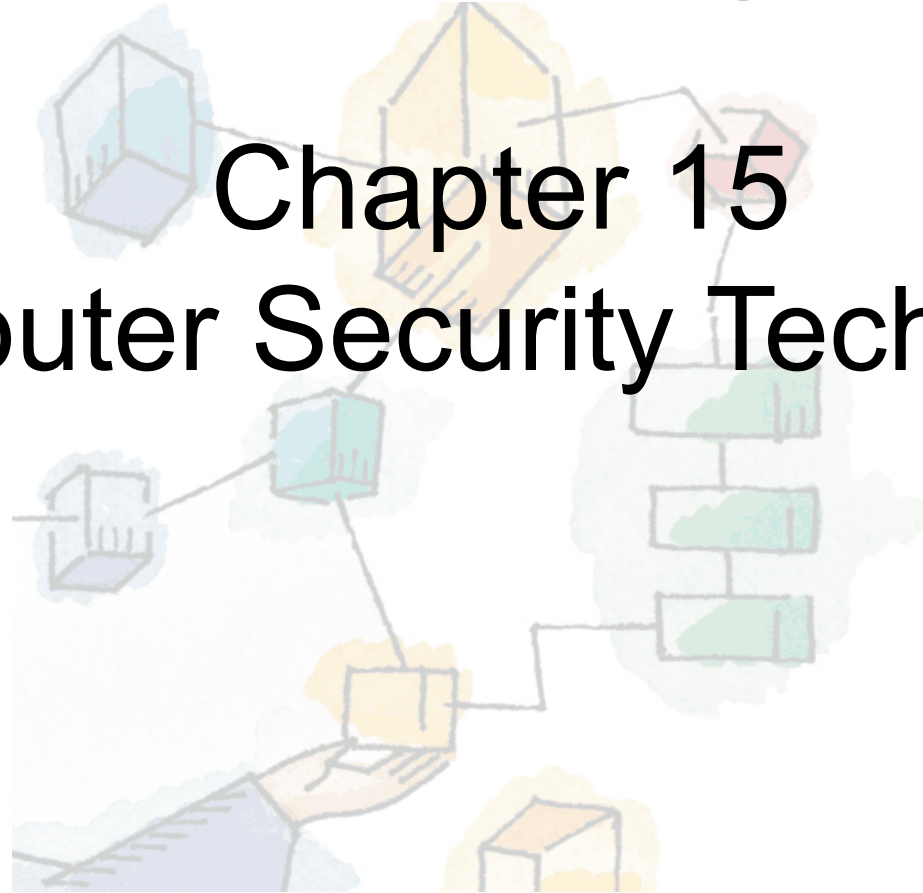
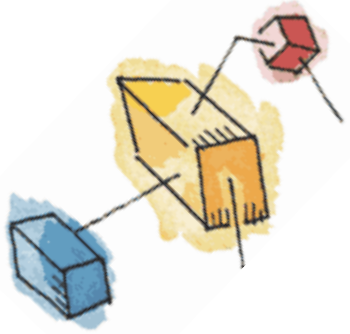


*Operating Systems:  
Internals and Design Principles, 6/E*  
William Stallings

**Chapter 15**  
**Computer Security Techniques**

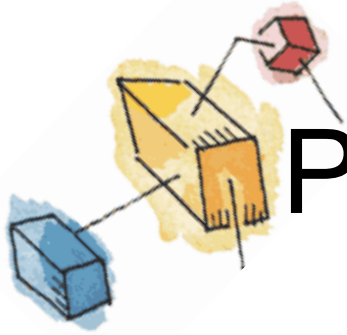




# Authentication

- Basis for most type of access control and accountability
- Identification step
- Verification step

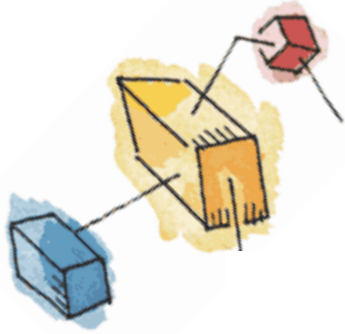




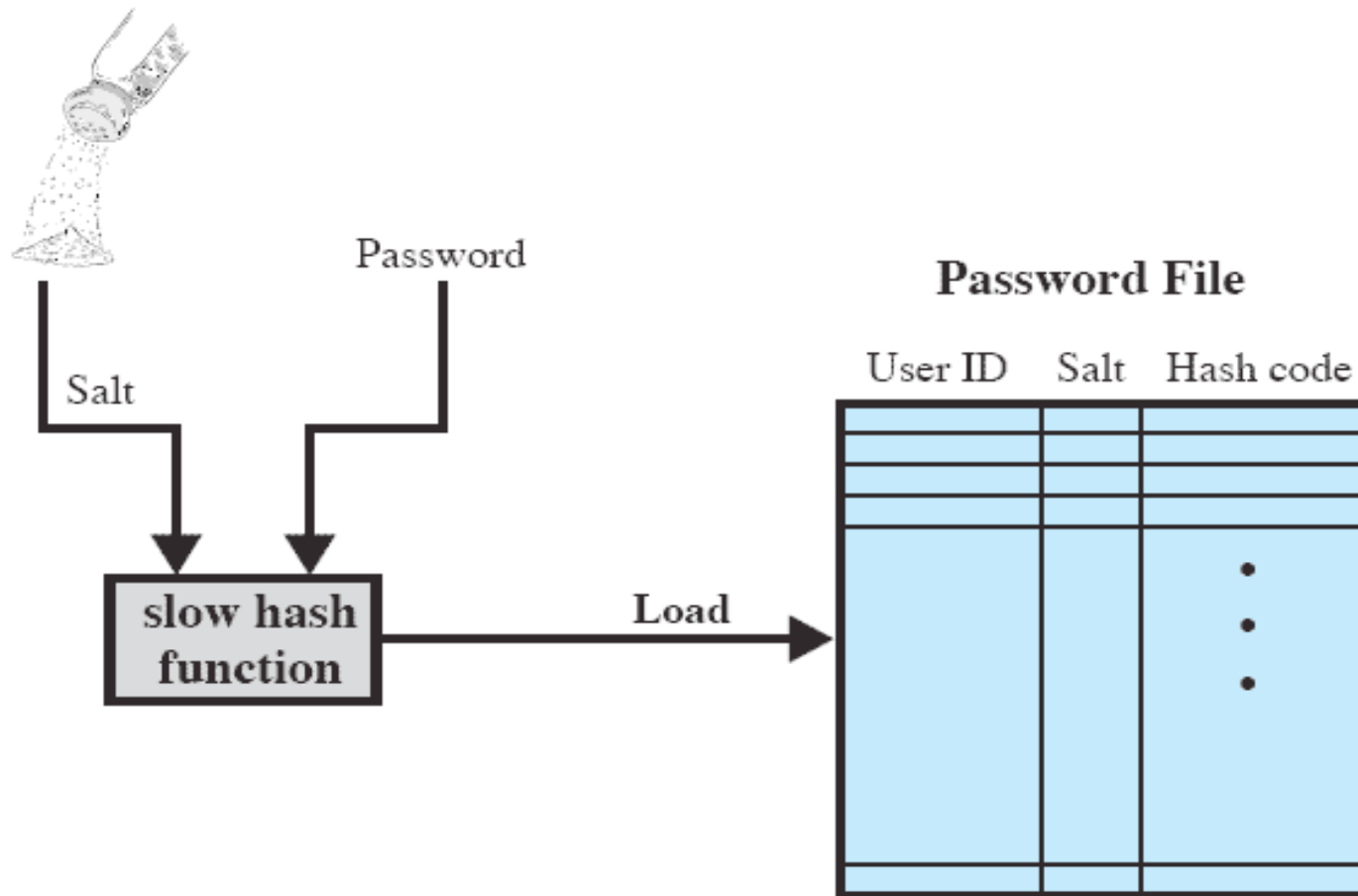
# Password-Based Authentication

- ID
  - Determines if user authorized to access system
  - Determines privileges for user
  - Discretionary access control



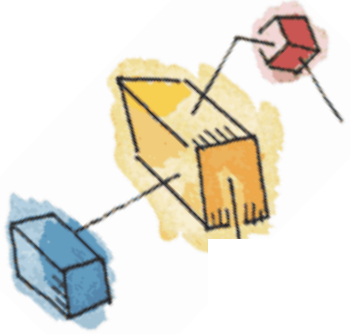


# UNIX Password Scheme

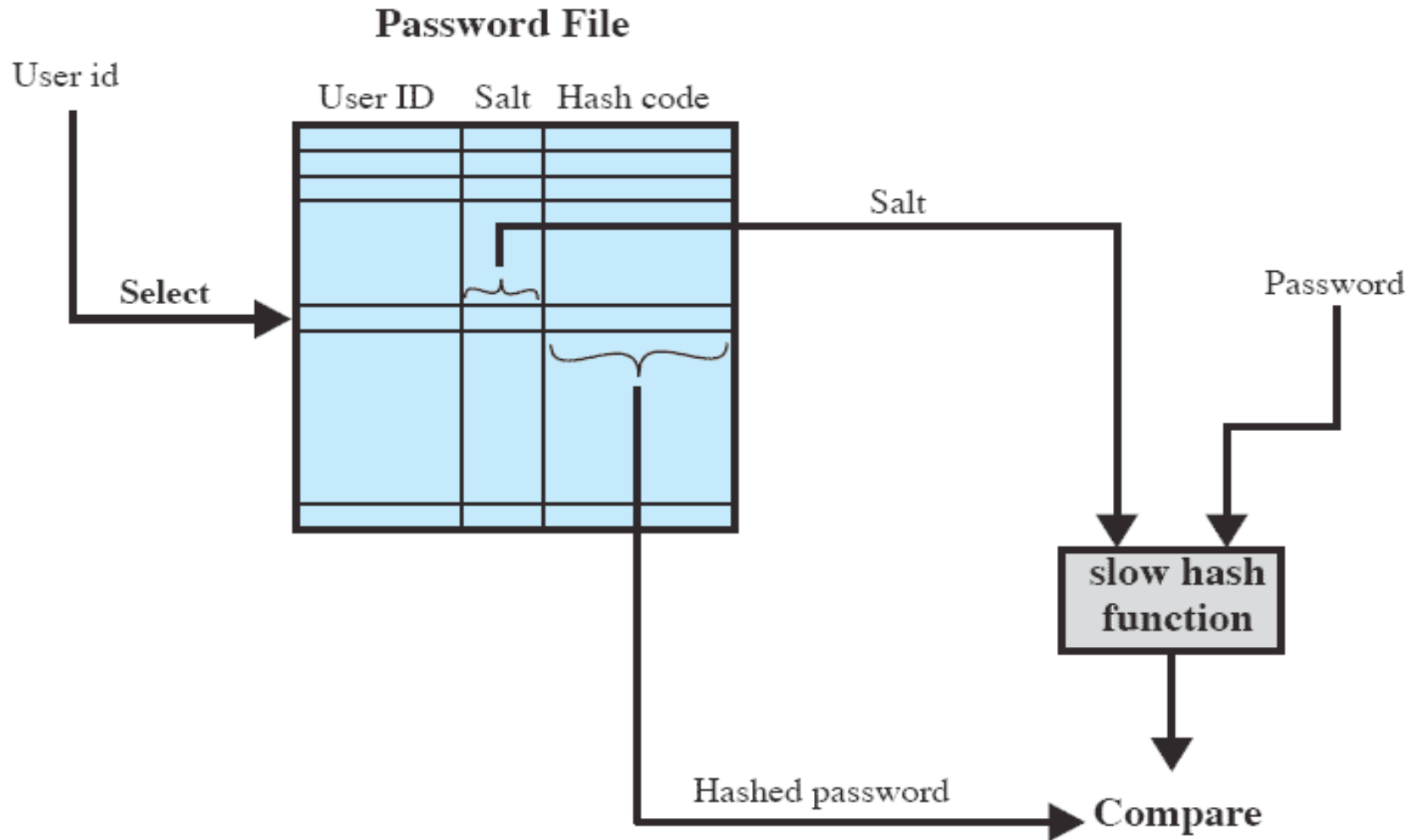


(a) Loading a new password



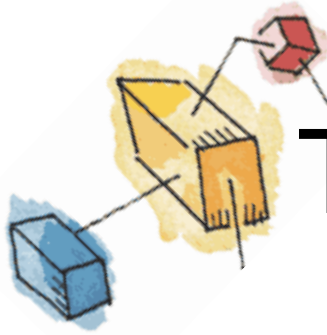


# UNIX Password Scheme



(b) Verifying a password

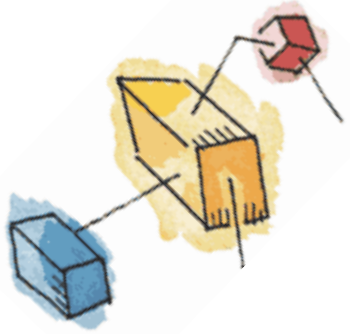




# Token-Based Authentication

- User posses object
- Memory cards
- Smart cards

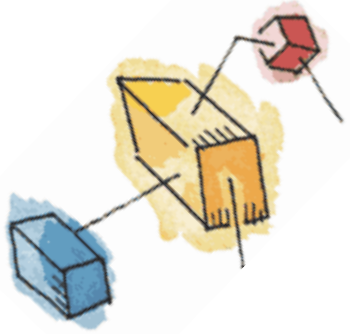




# Biometric Authentication

- Facial characteristics
- Fingerprints
- Hand geometry
- Retinal pattern

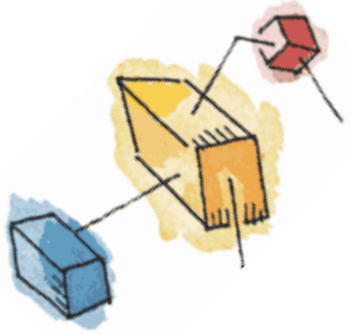




# Biometric Authentication

- Iris
- Signature
- Voice





# Cost versus Accuracy

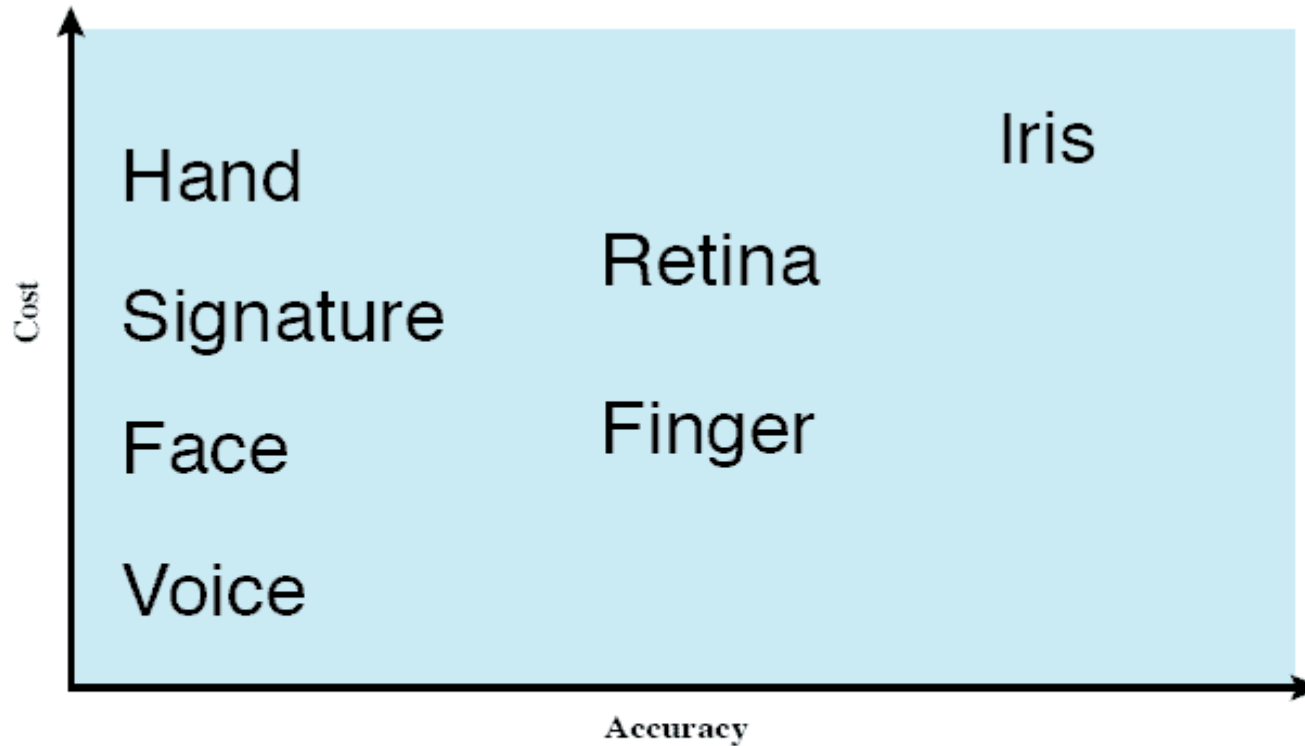
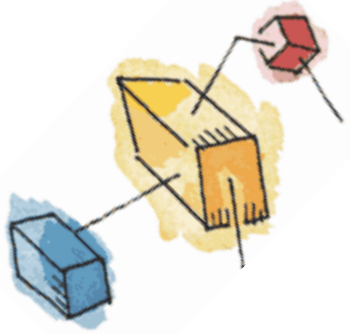


Figure 15.2 Cost Versus Accuracy of Various Biometric Characteristics in User Authentication Schemes.

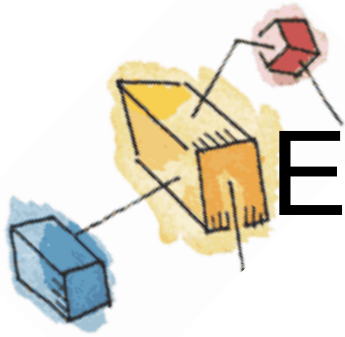




# Access Control

- Discretionary access control
  - Based on identity of requestor
- Mandatory access control
  - Based on comparing security labels with security clearances
- Role-based access control
  - Based on roles user has in system





# Extended Access Control Matrix

		OBJECTS								
		subjects			files		processes		disk drives	
		S <sub>1</sub>	S <sub>2</sub>	S <sub>3</sub>	F <sub>1</sub>	F <sub>2</sub>	P <sub>1</sub>	P <sub>2</sub>	D <sub>1</sub>	D <sub>2</sub>
SUBJECTS	S <sub>1</sub>	control	owner	owner control	read *	read owner	wakeup	wakeup	seek	owner
	S <sub>2</sub>		control		write *	execute			owner	seek *
	S <sub>3</sub>			control		write	stop			

\* - copy flag set

Figure 15.4 Extended Access Control Matrix





# Organization of the Access Control Function

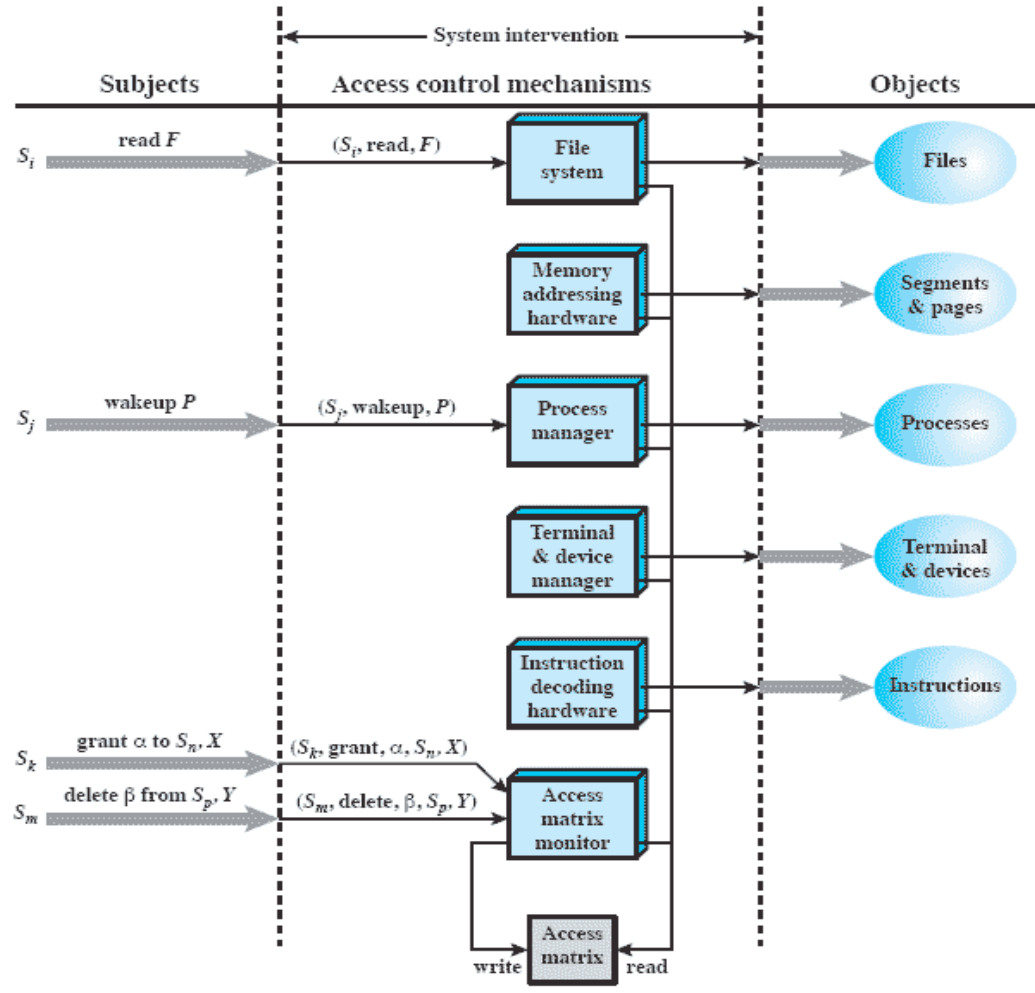


Figure 15.5 An Organization of the Access Control Function



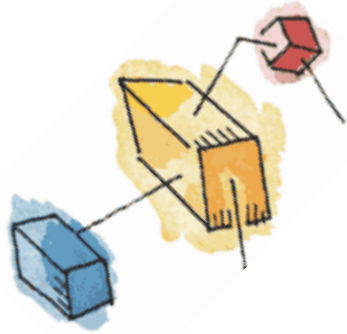
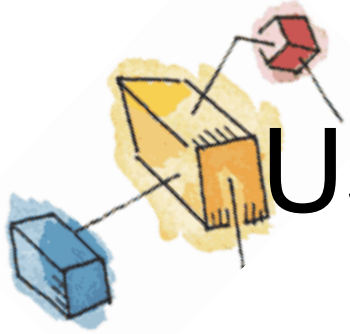


Table 15.1 Access Control System Commands

Rule	Command (by $S_0$ )	Authorization	Operation
R1	transfer $\begin{Bmatrix} \alpha^* \\ \alpha \end{Bmatrix}$ to $S, X$	' $\alpha^*$ ' in $A[S_0, X]$	store $\begin{Bmatrix} \alpha^* \\ \alpha \end{Bmatrix}$ in $A[S, X]$
R2	grant $\begin{Bmatrix} \alpha^* \\ \alpha \end{Bmatrix}$ to $S, X$	'owner' in $A[S_0, X]$	store $\begin{Bmatrix} \alpha^* \\ \alpha \end{Bmatrix}$ in $A[S, X]$
R3	delete $\alpha$ from $S, X$	'control' in $A[S_0, S]$ or 'owner' in $A[S_0, X]$	delete $\alpha$ 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 <b>create object</b> $S$ ; store 'control' in $A[S, S]$
R8	destroy subject $S$	'owner' in $A[S_0, S]$	delete row for $S$ from $A$ ; execute <b>destroy object</b> $S$



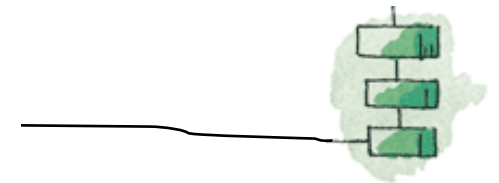
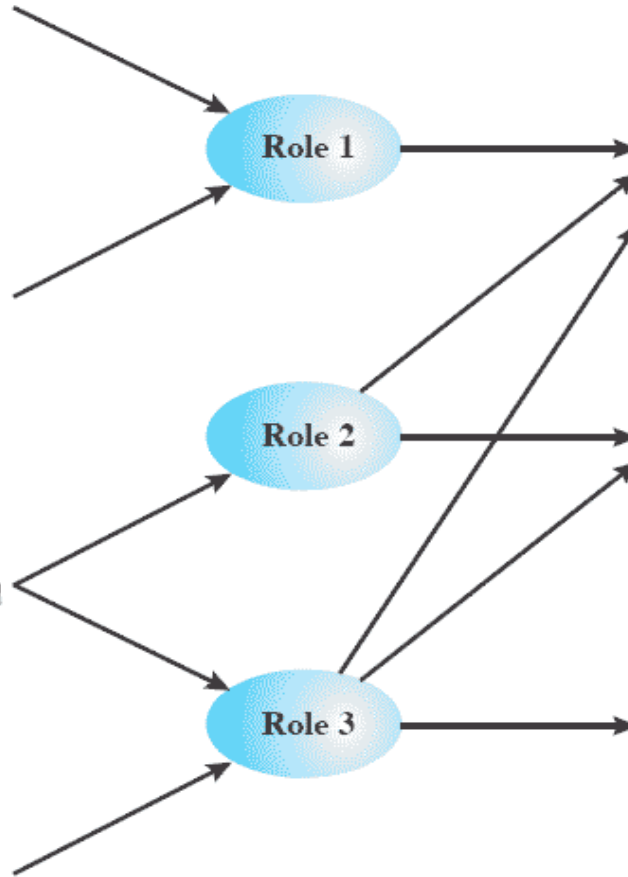


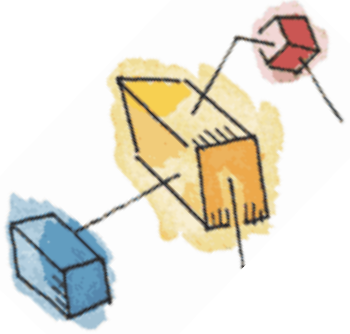
# Users, Roles, and Resources

Users

Roles

Resources

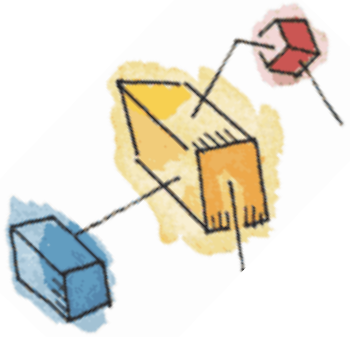




# Access Control Matrix Representation of RBAC

	$R_1$	$R_2$	$\dots$	$R_n$
$U_1$	×			
$U_2$	×			
$U_3$		×		×
$U_4$				×
$U_5$				×
$U_6$				×
$\vdots$				
$U_m$	×			

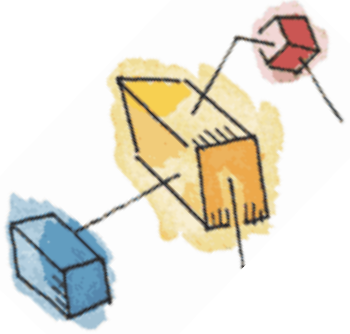




# Access Control Matrix Representation of RBAC

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

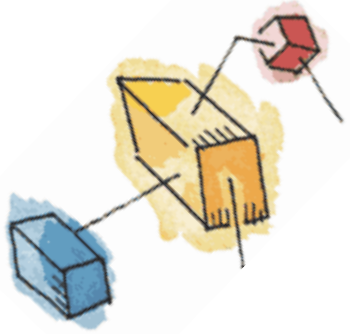




# Intrusion Detection

- Host-based
- Network-based

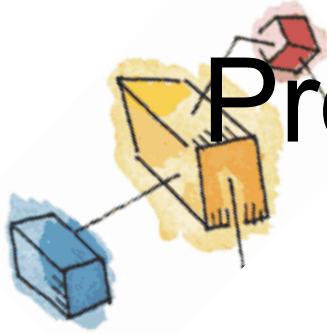




# Intrusion Detection

- Sensors
  - Collect data
- Analyzers
- User interface





# Profiles of Behavior of Intruders and Authorized Users

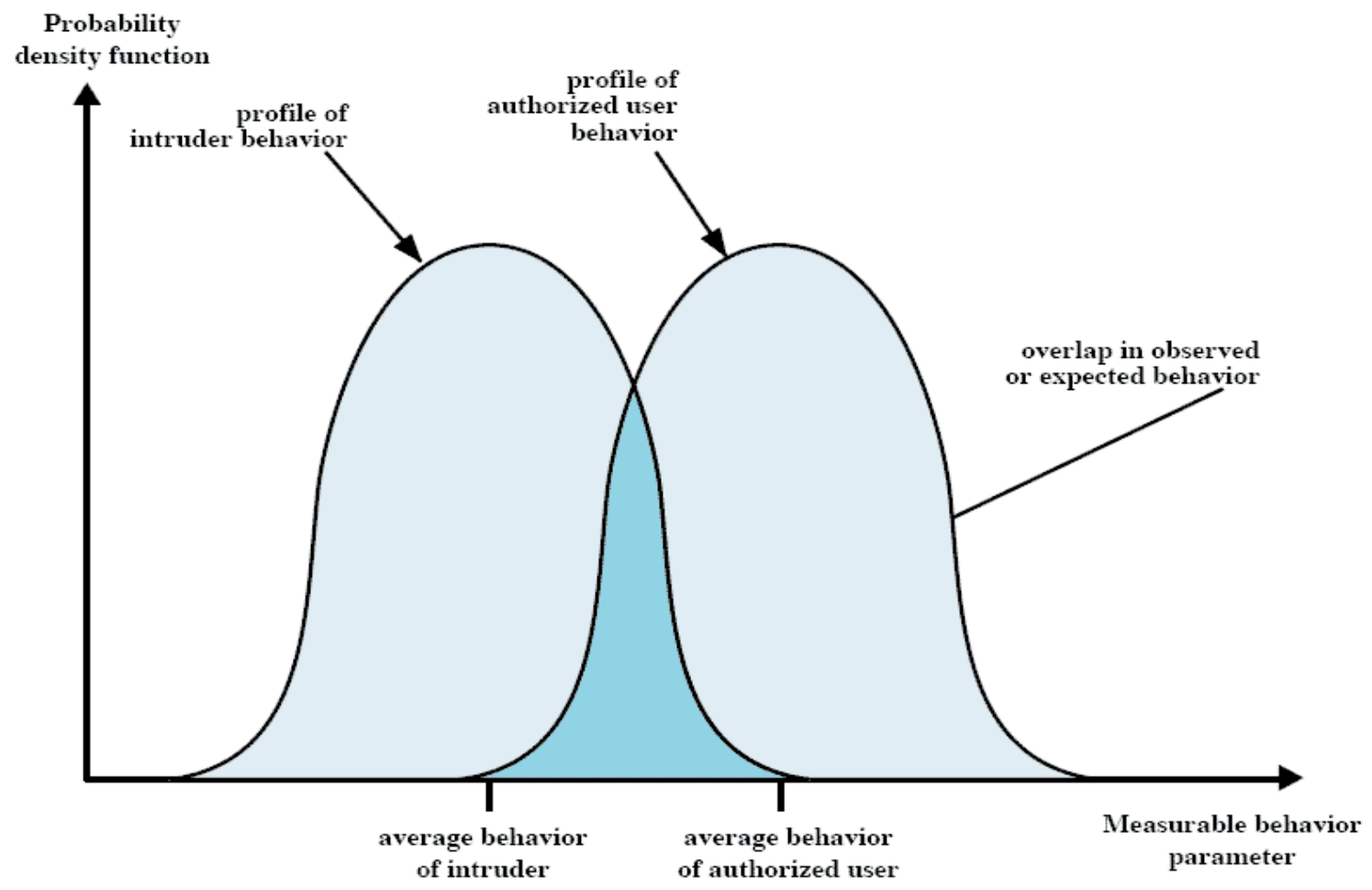
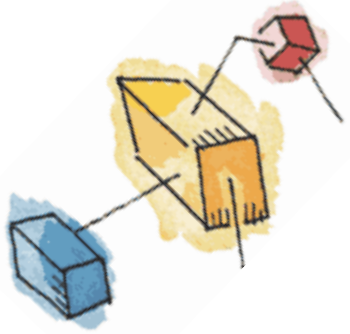


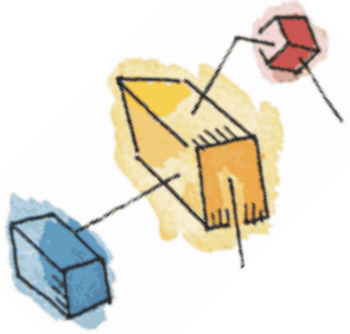
Figure 15.8 Profiles of Behavior of Intruders and Authorized Users



# Host-Based IDSs

- Anomaly detection
  - Collection of data relating to behavior of legitimated users over time
- Signature detection
  - Define set of rules or attack patterns

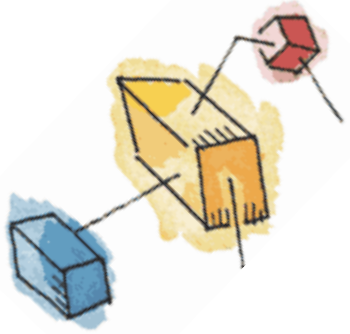




# Audit Records

- Native audit records
  - Operating system accounting software
- Detection-specific audit records
  - Generate audit records required by the IDS

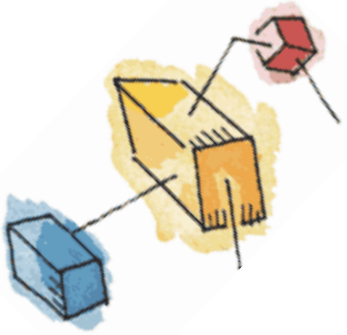




# Antivirus Approaches

- Detection
- Identification
- Removal





# Generic Decryption

- CPU emulator
- Virus signature scanner
- Emulation control module





# Digital Immune System

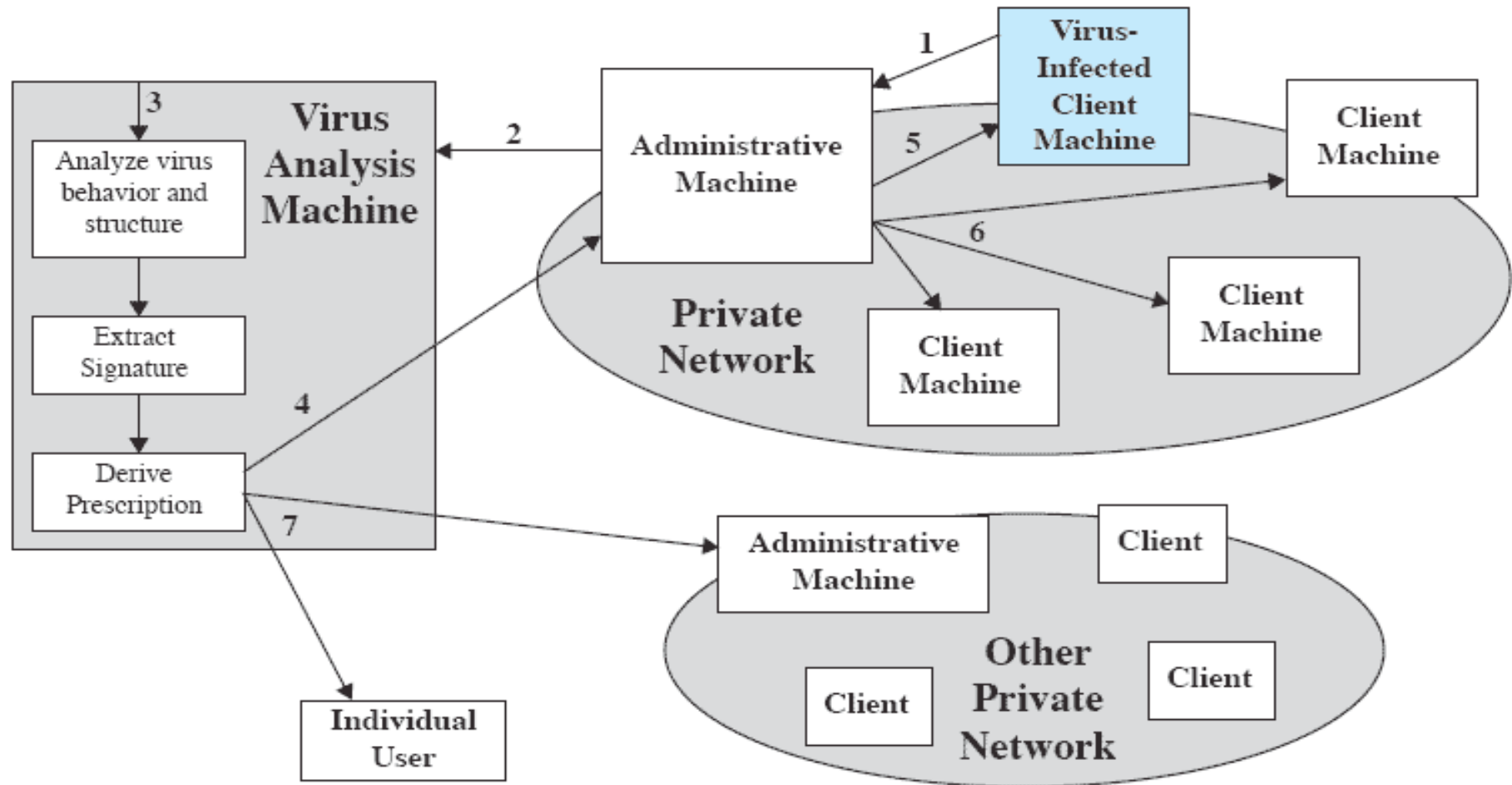


Figure 15.9 Digital Immune System



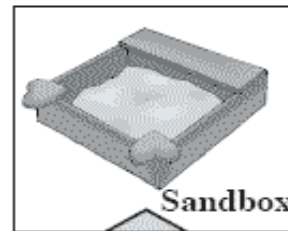


# Behavior-Blocking Software Operation

1. Administrator sets acceptable software behavior policies and uploads them to a server. Policies can also be uploaded to desktops.

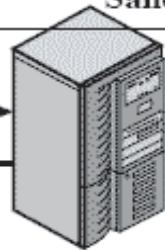


Administrator



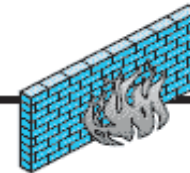
Sandbox

3. Behavior-blocking software at server flags suspicious code. The blocker "sandboxes" the suspicious software to prevent it from proceeding



Server running behavior-blocking software

2. Malicious software manages to make it through the firewall.



Firewall

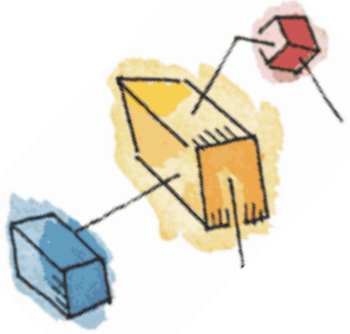


Internet

4. Server alerts administrator that suspicious code has been identified and sandboxed, awaiting administrator's decision on whether the code should be removed or allowed to run.

Figure 15.10 Behavior-Blocking Software Operation

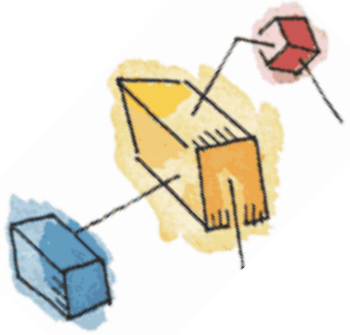




# Worm Countermeasures

- Signature-based worm scan filters
- Filter-based worm containment
- Payload-classification-based worm containment

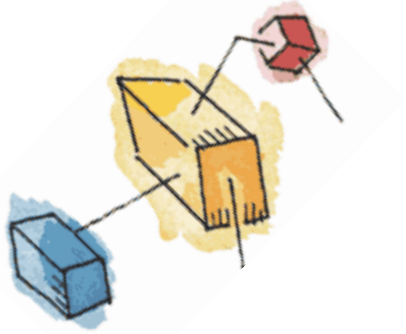




# Worm Countermeasures

- Threshold random walk scan detection
- Rate limiting
- Rate halting

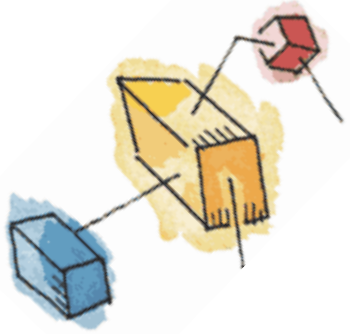




# Buffer Overflow

- Compile-time defenses
- Stack protection mechanisms

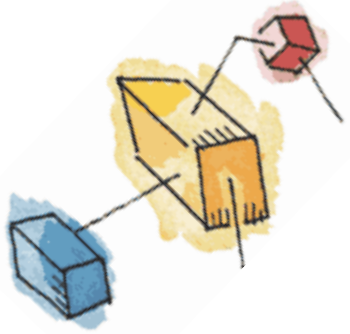




# Buffer Overflow

- Run-time defenses
- Executable address space protection
- Address space randomization
- Guard pages





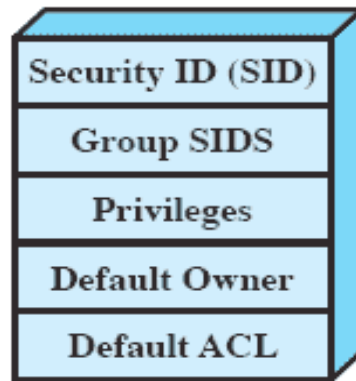
# Windows Vista Security

- Access control scheme
  - Access token
  - Indicates privileges

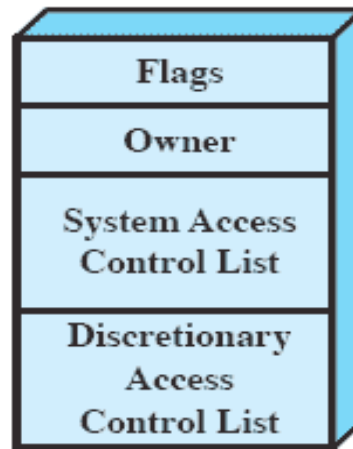




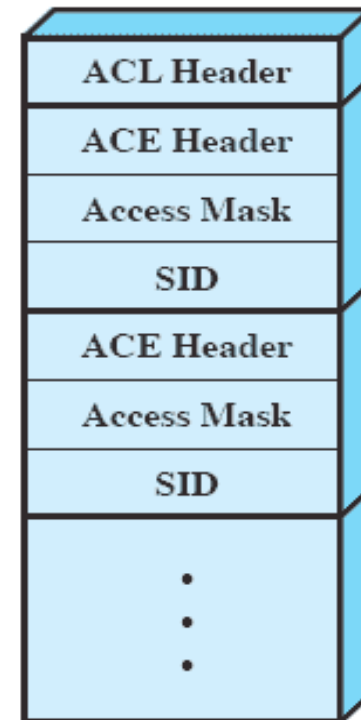
# Windows Security Structures



(a) Access token



(b) Security descriptor



(c) Access control list

Figure 15.11 Windows Security Structures



# Access Mask

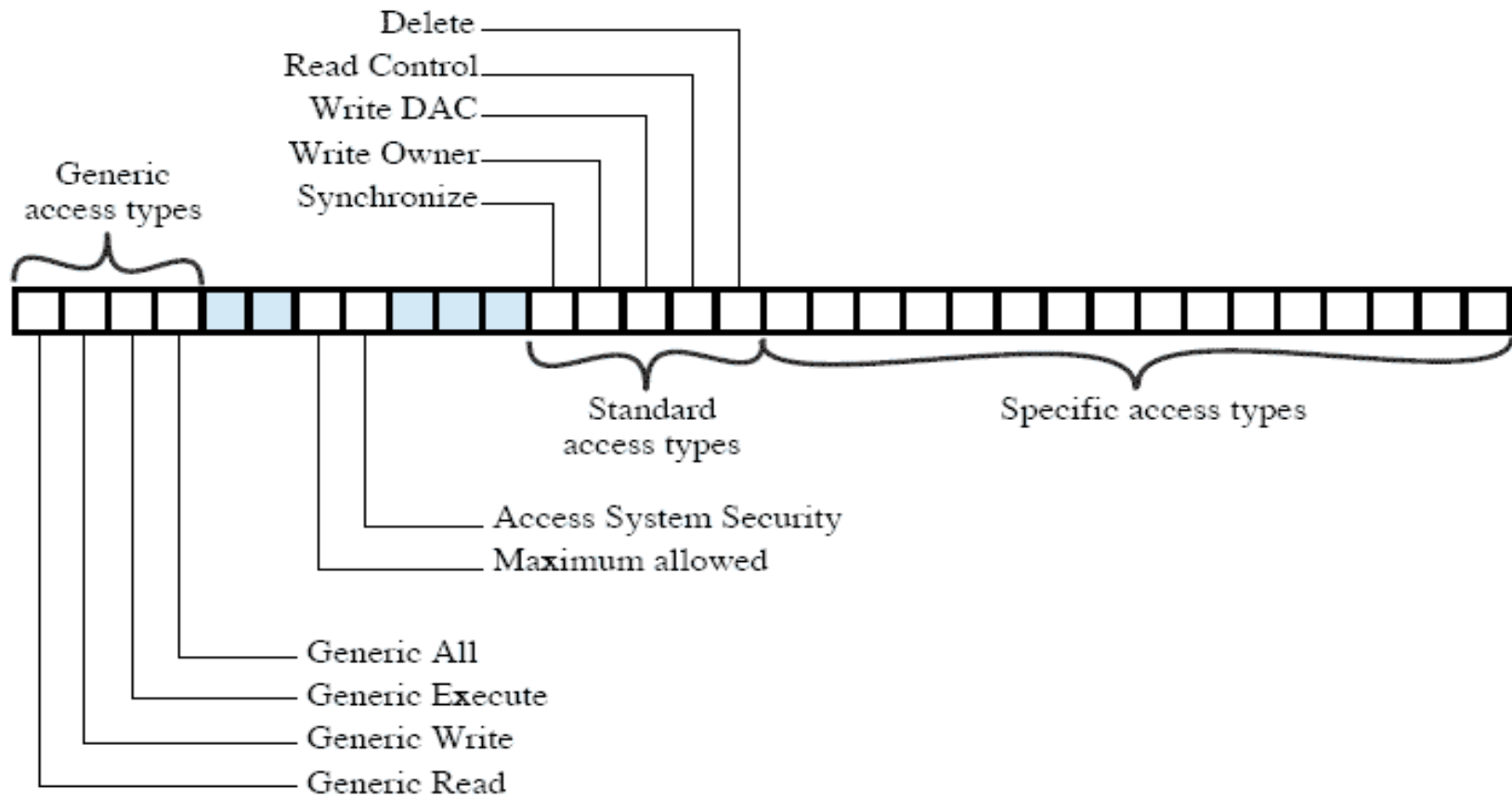


Figure 15.12 Access Mask