteriori test del prodotto, per confermare che esso soddisfi i requisiti funzionali e di garanzia specificati nell'obiettivo di sicurezza.
- **Certificatore:** L'agenzia governativa che controlla il processo di valutazione e in seguito certifica che un prodotto e successivamente certifica che un prodotto è stato valutato con successo. I certificatori generalmente un registro dei prodotti valutati, che può essere consultato dai clienti.

Il processo di valutazione ha tre grandi fasi:

1. **Preparazione:** Coinvolge il contatto iniziale tra lo sponsor e gli sviluppatori di un prodotto e i valutatori che lo valuteranno. Confermerà che lo sponsor e gli sviluppatori sono adeguatamente preparati a condurre la valutazione e includerà una revisione dell'obiettivo di sicurezza e possibilmente altre consegne di valutazione.

2. **Conduzione della valutazione:** Un processo strutturato e formale in cui i valutatori conducono una serie di attività specificate dal CC. Queste includono la revisione dei prodotti forniti dallo sponsor e dagli sviluppatori, e altri test del prodotto, per confermare che soddisfa l'obiettivo di sicurezza. Durante questo processo, possono essere identificati nel prodotto, che vengono riportati agli sviluppatori per la correzione.

3. **Conclusione:** I valutatori forniscono il rapporto tecnico di valutazione finale ai certificatori per l'accettazione. I certificatori usano questo rapporto, che può contenere informazioni confidenziali, per convalidare il processo di valutazione e per preparare un rapporto di certificazione pubblico. Il rapporto di certificazione viene poi elencato nel relativo registro dei prodotti valutati.

Il processo di valutazione è normalmente monitorato e regolato da un'agenzia governativa in ogni paese.