Sistemi Operativi Modulo I

Primo canale (A-L) e Teledidattica

A.A. 2019/2020

Corso di Laurea in Informatica

La Sicurezza nei Sistemi Operativi

Igor Melatti

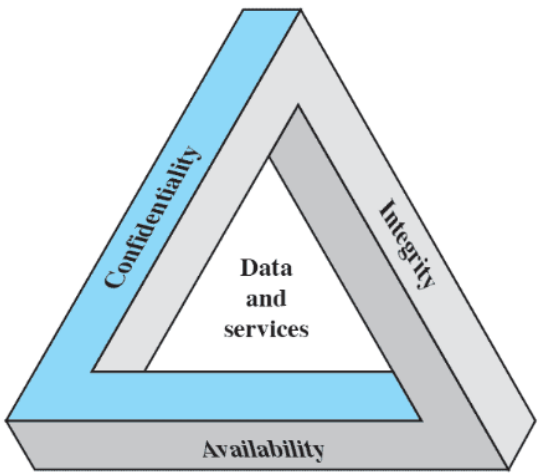
Sapienza Università di Roma
Dipartimento di Informatica

Definizione di Sicurezza

- Dal manuale sulla sicurezza informatica del NIST (National Institute of Standards and Technology):
  - La protezione offerta da un sistema informatico automatico al fine di conservare integrità, disponibilità e confidenzialità delle risorse del sistema stesso

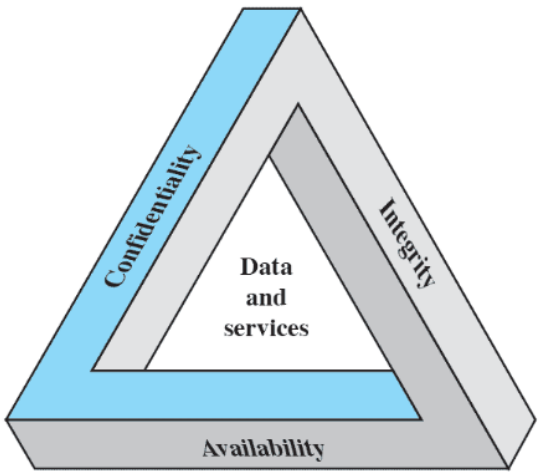
Sicurezza: la Triade

- Ci sono tre obiettivi che costituiscono il cuore della sicurezza
  - integrità
  - disponibilità
  - confidenzialità



Sicurezza: Concetti Ulteriori

- Ci sono due ulteriori obiettivi che vengono aggiunti al nucleo della sicurezza informatica
  - autenticità
  - tracciabilità (*accountability*)



Gli obiettivi nel dettaglio

- Integrità: riferita tipicamente ai dati, che non devono essere modificati senza le dovute autorizzazioni
- Confidenzialità: riferita tipicamente ai dati, che non devono essere letti senza le dovute autorizzazioni
- Disponibilità: riferita tipicamente ai servizi, che devono essere disponibili senza interruzioni
- Autenticità: riferita tipicamente agli utenti, che devono essere chi dichiarano di essere
  - per estensione, vale anche per messaggi e dati

Minacce (*Threats*)

- L'RFC 2828 descrive quattro conseguenze delle minacce informatiche
  - Accesso non autorizzato (*Unauthorized disclosure*)
  - Imbroglio (*Deception*)
  - Distruzione (*Disruption*)
  - Usurpazione (*Usurpation*)

Accesso non Autorizzato

- Un'entità ottiene l'accesso a dati per i quali non ha autorizzazione
- Minaccia alla confidenzialità
- Attacchi:
  - esposizione (intenzionale o per errore)
  - intercettazione
  - inferenza
  - intrusione

Imbroglio

- Un'entità autorizzata riceve dati falsi e pensa siano veri
- Minaccia all'integrità (del sistema o dei dati)
- Attacchi:
  - mascheramento
    - l'attaccante riesce ad entrare in possesso delle credenziali di un utente autorizzato
    - trojan
  - falsificazione
    - uno studente che modifica i suoi voti...
  - ripudio
    - un utente nega di aver ricevuto o inviato dei dati

Distruzione

- Impedimento al corretto funzionamento dei servizi
- Minaccia all'integrità del sistema o alla disponibilità
- Attacchi:
  - incapacitazione
    - rompendo un qualche componente del sistema
  - ostruzione
    - Denial of Service (DoS), per esempio riempiendo il sistema di richieste
  - corruzione
    - alterazione dei servizi

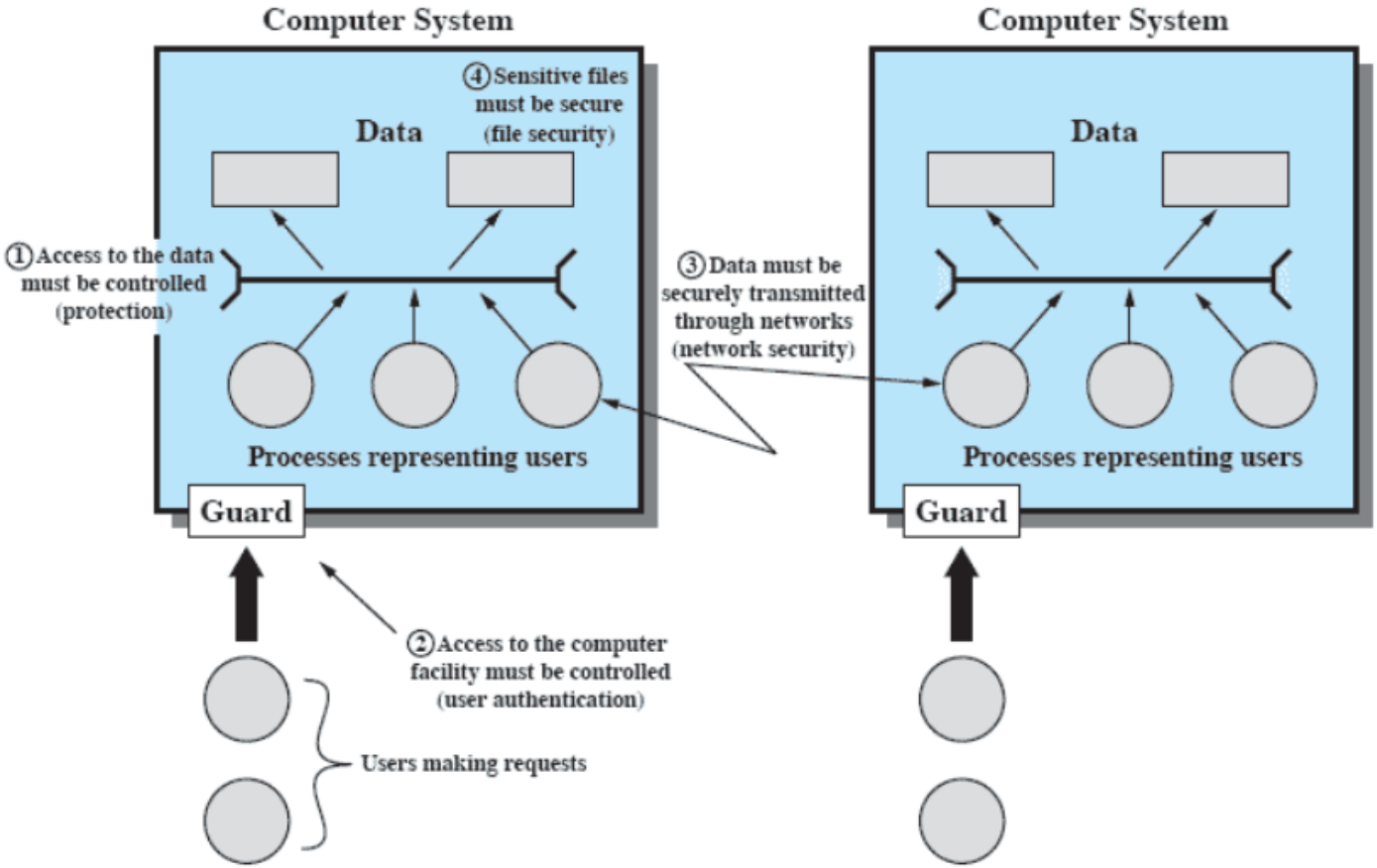
Usurpazione

- Il sistema viene direttamente controllato da chi non ne ha l'autorizzazione
- Minaccia all'integrità del sistema
- Attacchi:
  - appropriazione indebita, ovvero diventare amministratore di una macchina non propria
    - es.: le macchine che compongono le botnet per poter poi fare DoS
  - uso non appropriato
    - virus che cancella file o fa comunque danni

Asset

- Traducibile con “risorsa”
- Gli asset di un sistema computerizzato possono essere categorizzati come:
  - hardware
  - software
  - dati
  - linee di comunicazione e reti

Ambito della Sicurezza Informatica



Relazione tra Asset e la Triade

	Disponibilità	**Confidenzialità**	**Integrità**
Hardware	Workstation rubate o rese inutilizzabili		
Software	Programmi cancellati	Copia non autorizzata dei programmi	Modifica dei programmi (per non farli funzionare o per fargli fare compiti indesiderati)
Dati	File cancellati	File letti senza autorizzazione. Dati inferiti da analisi statistica	Modifica di file esistenti o creazione di file
Comunicazione	Messaggi distrutti. Linee di comunicazione rese inutilizzabili	Lettura dei messaggi o osservazione dei pattern	Modifica, ritardo, riordino o duplicazione di messaggi esistenti, creazione di messaggi falsi

Autenticazione

- Base per la maggior parte dei tipi di controllo di accesso e tracciabilità
- Due passi:
  - identificazione
  - verifica
- Determina se un utente è abilitato ad accedere al sistema
- In più, determina anche i privilegi dell'utente abilitato
- Rende possibile il *discretionary control access* (controllo di accesso discrezionale)
  - un utente può decidere a quali utenti concedere determinati permessi

Mezzi per l'Autenticazione

- Tradizionalmente divisi in tre fattori
  - almeno uno deve essere presente
  - meglio due contemporaneamente (autenticazione a 2 fattori)
- Qualcosa che *sai*
  - password
- Qualcosa che *hai*
  - chiave, badge RFID
- Qualcosa che *sei*
  - biometrica (retina...)

Un Altro Punto di Vista

- Per sottolineare le possibili problematiche, Nick Mathewson notò come i mezzi per l'autenticazione possano anche essere:
  - qualcosa che *hai dimenticato*
  - qualcosa che *avevi*
  - qualcosa che *eri*

Autenticazione con Password

- Quella più nota ed usata
- Spesso anche l'unica
- Importante che le password siano memorizzate non in chiaro

Autenticazione con Token

- Oggetti fisici posseduti da un utente per l'autenticazione vengono chiamati *token*
- Esempi:
  - memory card
  - smartcard

Memory Card

- Possono memorizzare dati, ma senza elaborarli
  - bancomat tradizionali
- Spesso usati insieme a password o PIN
  - anche senza: carte per accesso a camere d'albergo
- Svantaggi:
  - serve un lettore apposito
  - se perdo il token?
  - utenti non soddisfatti

Smartcard

- Hanno un microprocessore, memoria e porte I/O
- Ne esistono di diversi tipi, a seconda dei seguenti aspetti:
  - caratteristiche fisiche
    - come una carta di credito, o come una chiavetta USB
  - interfaccia
    - lettore apposito, ma alcune hanno un tastierino
  - protocollo di autenticazione:
    - generatore di password statico o dinamico
    - domanda - risposta

Biometrica, Ultimi Sviluppi

- Recentemente, la biometrica è stata espansa come segue:
- Qualcosa che *sei*
  - biometrica *statica*: impronta digitale, faccia
- Qualcosa che *fai*
  - biometrica *dinamica*: scrittura a mano, riconoscimento vocale, ritmo di battitura

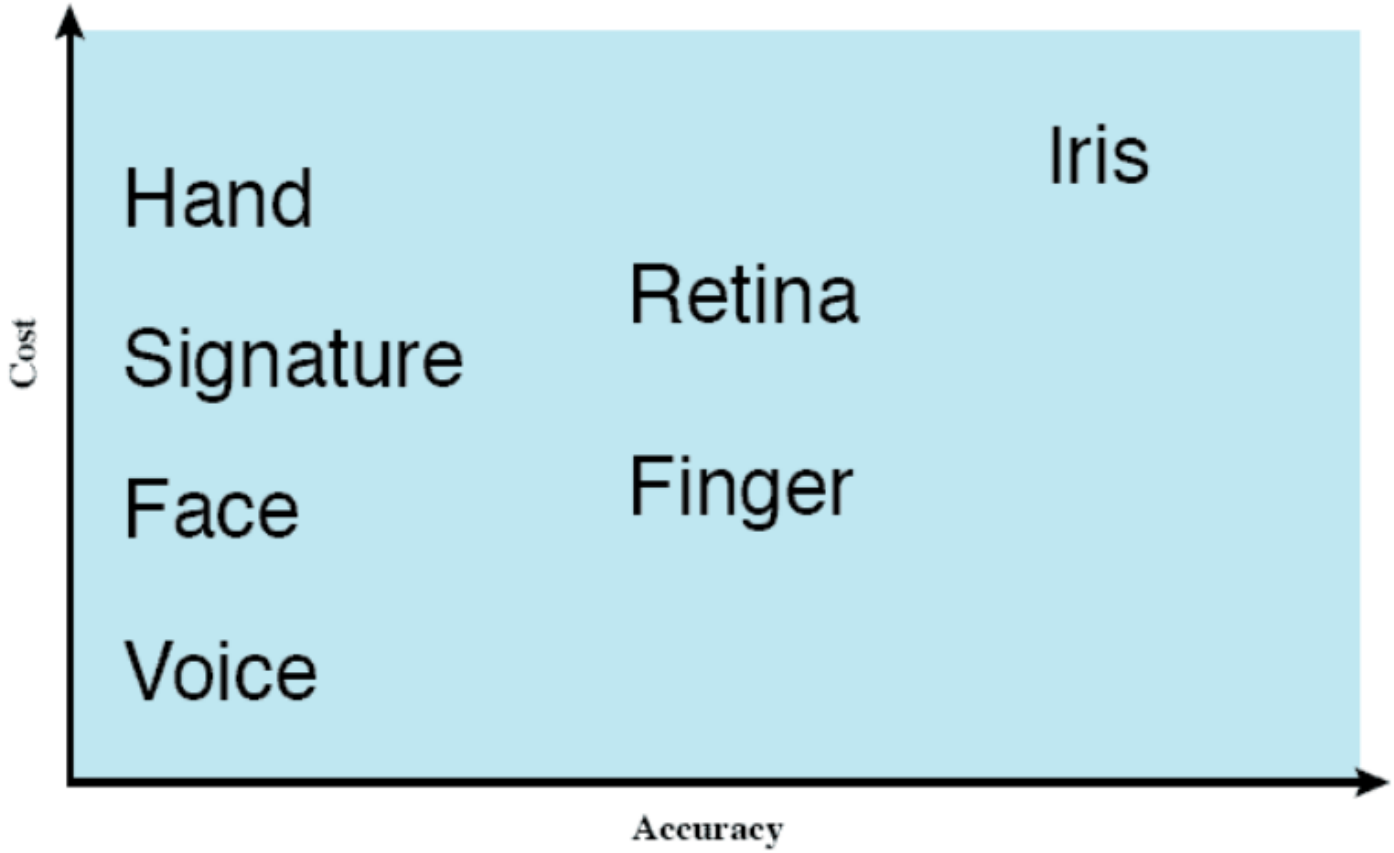
Autenticazione Biometria Statica

- Include:
  - caratteristiche facciali
  - impronte digitali
  - geometria della mano
  - retina
  - iride
- Basata su riconoscimento di pattern
  - complesso e costoso

Autenticazione Biometria Dinamica

- I pattern possono cambiare
- Include:
  - firma
  - voce
  - ritmo di battitura

Costo vs. Accuratezza



Controllo di Accesso

- Determina quali tipi di accesso sono ammessi, sotto quali circostanze, e da chi
- Può essere:
  - discrezionale
  - obbligatorio
  - basato su ruoli
- Discrezionale: un utente può concedere i suoi stessi privilegi ad altri utenti
- Obbligatorio: un utente non può concedere i suoi stessi privilegi ad altri utenti
  - ambienti militari, non trattato qui

Controllo di Accesso

- Le 3 modalità possono essere presenti contemporaneamente, ovviamente applicate a diverse classi di risorse

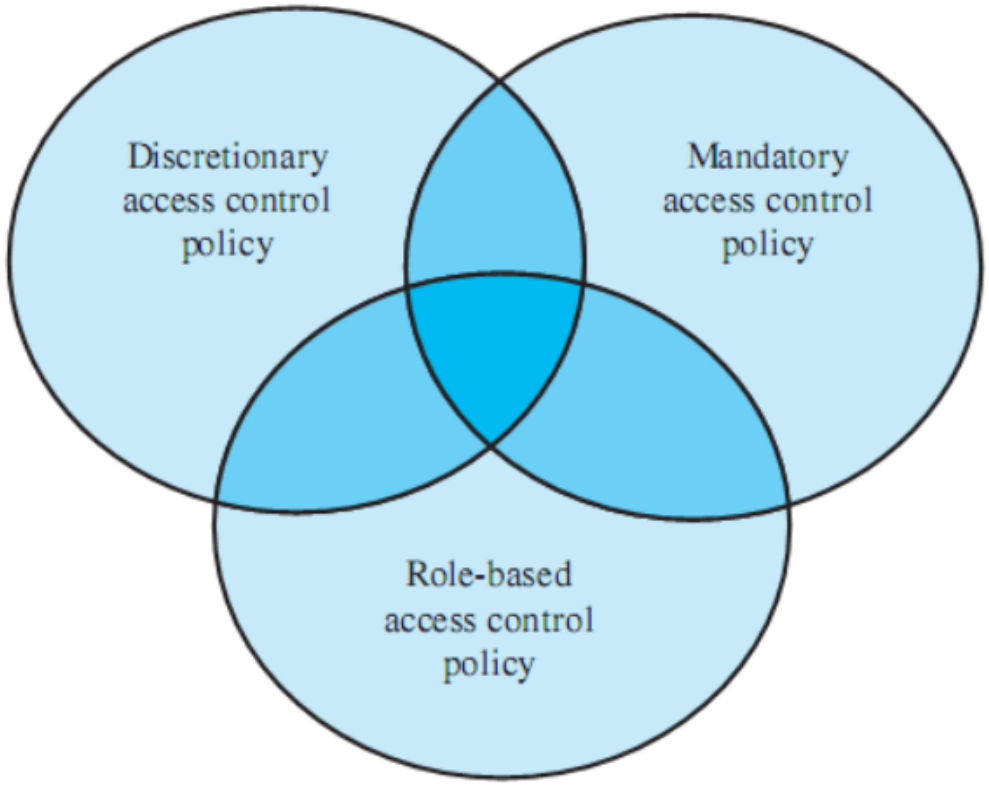


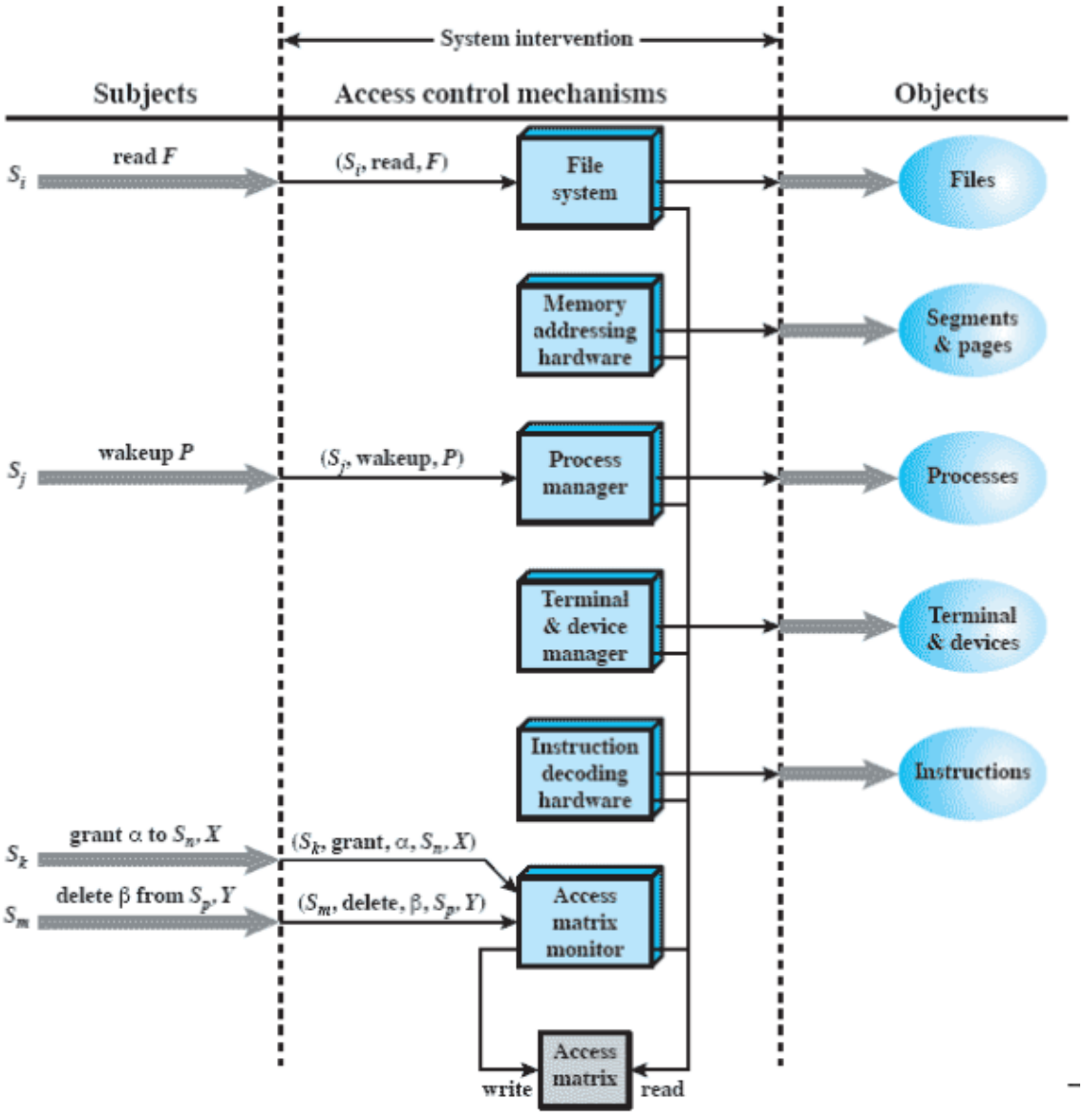
Figure 15.3 Access Control Policies

Controllo di Accesso (Discrezionale)

		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

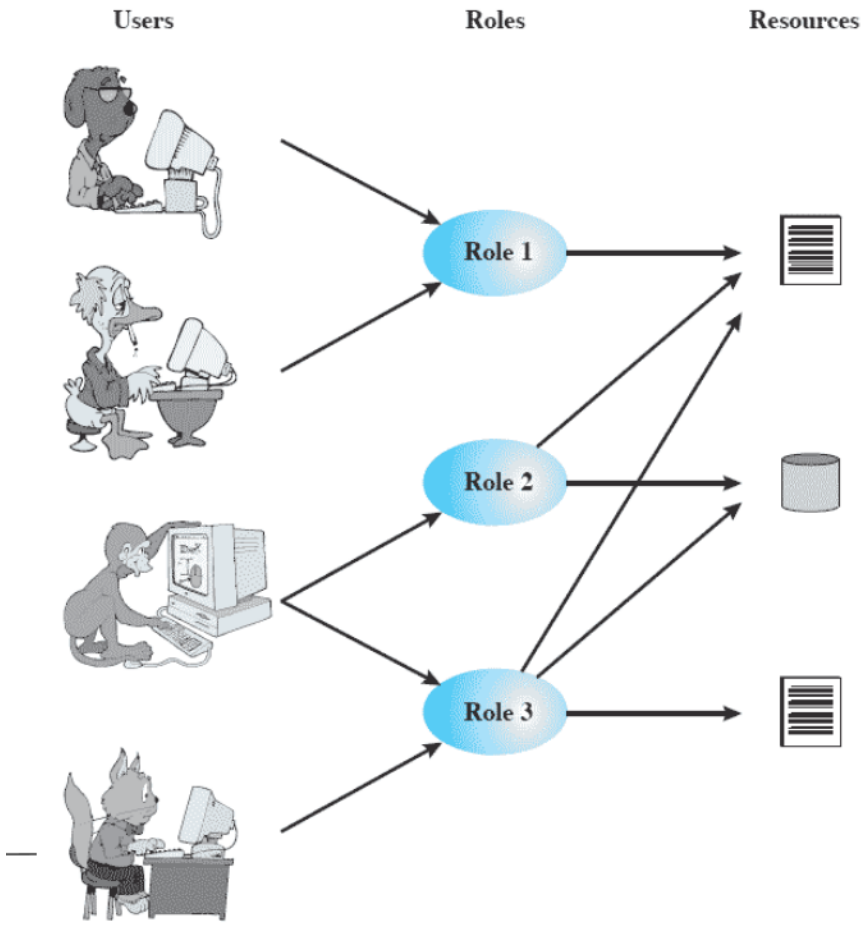
Organizzazione del Controllo di Accesso



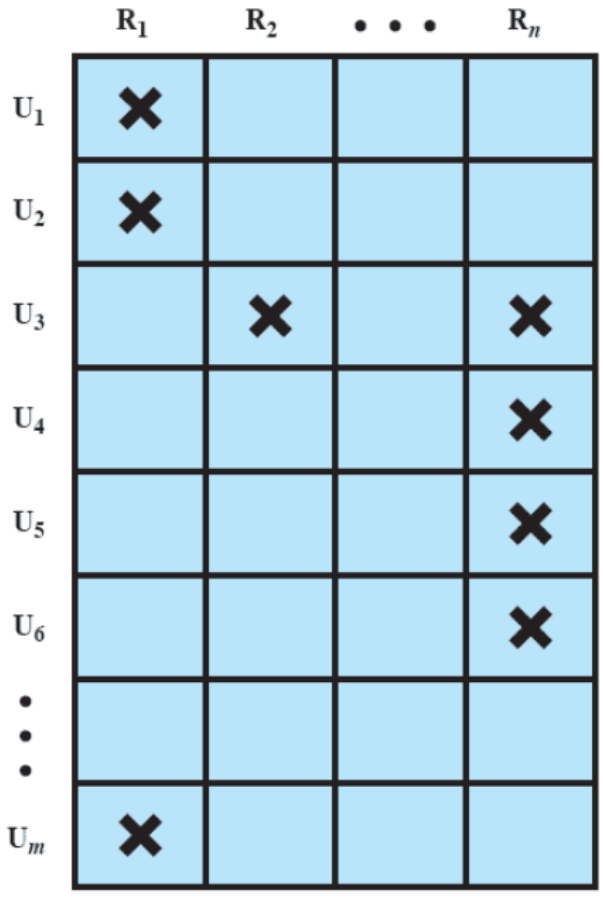
Controllo di Accesso Basato su Ruoli

- Implementazione del principio di minimo privilegio
- Ciascun ruolo deve contenere il minimo insieme di diritti d'accesso per il ruolo stesso
- Un utente viene assegnato ad un ruolo, che lo abilita ad effettuare le operazioni richieste per quel ruolo
  - ma solo mentre si sta agendo sotto quel ruolo

Ruoli



Matrice del Controllo di Accesso: Rappresentazione RBAC



Matrice del Controllo di Accesso: Rappresentazione RBAC

ROLES	OBJECTS								
	R_1	R_2	R_n	F_1	F_1	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			

UNIX: Meccanismi di Protezione

- Autenticazione dell'utente (*User-Oriented Access Control*)
- Diritti o permessi di accesso ai dati (*Data-Oriented Access Control*)
- Ci possono essere altri meccanismi
  - NIS
  - LDAP
  - Kerberos

Utenze e Gruppi

- Per ogni utente c'è uno *username* (alfanumerico) e un *uid* (numerico intero)
- Lo uid è usato ogni volta che occorre dare un proprietario ad una risorsa (file, processi, ...)
- Ogni utente appartiene ad un gruppo, analogamente identificato da *groupname* e *gid*
- File di sistema: `/etc/group` e `/etc/passwd` (talvolta in combinazione con `/etc/shadow`)
  - `/etc/passwd`: `sabinar:x:6335:283:Sabina Rossi:/home/sabinar:/bin/csh`
  - `/etc/group`: `aan:x:283:`

Login

- Può essere fatto su un terminale della macchina (processo `getty`) o tramite rete (`telnet`, `ssh`)
- Richiede una coppia username+password
- Se corrisponde ad una entry di `/etc/passwd`, viene eseguita la shell ivi indicata, a partire dalla directory di home ivi indicata
- Quando la shell esegue `exit`, o si ritorna al `getty` o si chiude la connessione di rete
- All'interno di una shell si può cambiare identità con il comando `su`

Accesso ai File

- Per ogni file ci sono tre terne di permessi: lettura, scrittura, esecuzione
- La prima terna è per il proprietario del file, la seconda per il gruppo cui il proprietario del file appartiene, la terza per tutti gli altri utenti
- Il proprietario è lo stesso del processo che ha creato il file, ma si può cambiare con `chown`
- I diritti si possono cambiare con `chmod`

```
-rwxr-xr-x 1 federico em 5120 Nov 7 11:03 a.out
-rw-r--r-- 1 federico em 233 Nov 7 11:03 test.c
```

SETUID e STGID

- Le terne di diritti sono usate ogni volta che un processo richiede l'accesso ad un file
- Se proprietario del file e del processo coincidono, si guarda la prima terna, altrimenti la seconda terna se almeno appartengono allo stesso gruppo, altrimenti la terza terna
- Si prende poi l'elemento della terna corrispondente all'accesso richiesto
- Come si fa con comandi come `passwd`??

```
-rwxr-xr-x 1 federico em 5120 Nov 7 11:03 a.out
-rw-r--r-- 1 root root 1715 Oct 12 2014 /etc/passwd
-r-sr-sr-x 1 root sys 21964 Apr 7 2002 /bin/passwd
```

SETUID e STGID

- Comandi come `passwd` hanno il permesso speciale SETUID e/o SETGID
- Tale permesso può essere accordato solo da un utente amministratore con `chmod u+s nomefile` e/o `chmod g+s nomefile`
- Vuol dire che l'uid o il gid del processo non sono quelli dell'utente che lo ha lanciato, ma del proprietario del file eseguibile
- Meccanismo da usare con estrema cautela, facile fare attacchi rootkit

```
-rw-r--r-- 1 root root 1715 Oct 12 2014 /etc/passwd
-r-sr-sr-x 1 root sys 21964 Apr 7 2002 /bin/passwd
```