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

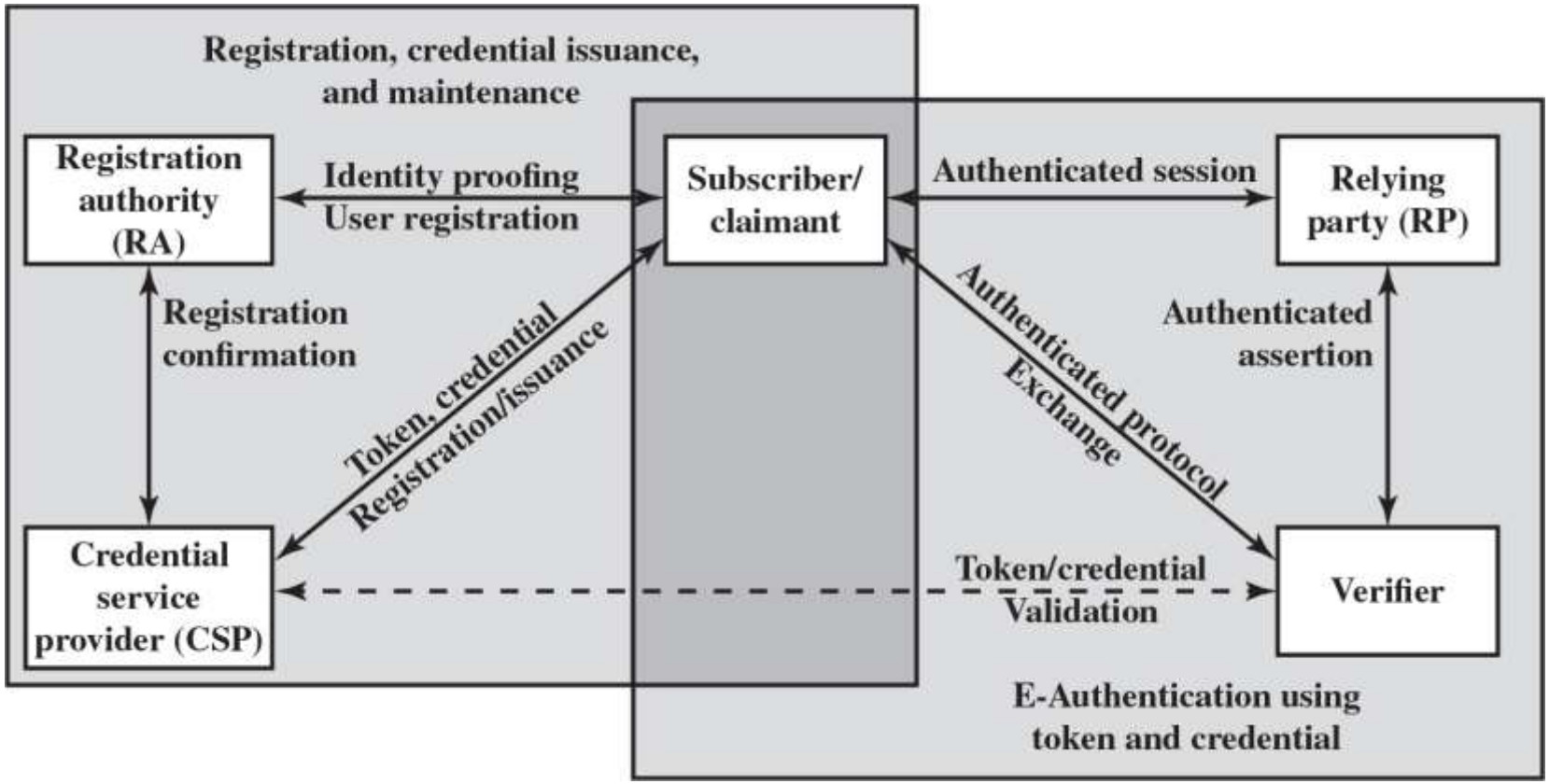


Figure 3.4 The Percentage of Passwords Guessed After a Given Number of Guesses

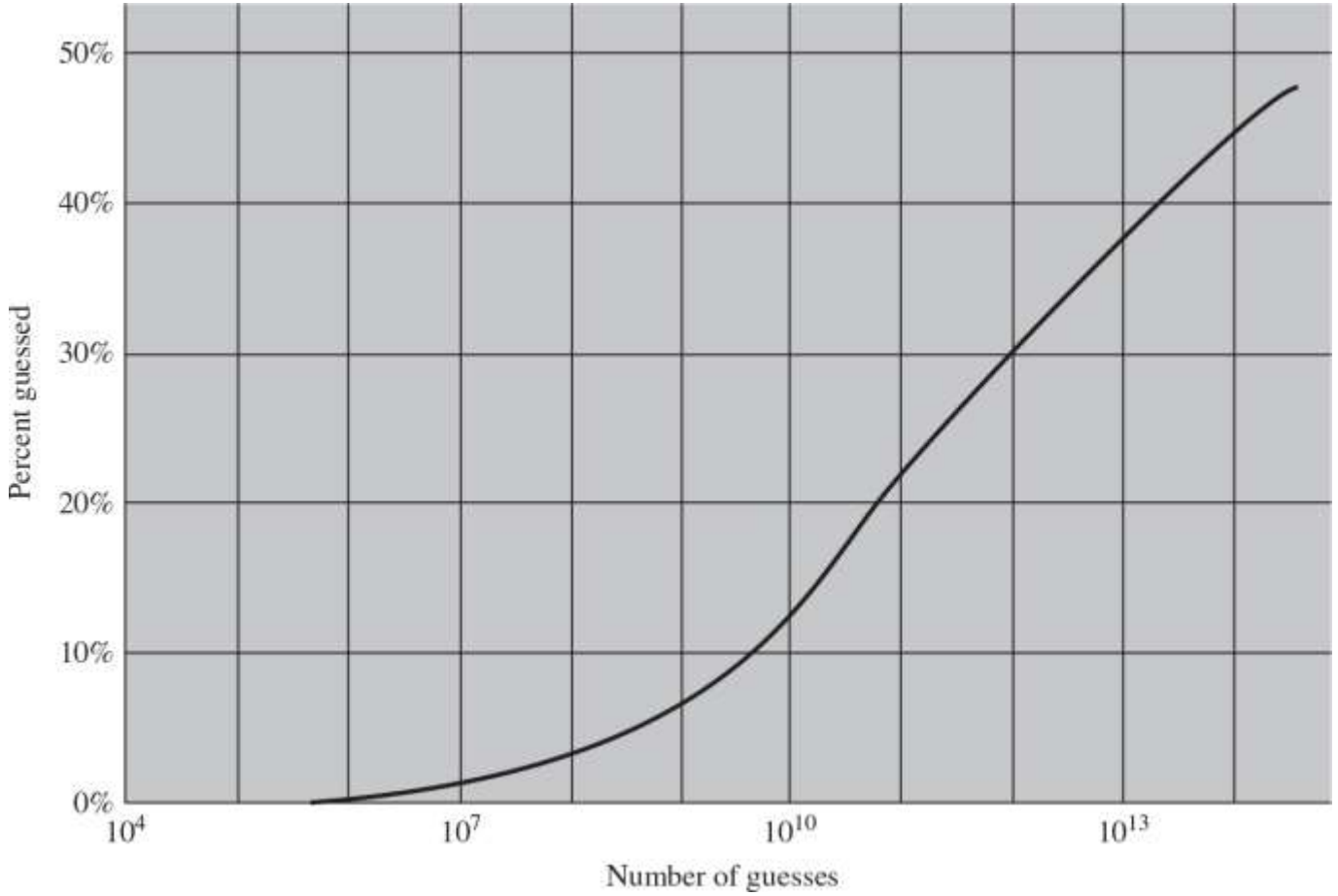


Figure 3.7 User Authentication with eID

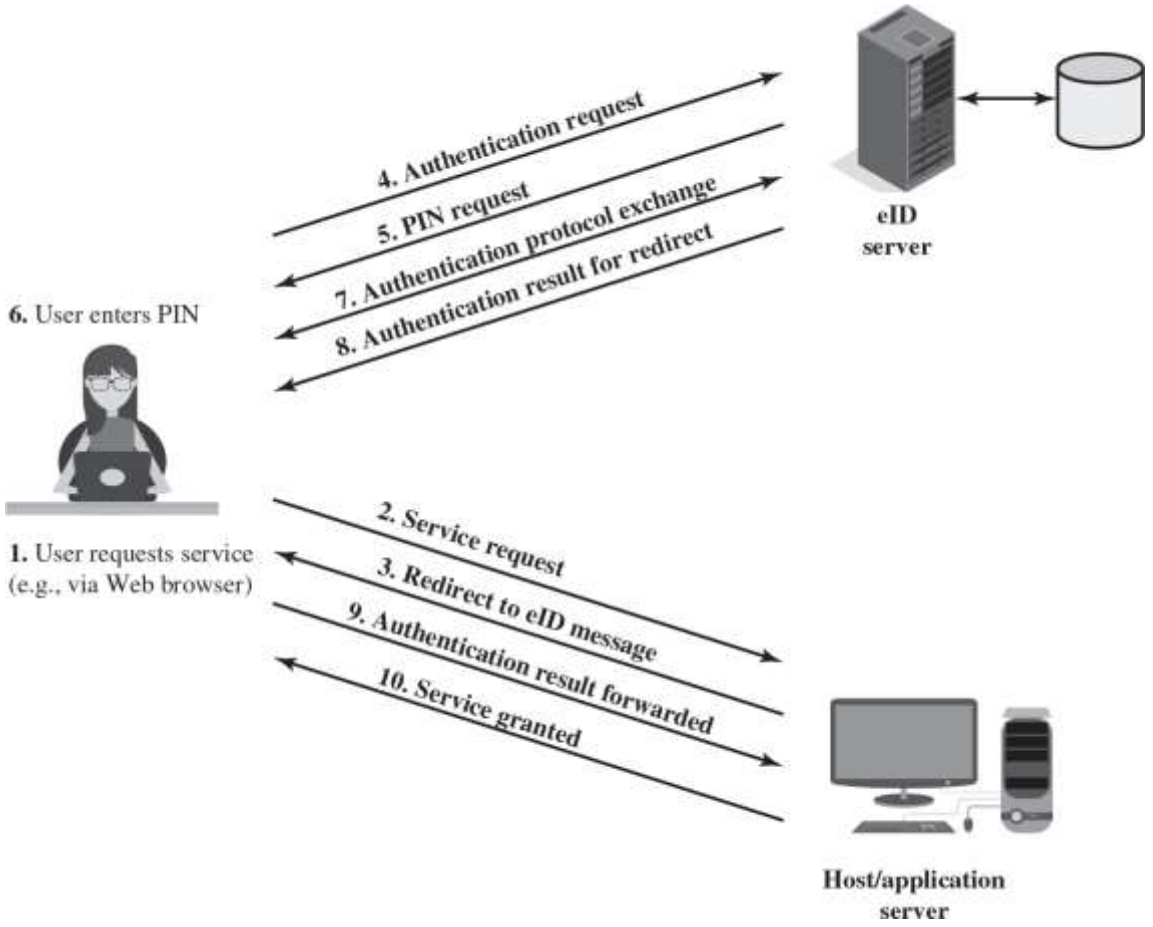


Figure 3.8 Cost Versus Accuracy of Various Biometric Characteristics in User Authentication Schemes

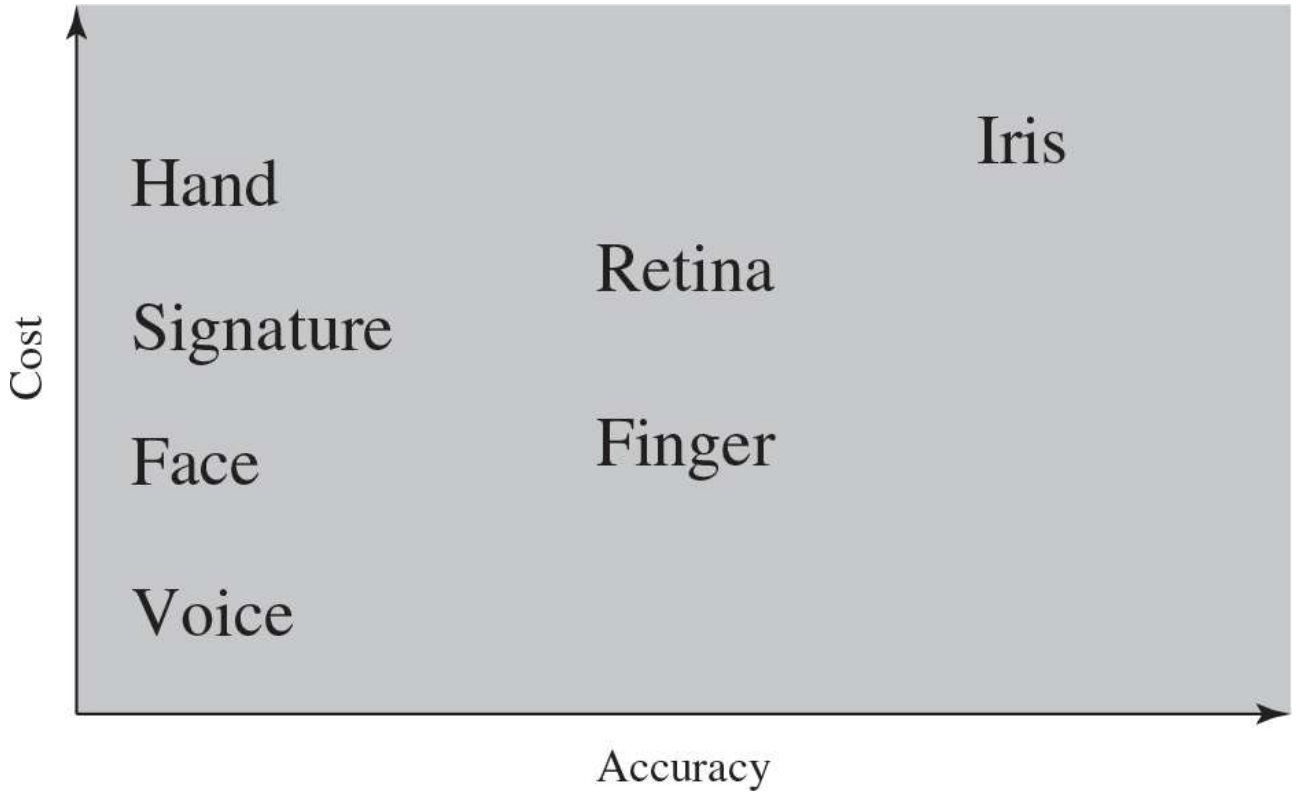


Figure 3.9 A Generic Biometric System

Enrollment creates an association between a user and the user's biometric characteristics. Depending on the application, user authentication either involves verifying that a claimed user is the actual user or identifying an unknown user.

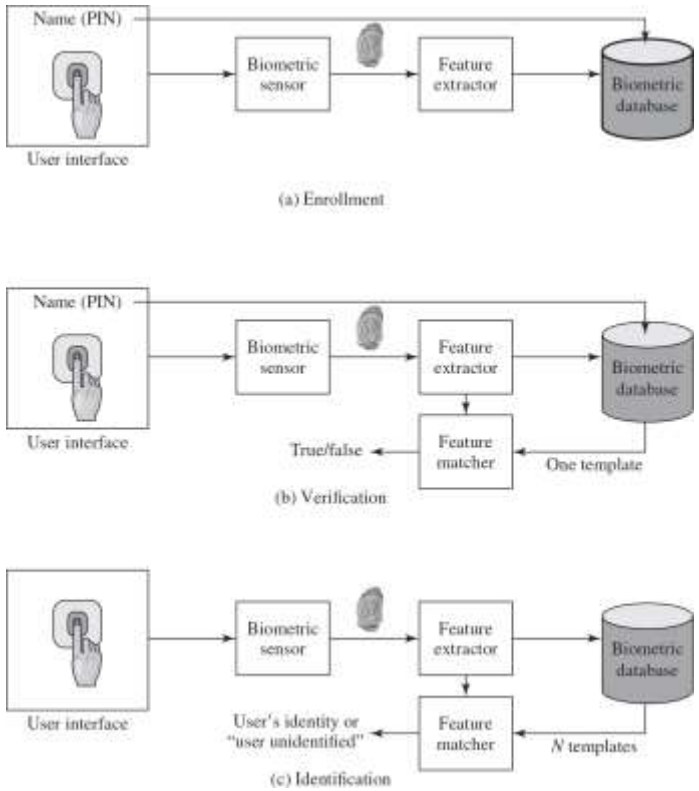


Figure 3.13 Basic Challenge-Response Protocols for Remote User Authentication

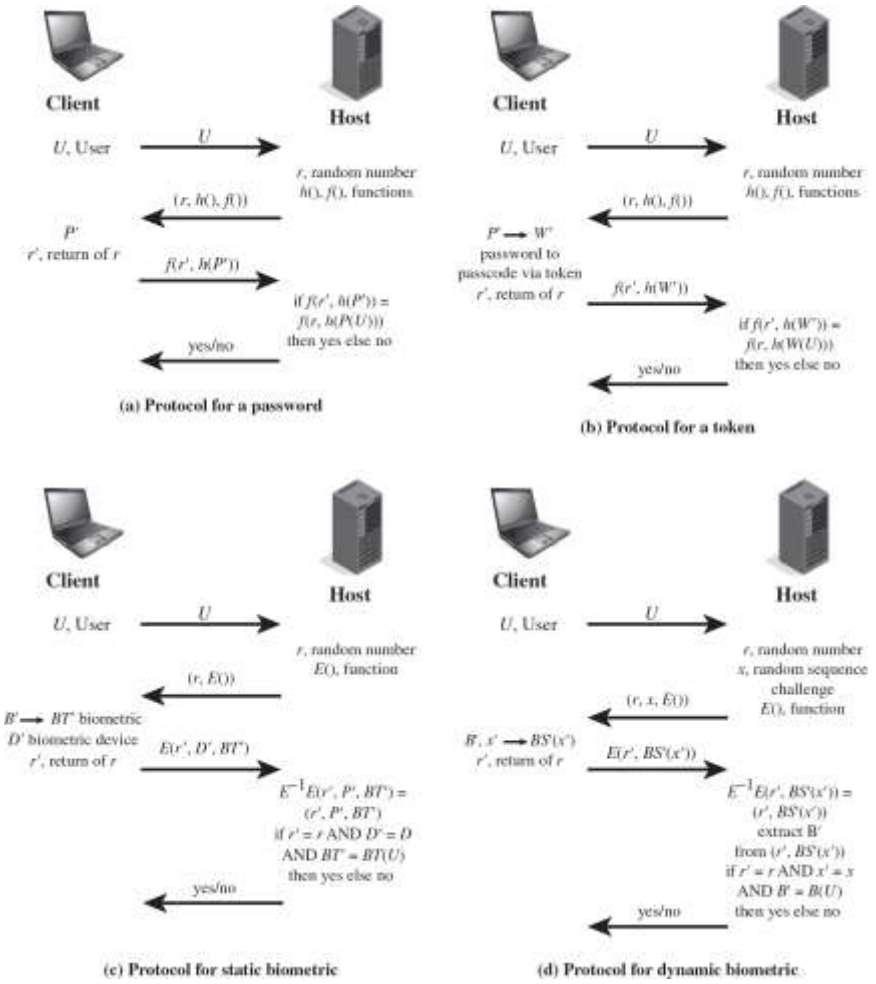
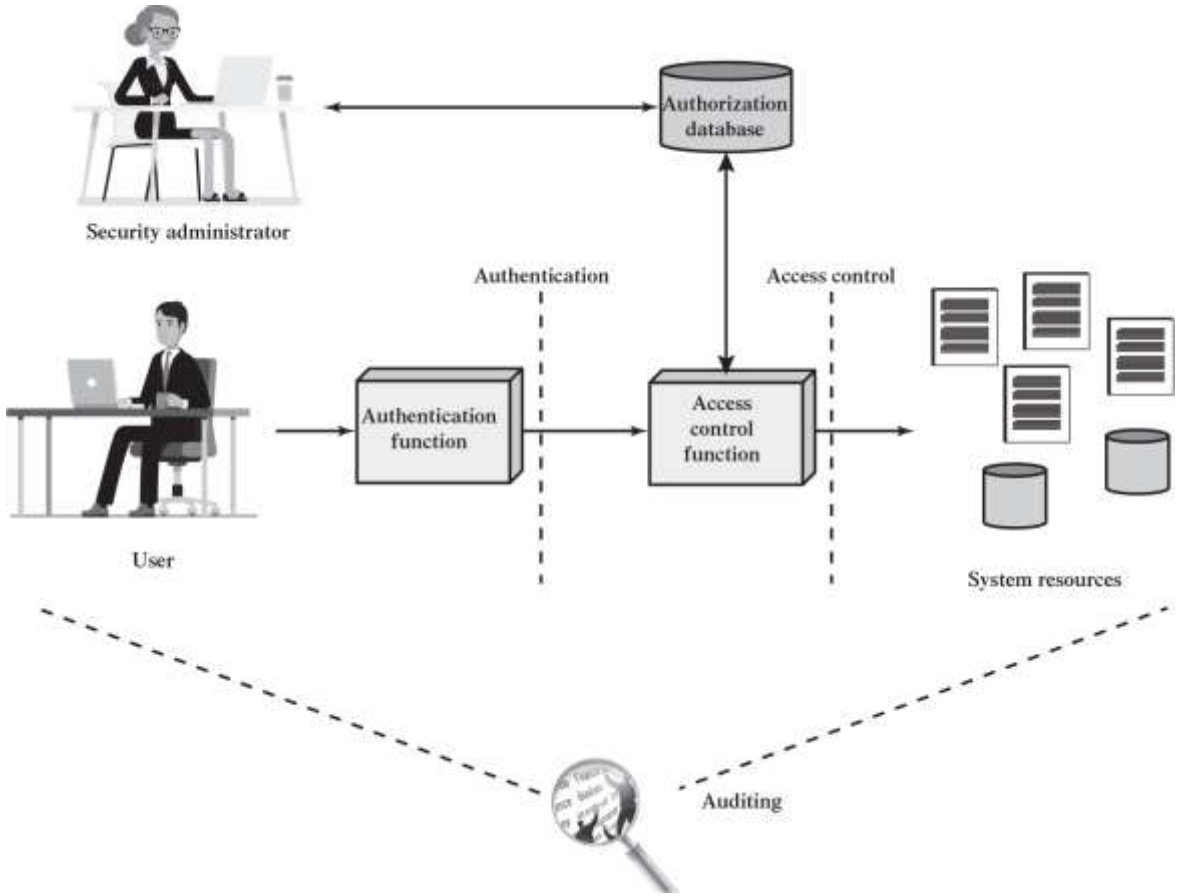
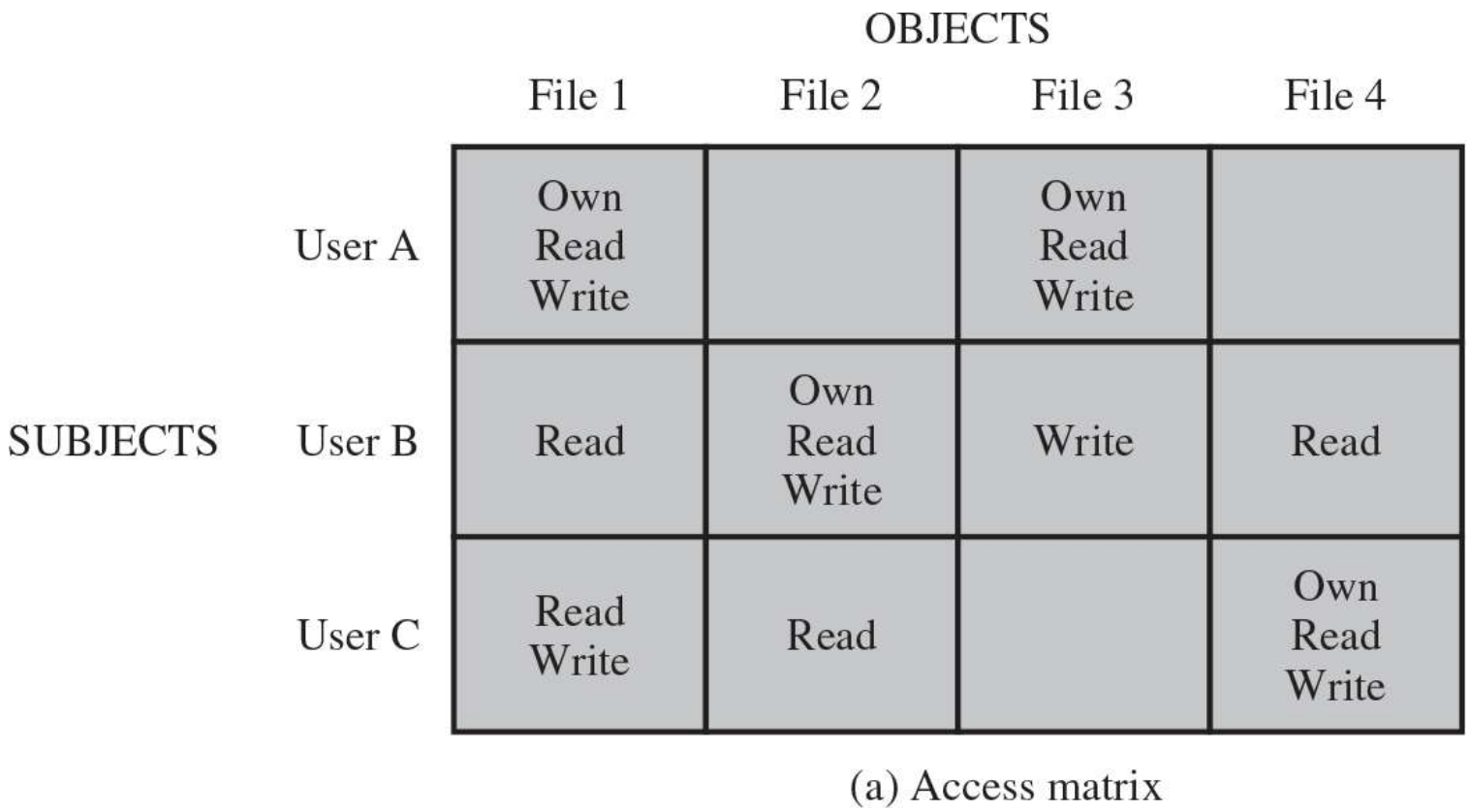


Figure 4.1 Relationship Among Access Control and Other Security Functions



Source: Based on [SAND94].

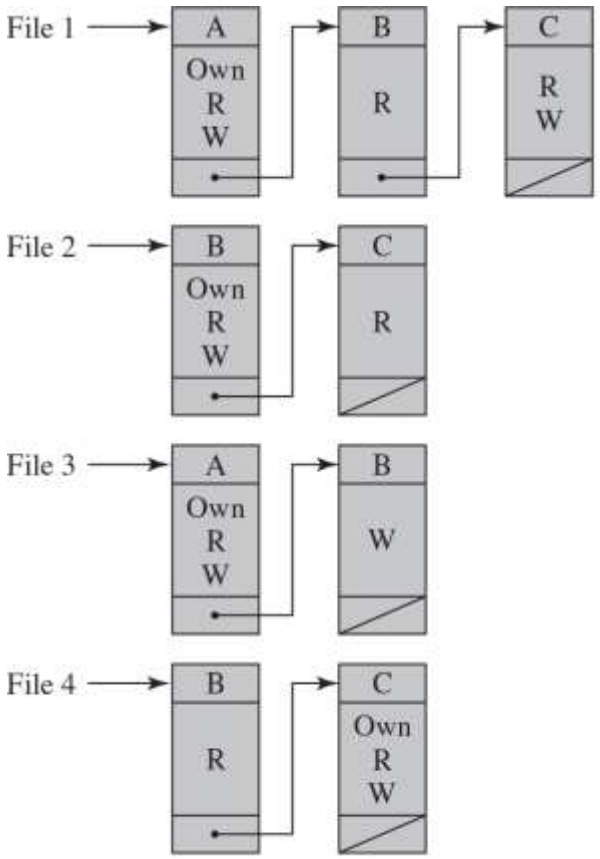
Figure 4.2 Example of Access Control Structures (1 of 2)



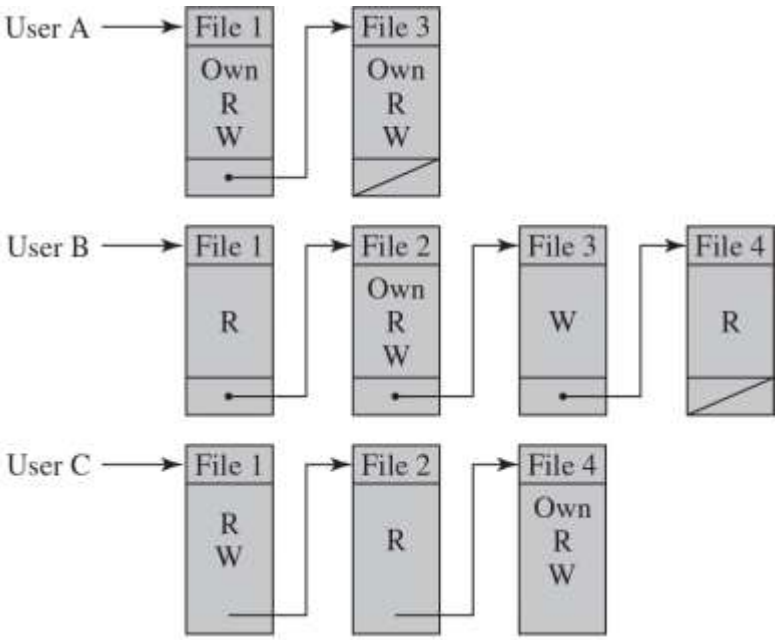
		OBJECTS			
		File 1	File 2	File 3	File 4
SUBJECTS	User A	Own Read Write		Own Read Write	
	User B	Read	Own Read Write	Write	Read
	User C	Read Write	Read		Own Read Write

(a) Access matrix

Figure 4.2 Example of Access Control Structures (2 of 2)



(b) Access control lists for files of part (a)



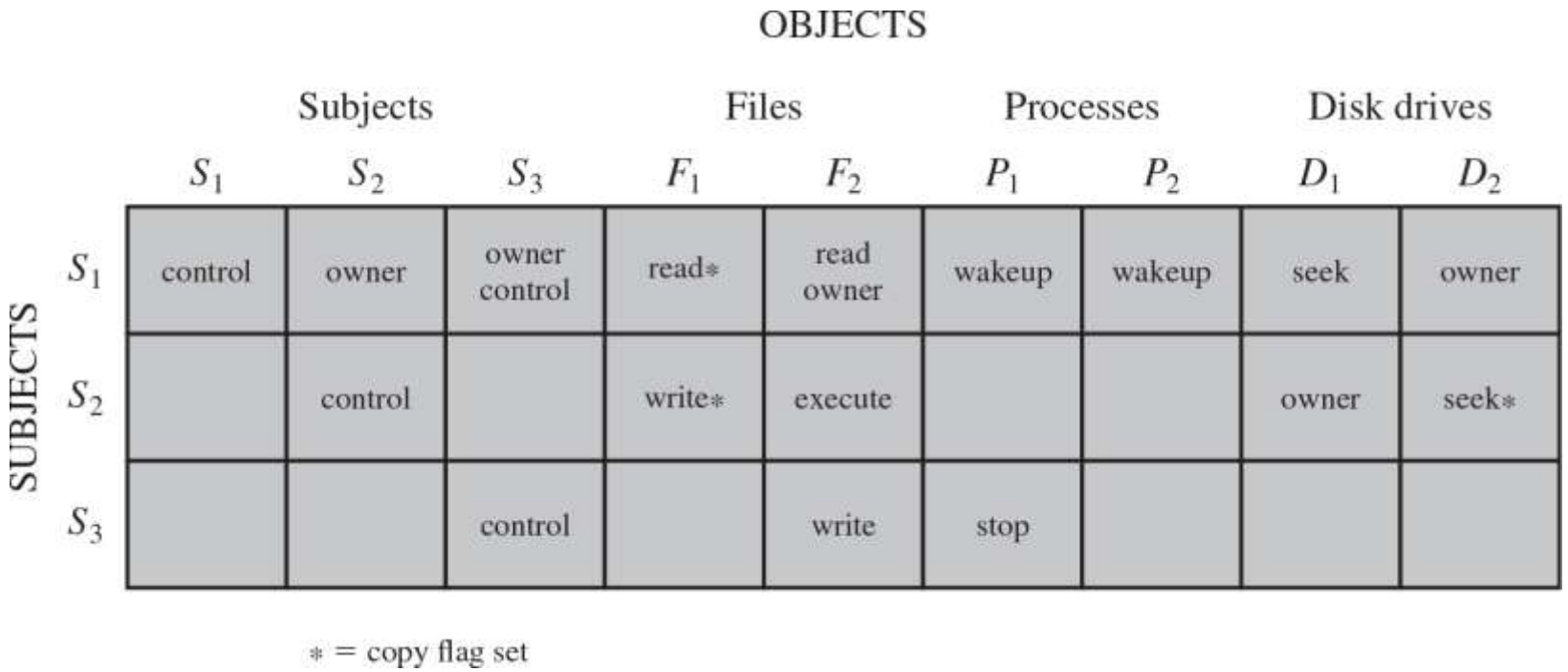
(c) Capability lists for files of part (a)

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

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

Figure 4.3 Extended Access Control Matrix



SUBJECTS	OBJECTS: Subjects S_1	Subjects S_2	Subjects S_3	Files F_1	Files F_2	Processes P_1	Processes P_2	Disk drives D_1	Disk drives D_2
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 4.4 An Organization of the Access Control Function

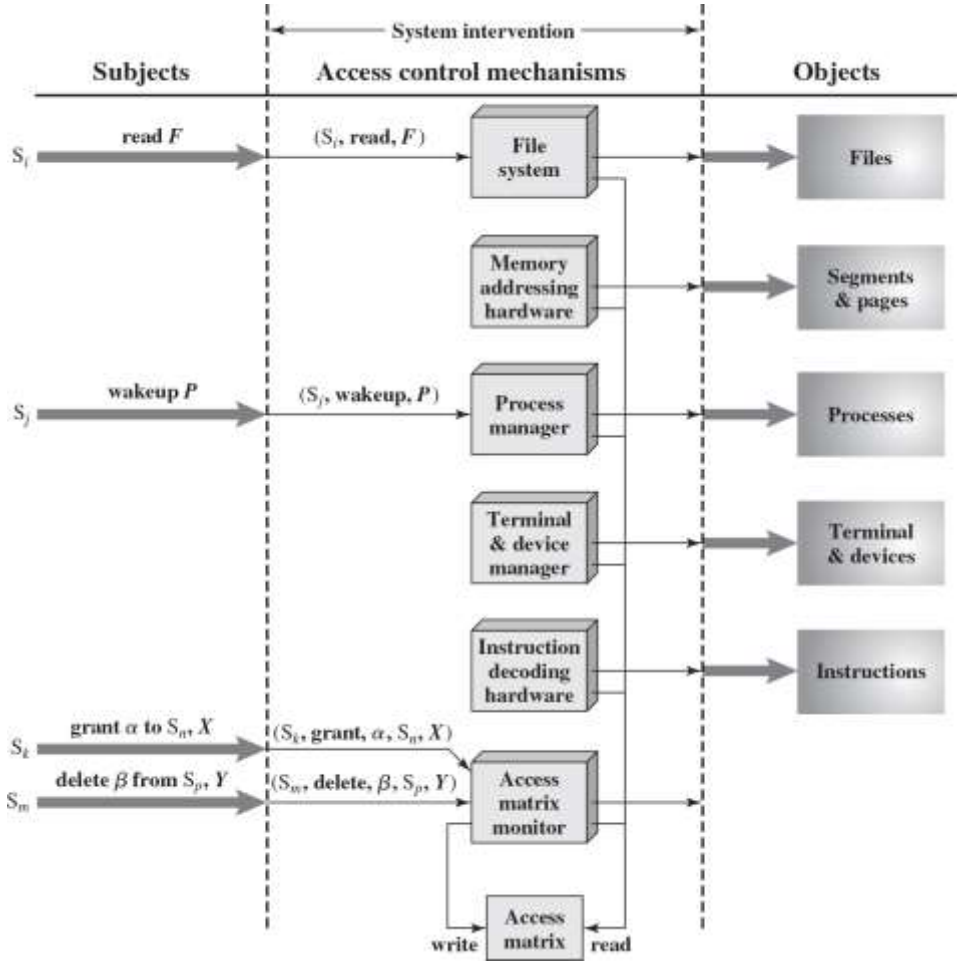


Figure 4.6 Users, Roles, and Resources

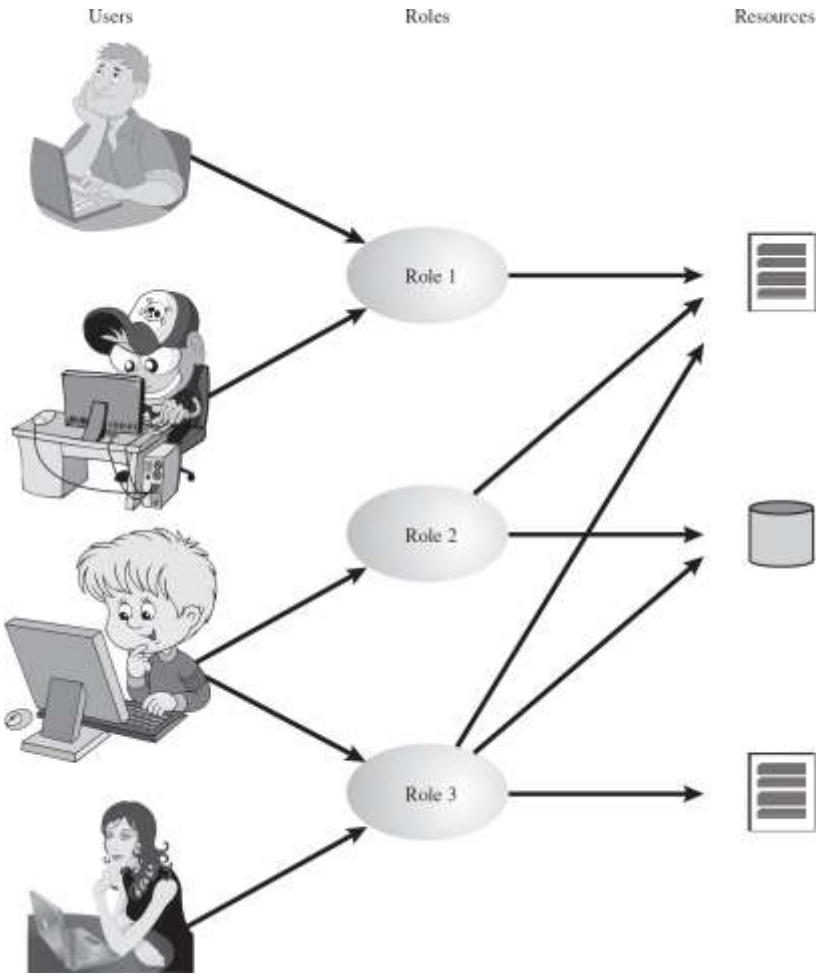
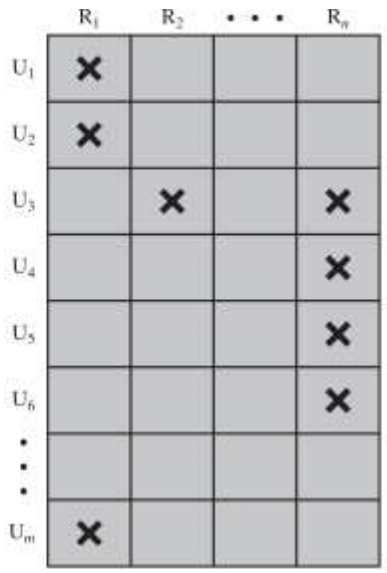
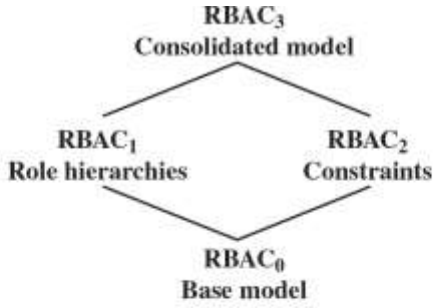


Figure 4.7 Access Control Matrix Representation of RBAC

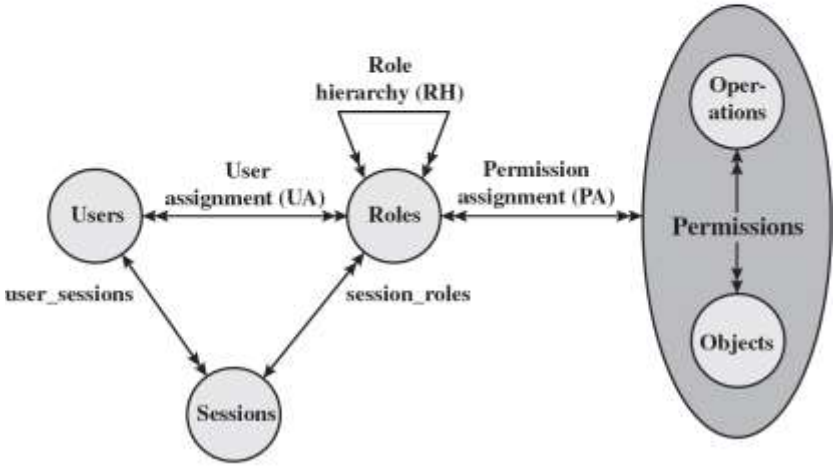


	OBJECTS								
ROLES	R_1	R_2	R_n	F_1	F_2	P_1	P_2	D_1	D_2
R_1	control	owner	owner control	read *	read owner	wakeup	wakeup	seek	owner
R_2		control		write *	execute			owner	seek *
...									
R_n			control		write	stop			

Figure 4.8 A Family of Role-Based Access Control Models



(a) Relationship among RBAC models



(b) RBAC models

Figure 4.9 Example of Role Hierarchy

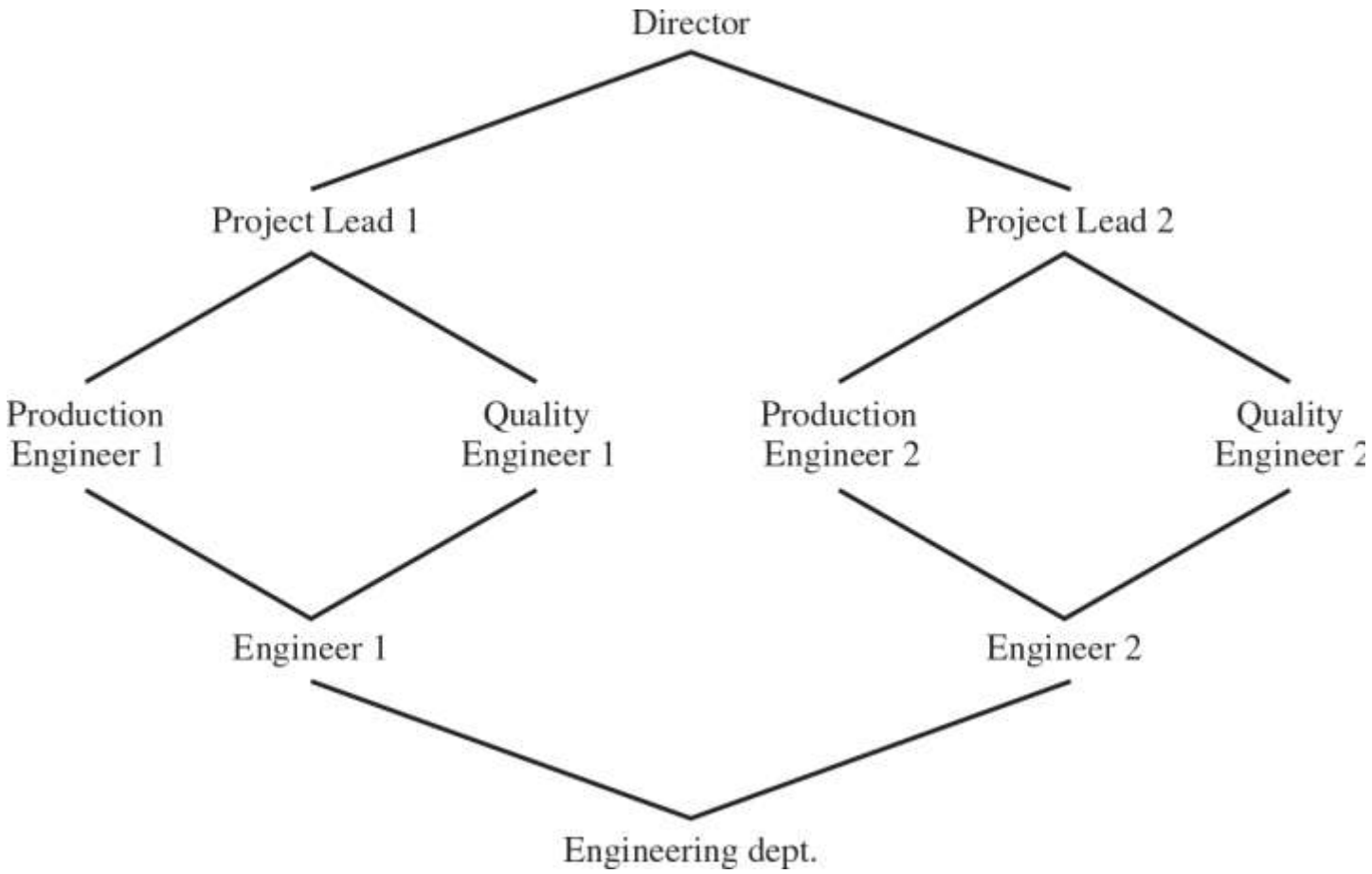


Figure 7.1 Example Network to Illustrate DoS Attacks

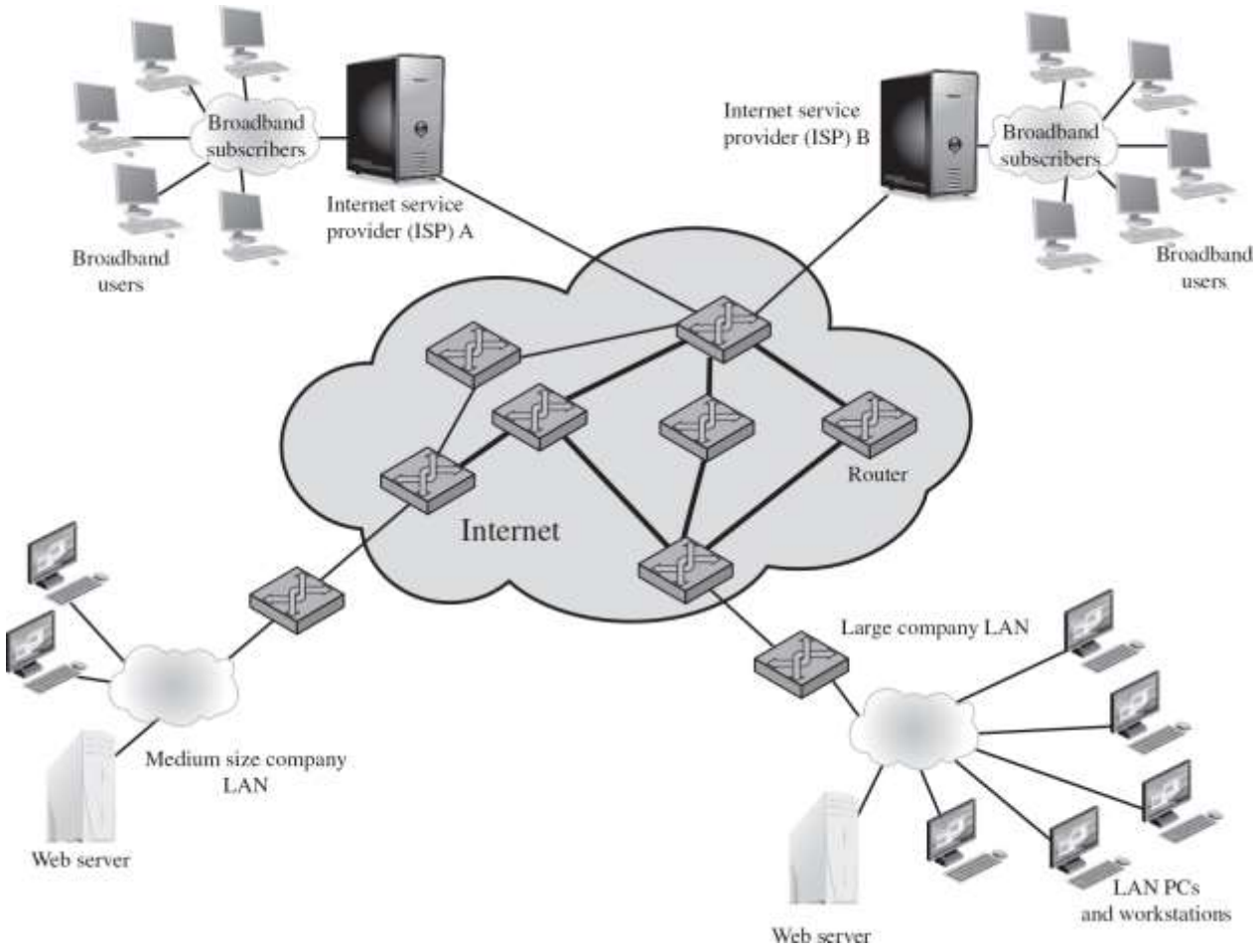


Figure 7.2 TCP Three-Way Connection Handshake

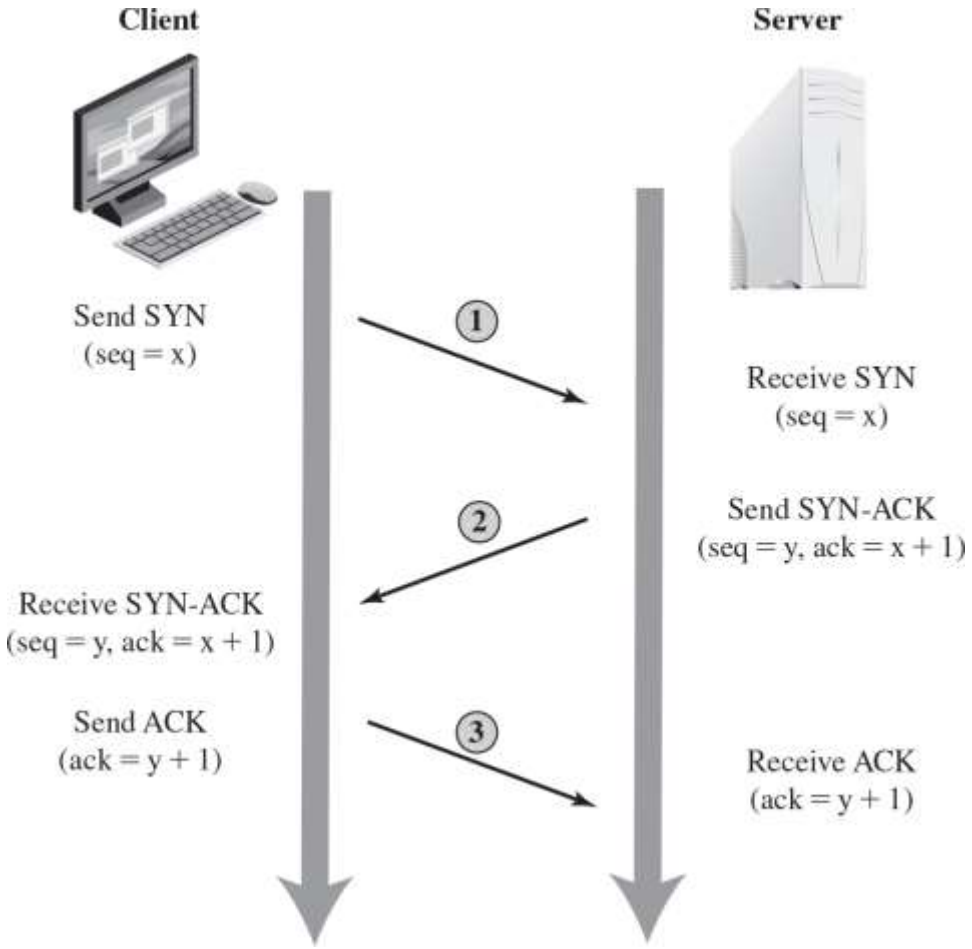


Figure 8.5 Example of NIDS Sensor Deployment

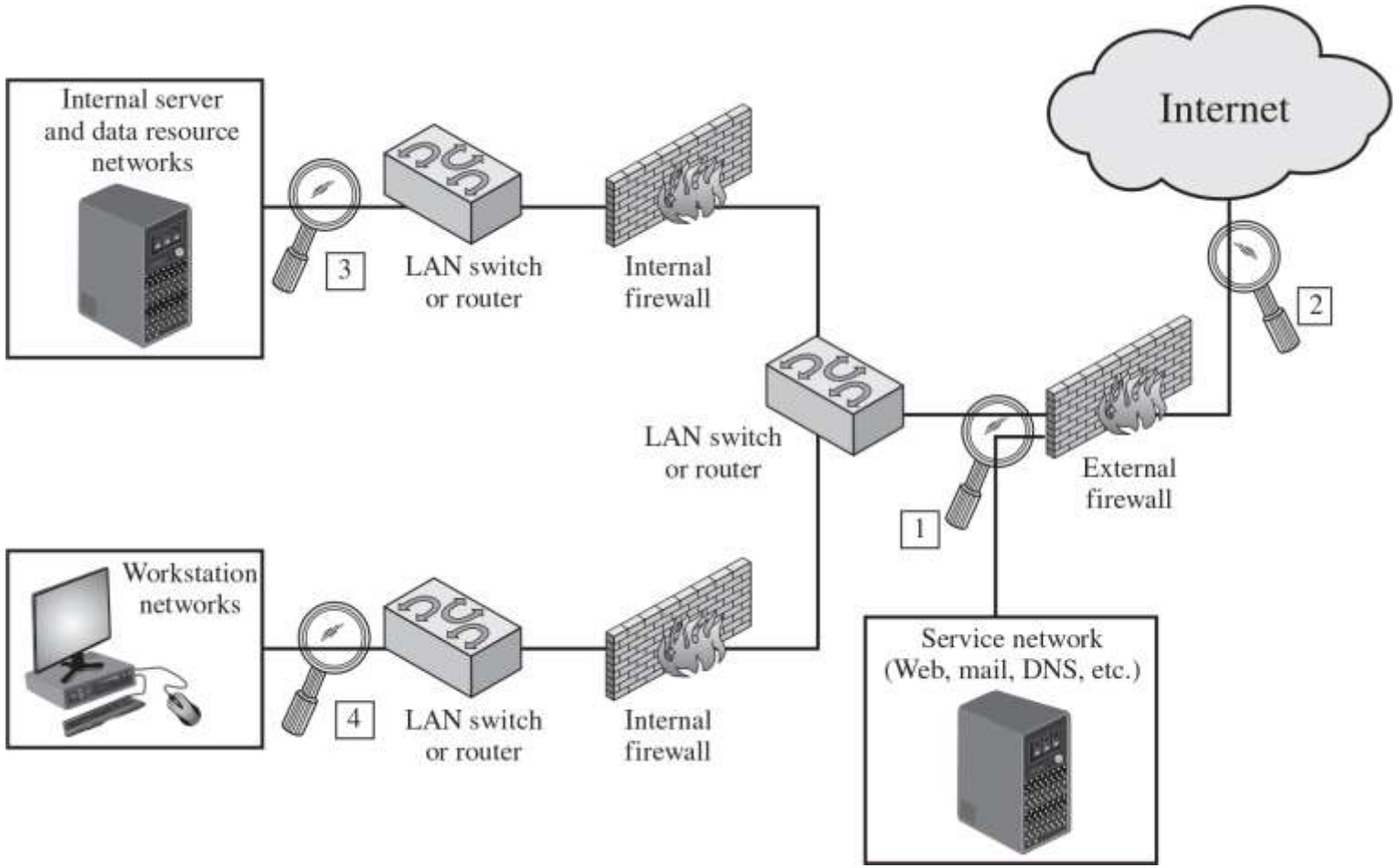


Figure 8.8 Example of Honeypot Deployment

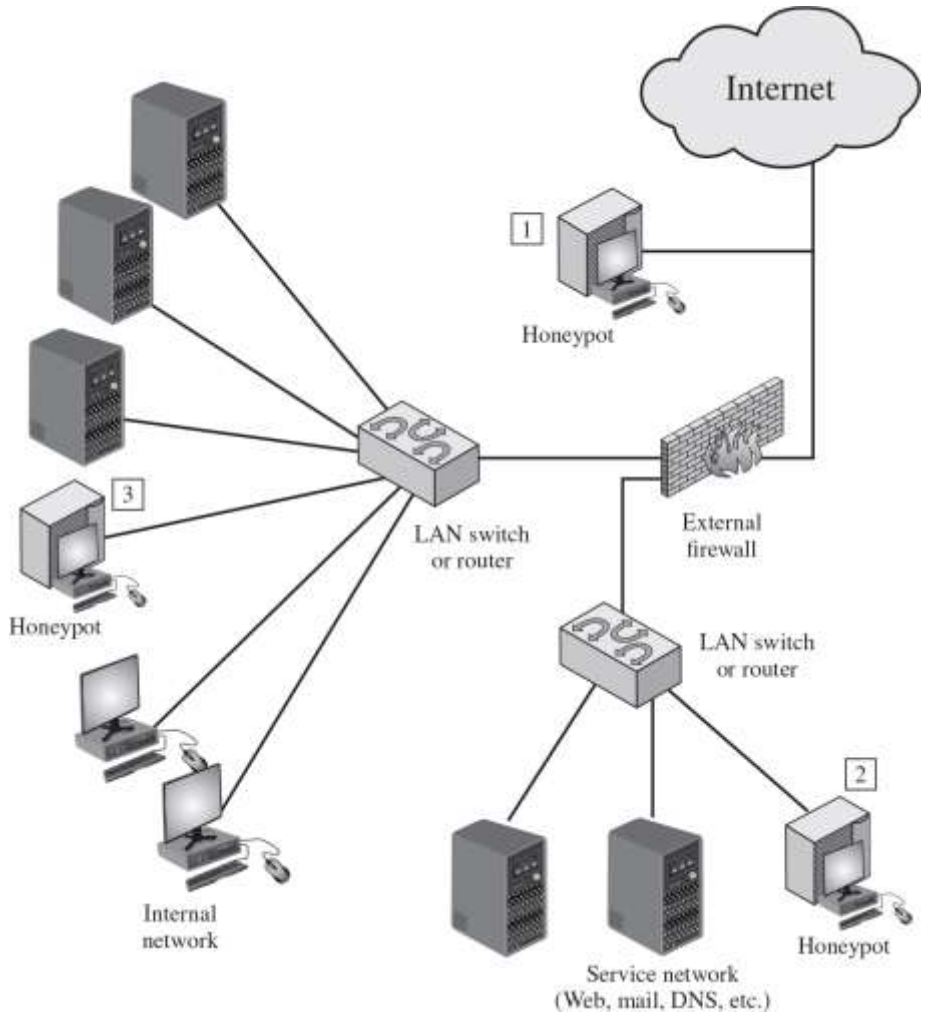


Figure 9.2 Example Firewall Configuration

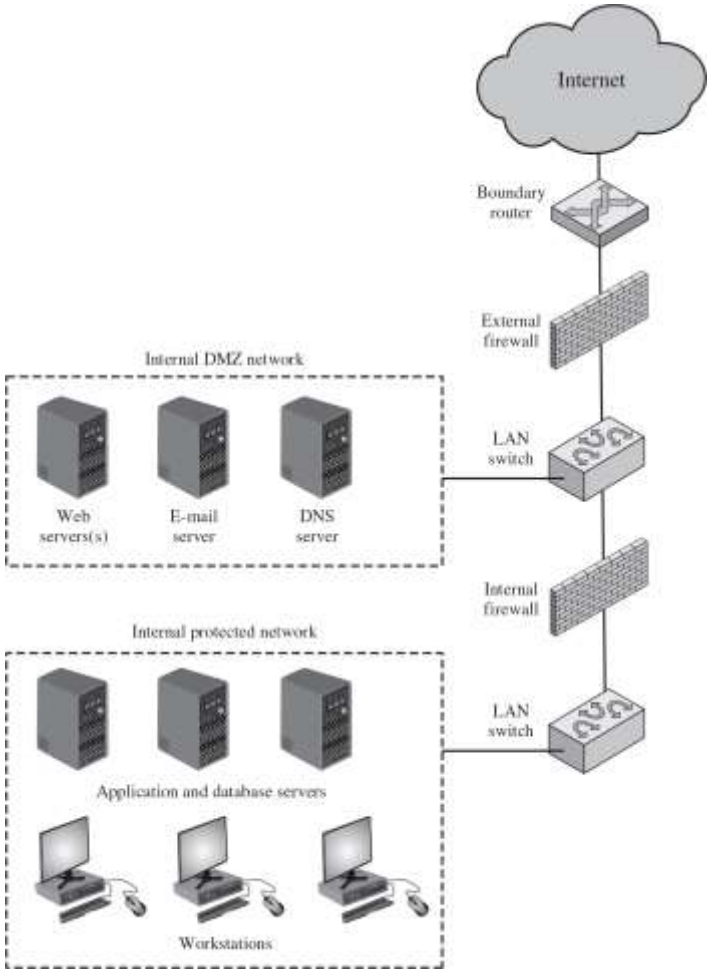


Figure 9.4 Example Distributed Firewall Configuration

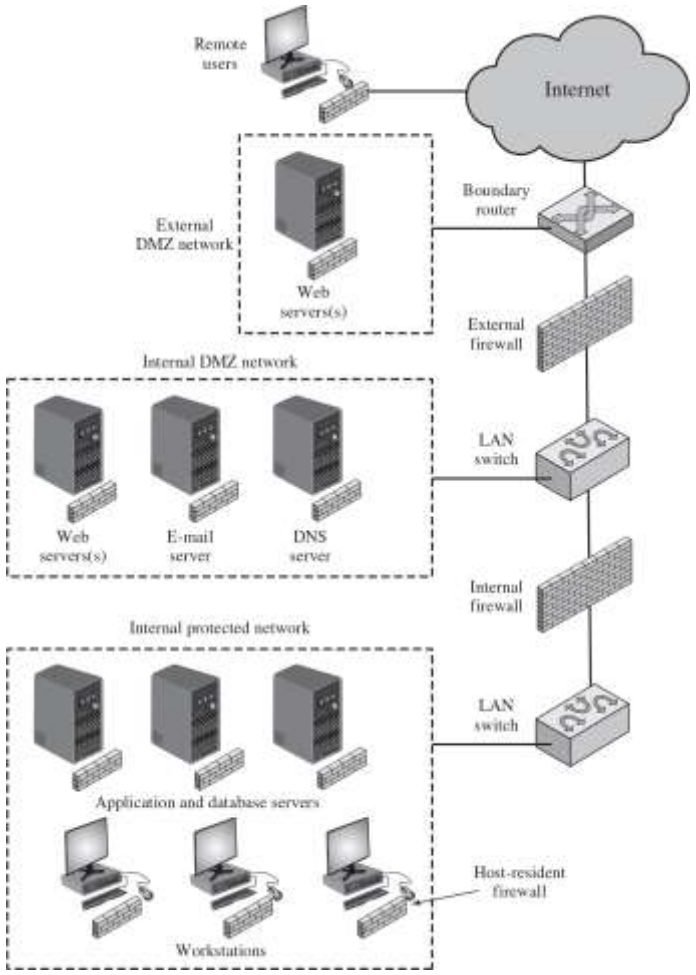


Figure 14.3 Risk Assessment Process

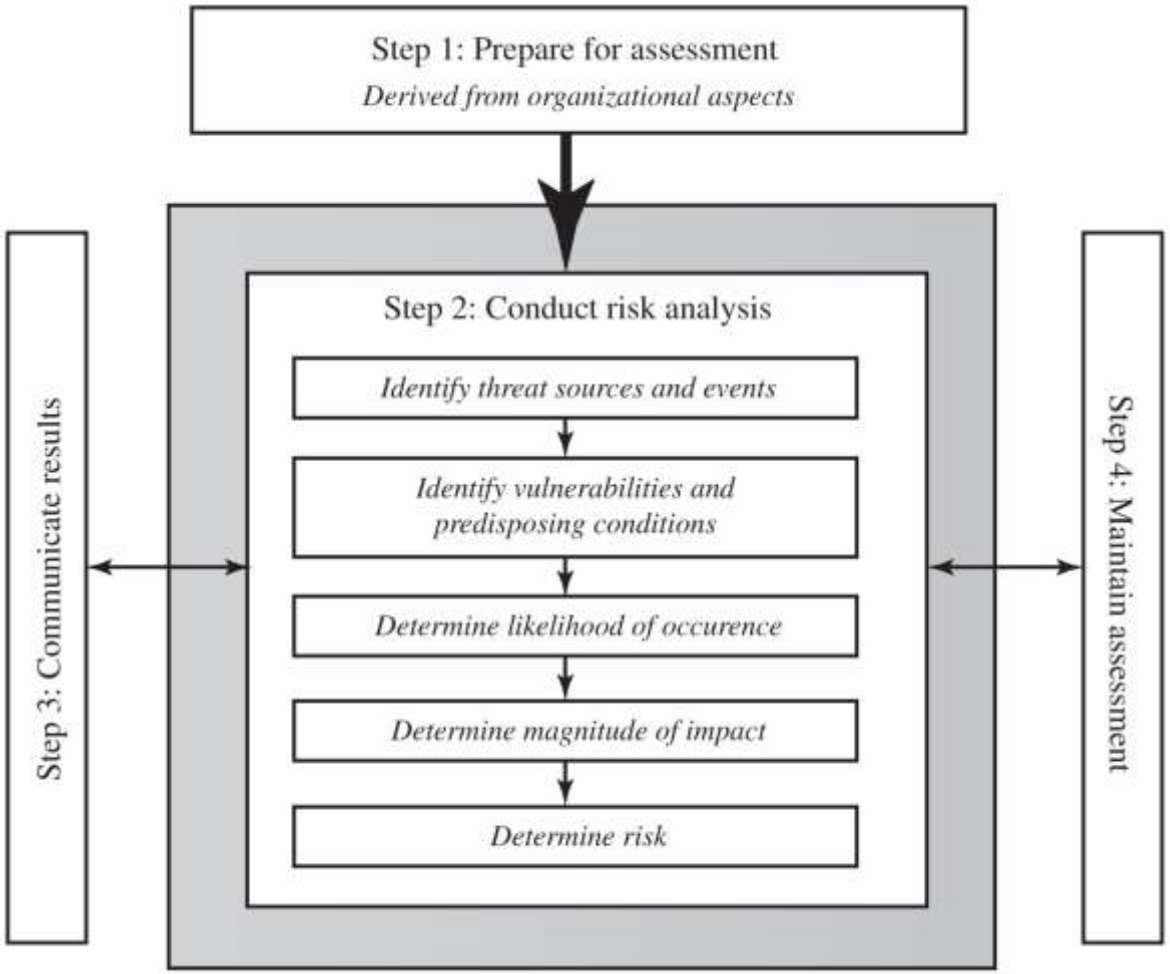


Figure 14.4 Generic Organizational Risk Context

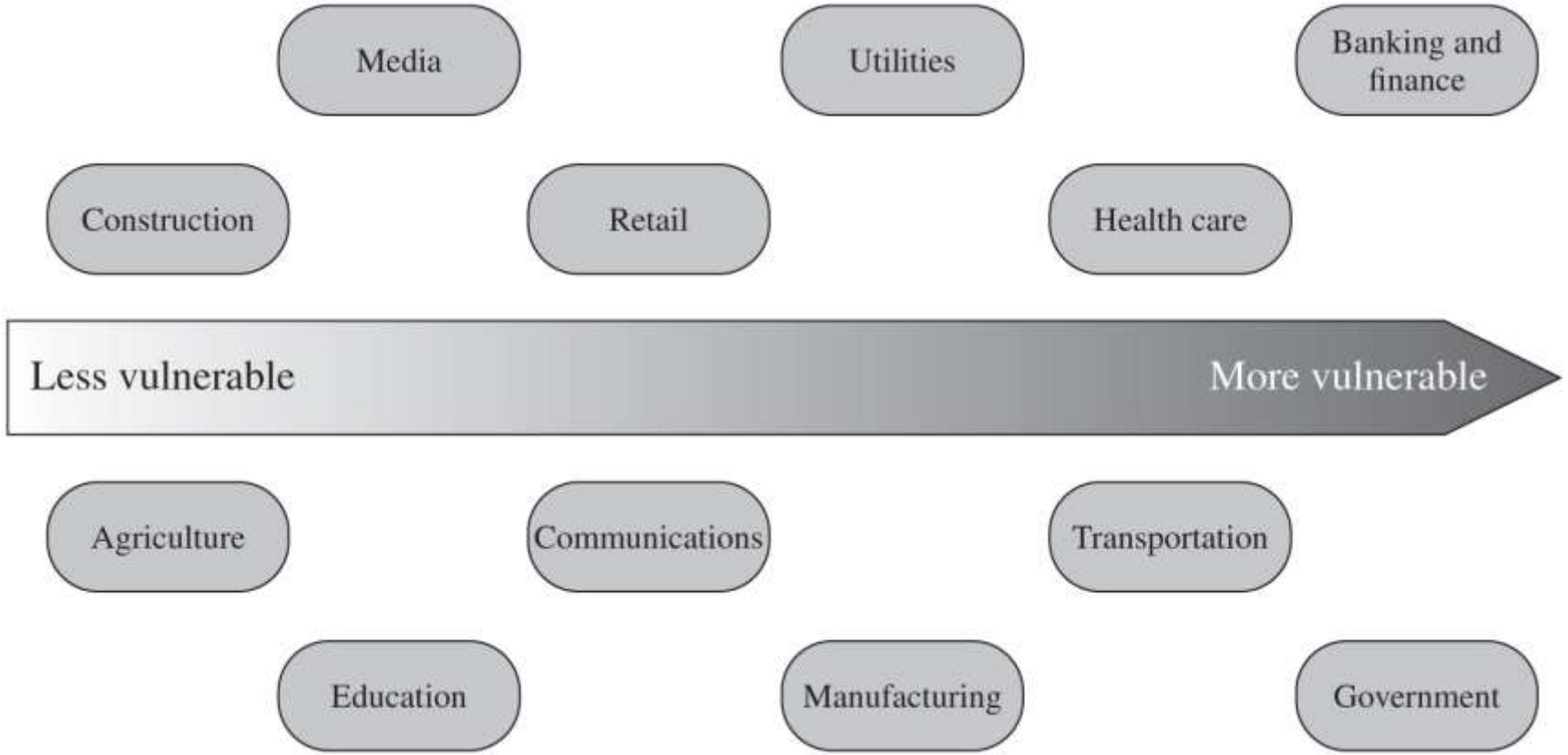


Figure 14.5 Judgment About Risk Treatment