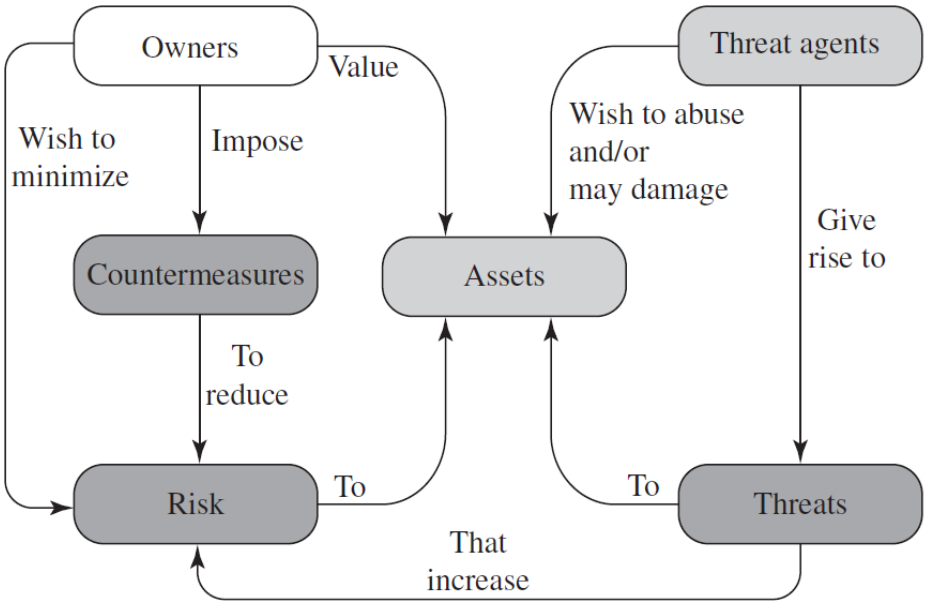


Figure 1.2 Security Concepts and Relationships

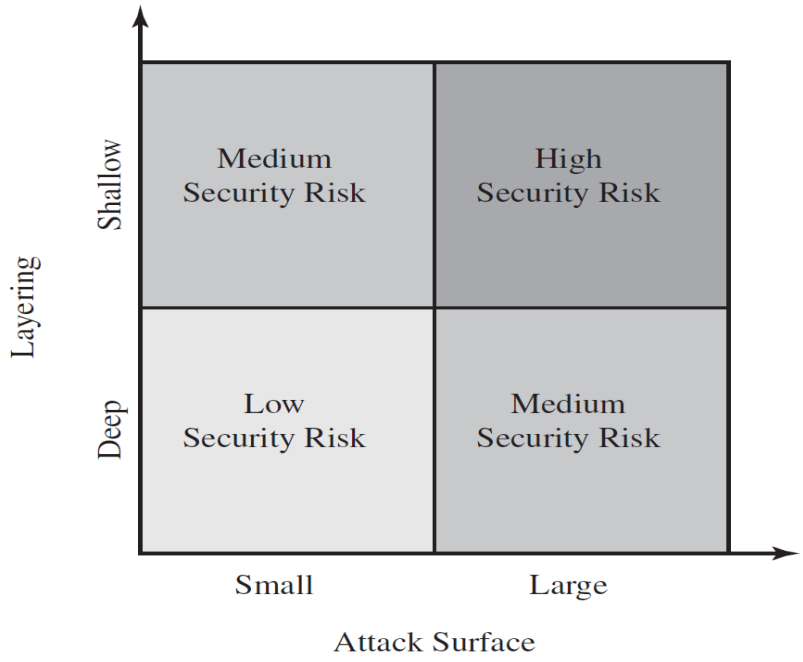


Figure 1.4 Defense in Depth and Attack Surface

Chap 2

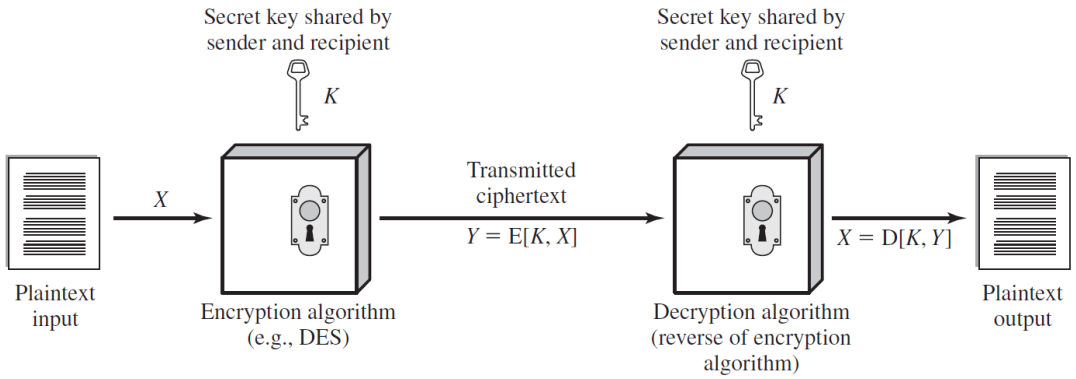
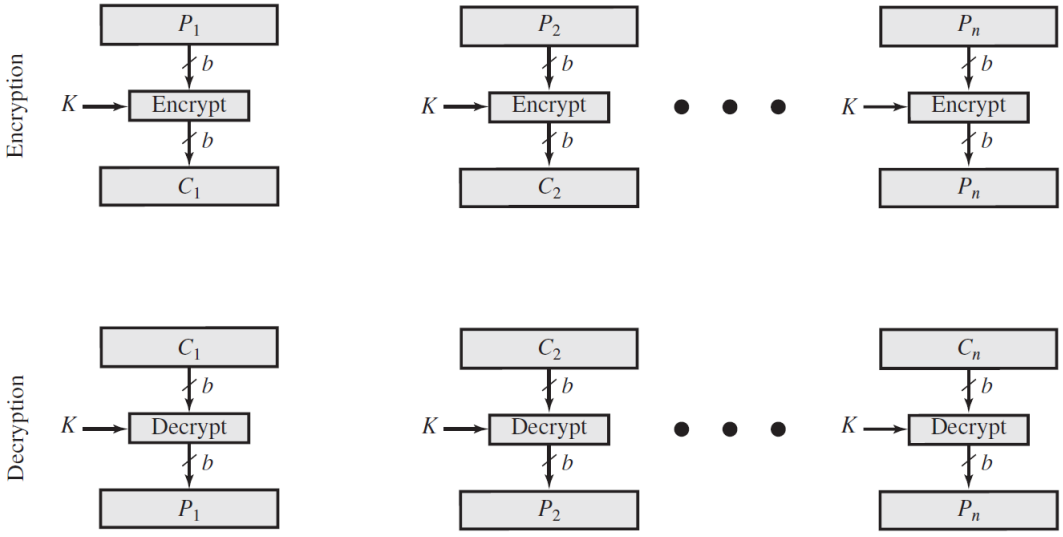
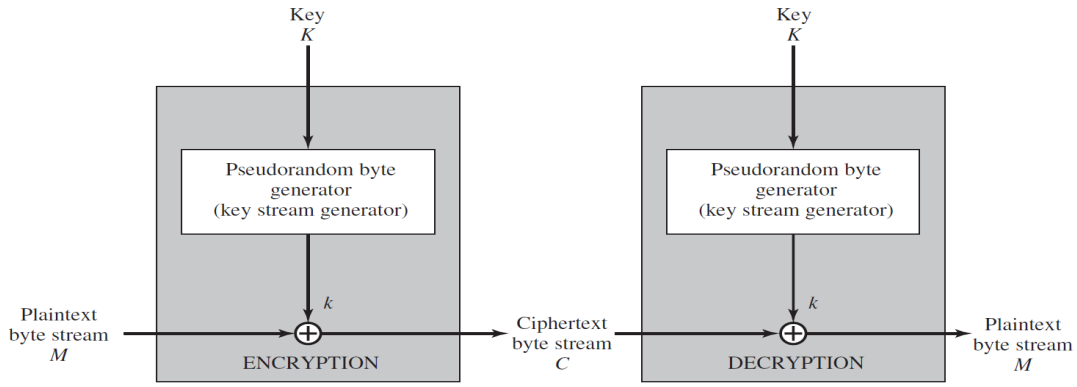


Figure 2.1 Simplified Model of Symmetric Encryption



(a) Block cipher encryption (electronic codebook mode)



(b) Stream encryption

Figure 2.2 **Types of Symmetric Encryption**

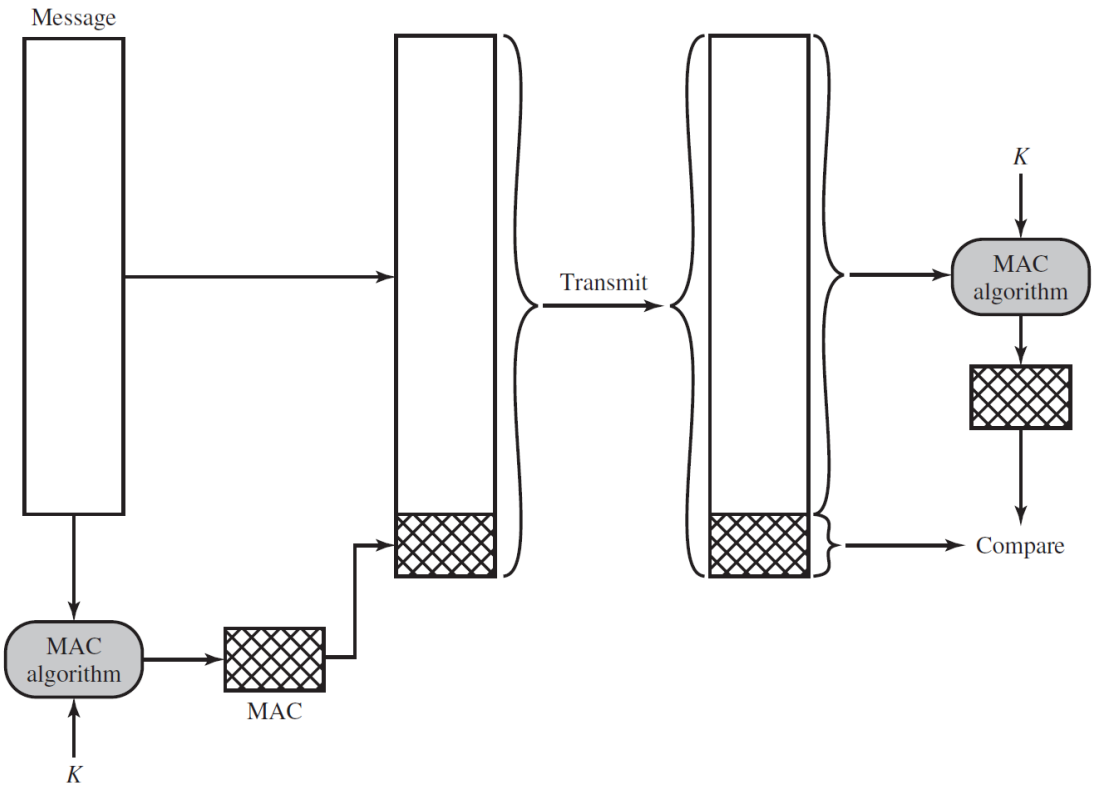
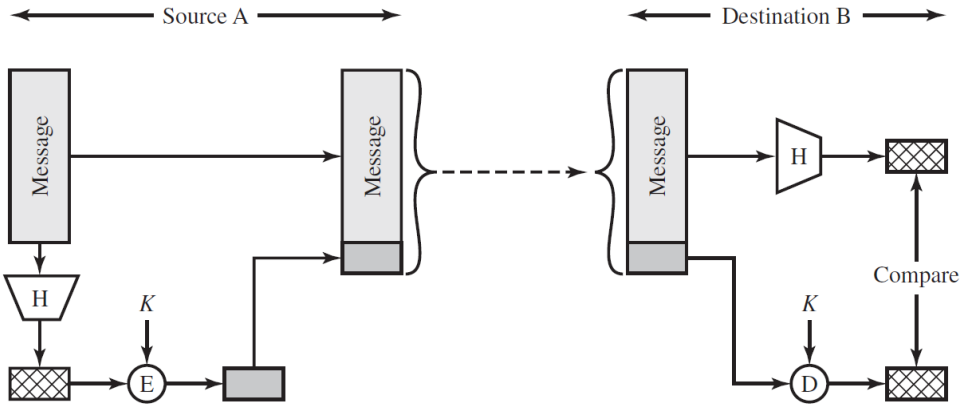
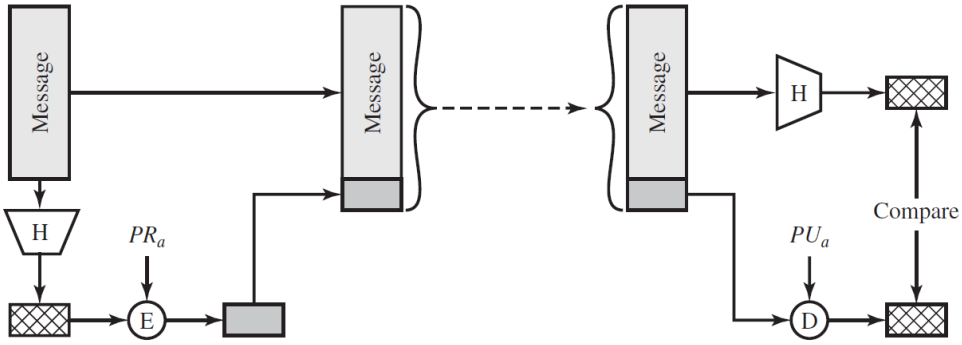


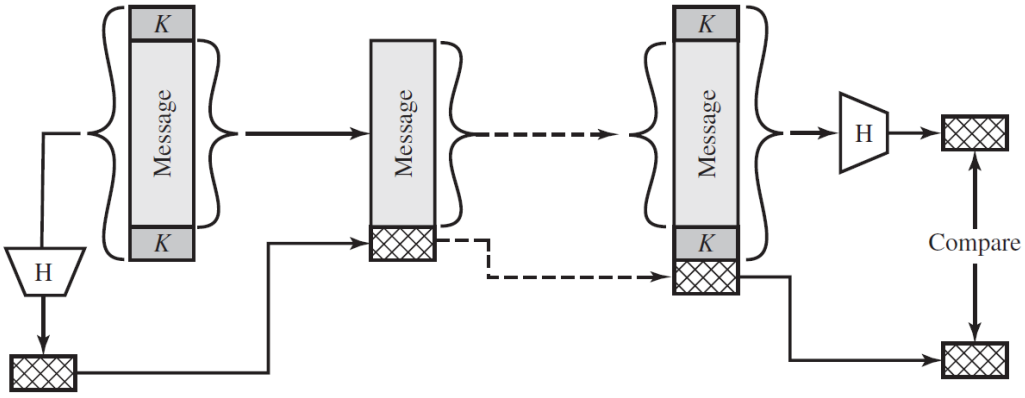
Figure 2.3 **Message Authentication Using a Message Authentication Code (MAC)**



(a) Using symmetric encryption

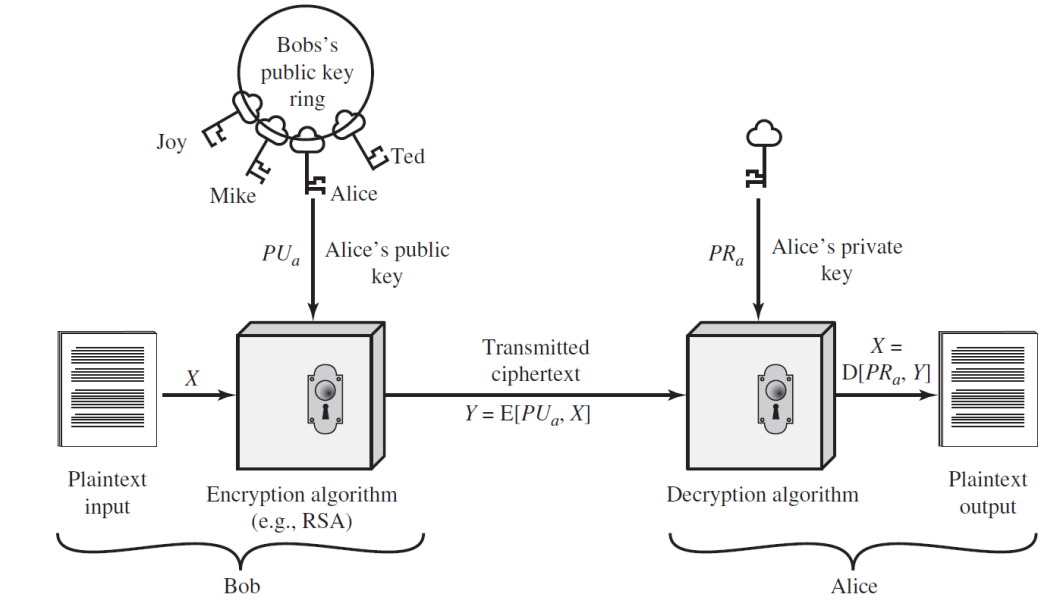


(b) Using public-key encryption

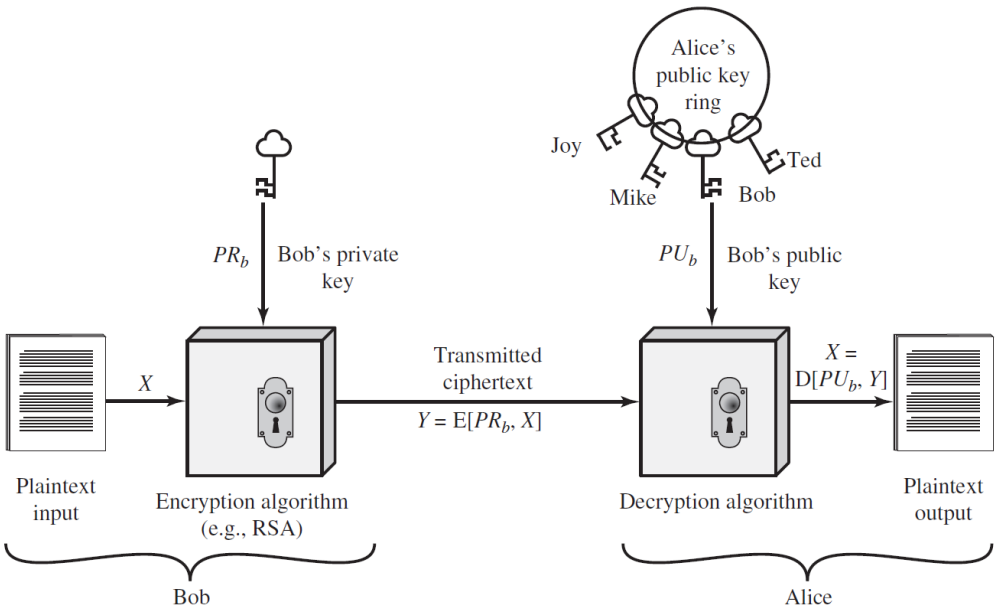


(c) Using secret value

Figure 2.5 Message Authentication Using a One-Way Hash Function

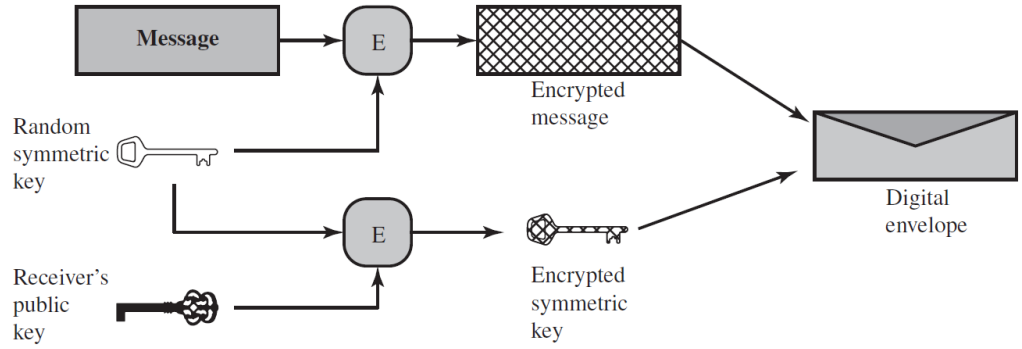


(a) Encryption with public key

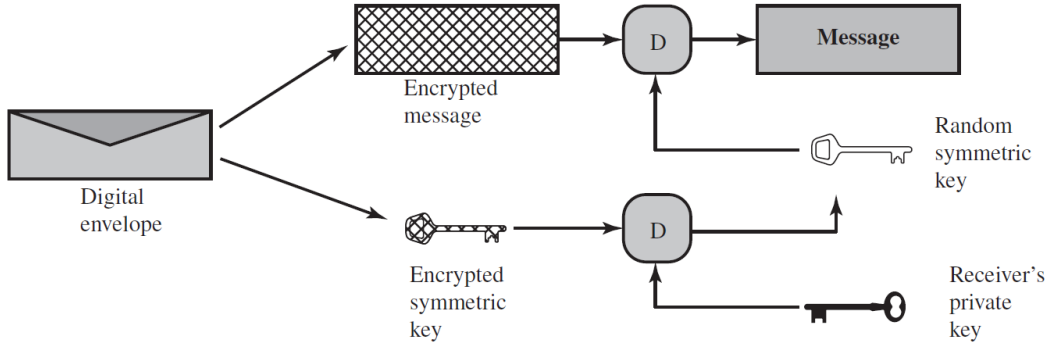


(b) Encryption with private key

Figure 2.6 **Public-Key Cryptography**



(a) Creation of a digital envelope



(b) Opening a digital envelope

Figure 2.9 Digital Envelopes

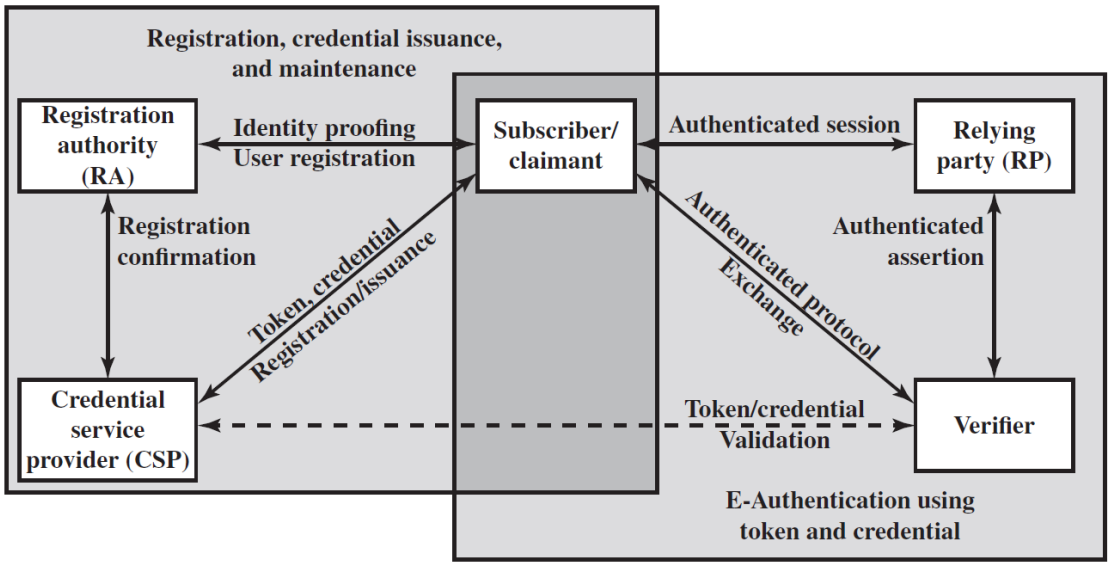


Figure 3.1 The NIST SP 800-63-3 E-Authentication Architectural Model

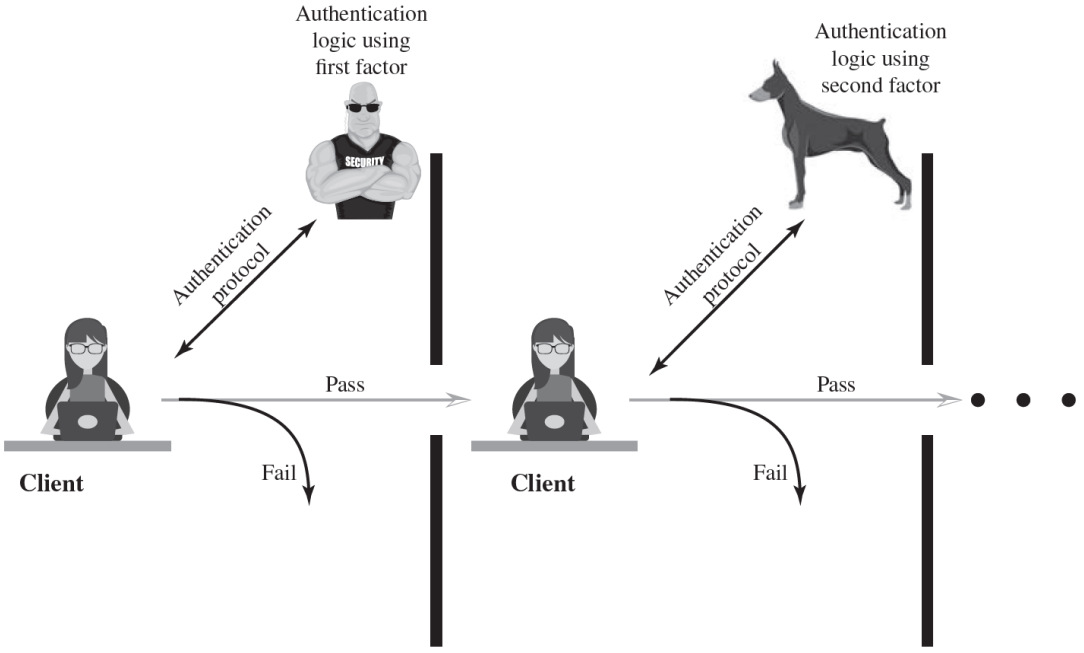
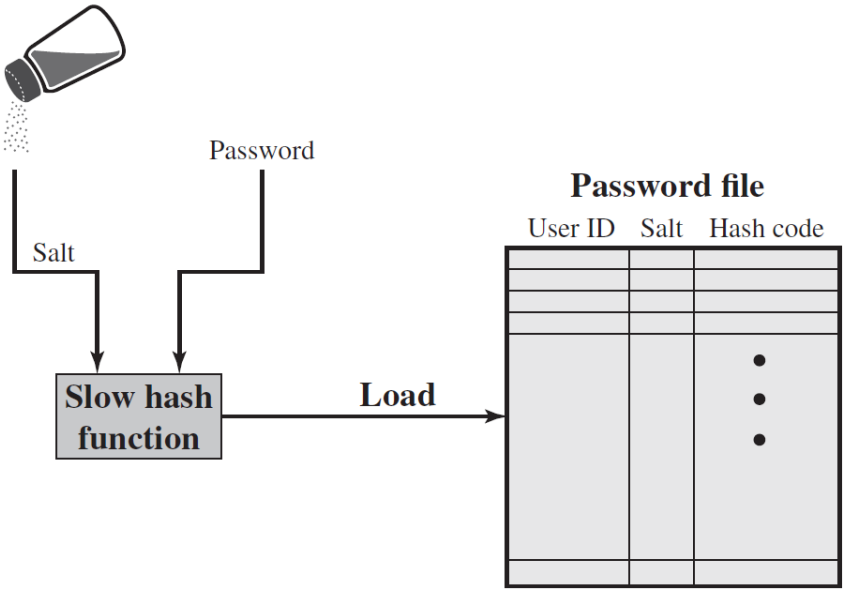
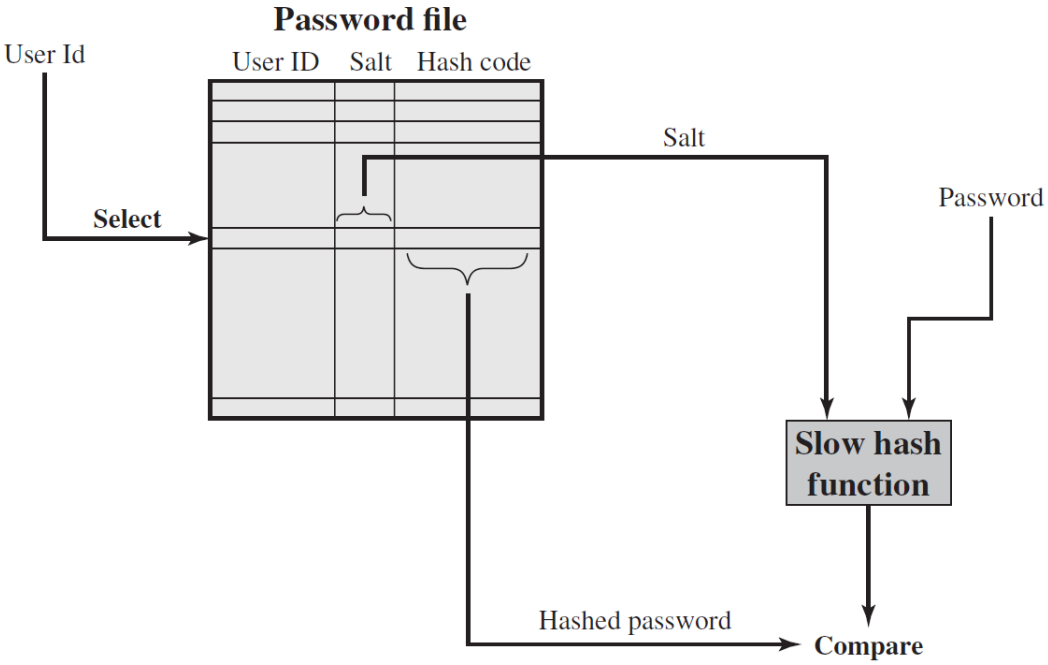


Figure 3.2 Multifactor Authentication



(a) Loading a new password



(b) Verifying a password

Figure 3.3 UNIX Password Scheme

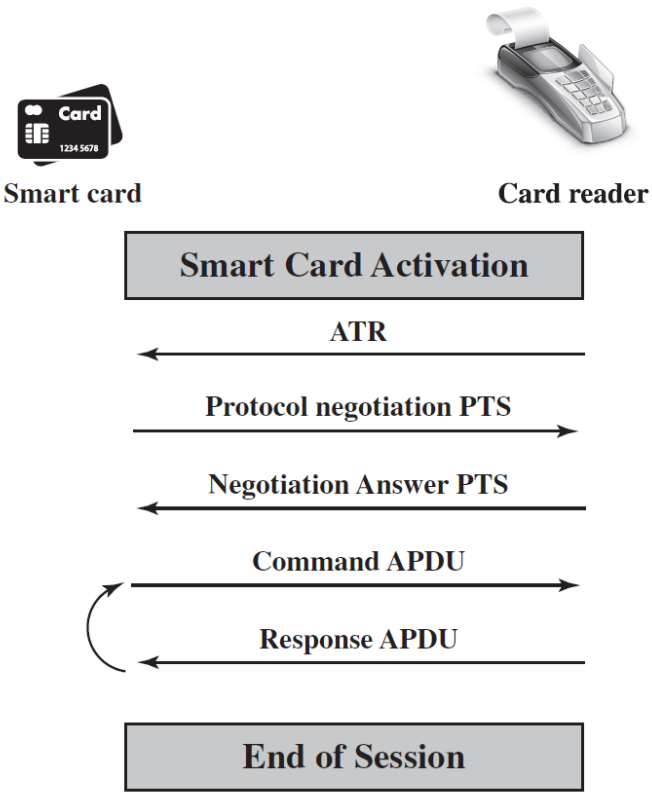


Figure 3.6 **Smart Card/Reader Exchange**

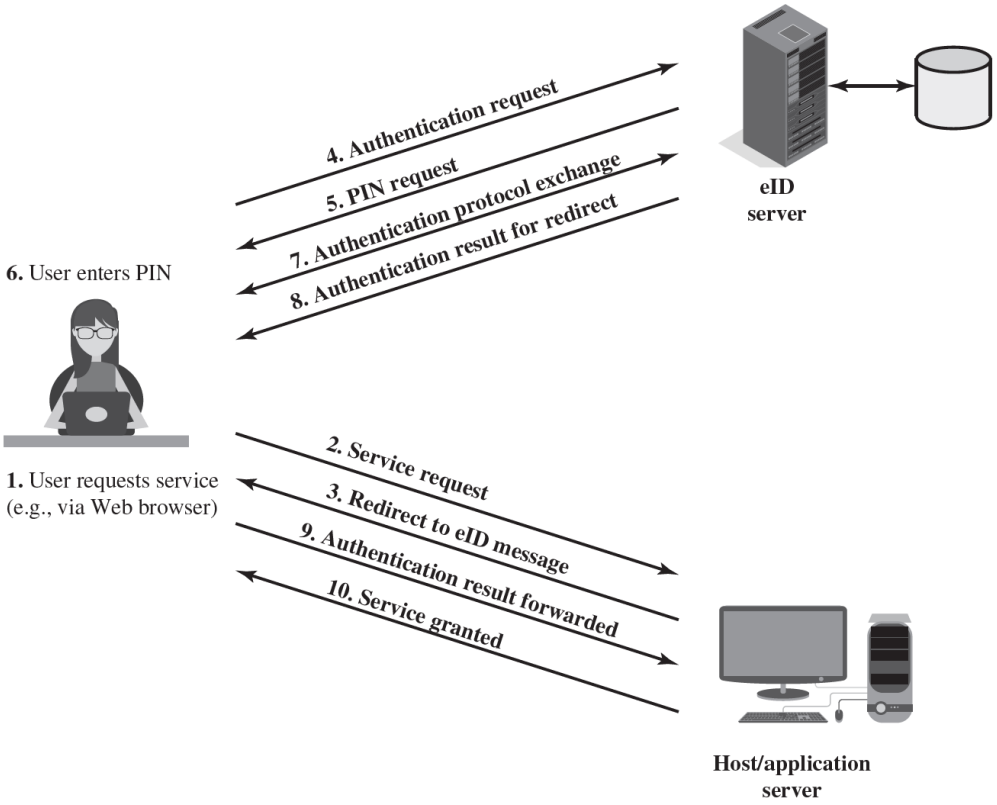


Figure 3.7 **User Authentication with eID**

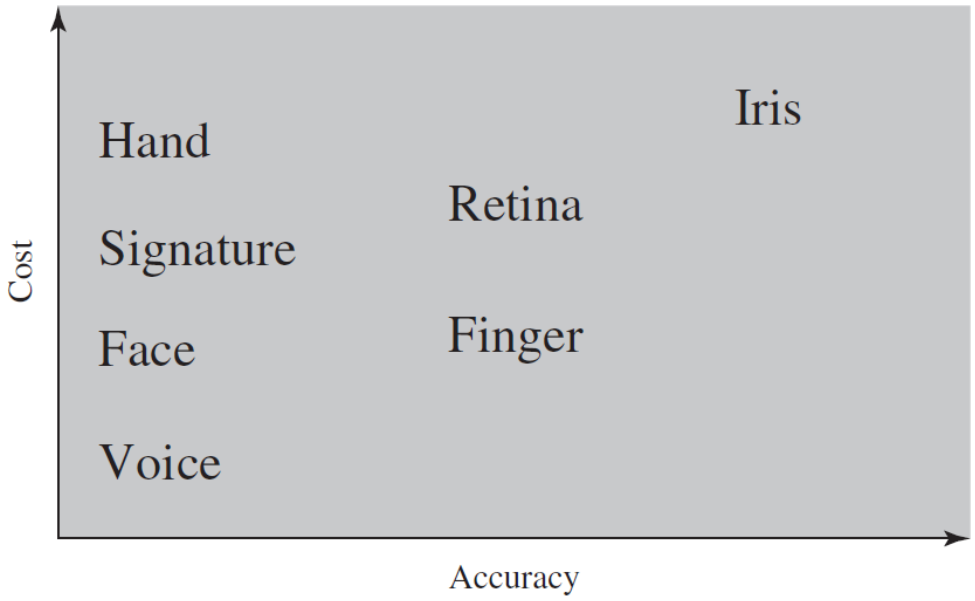
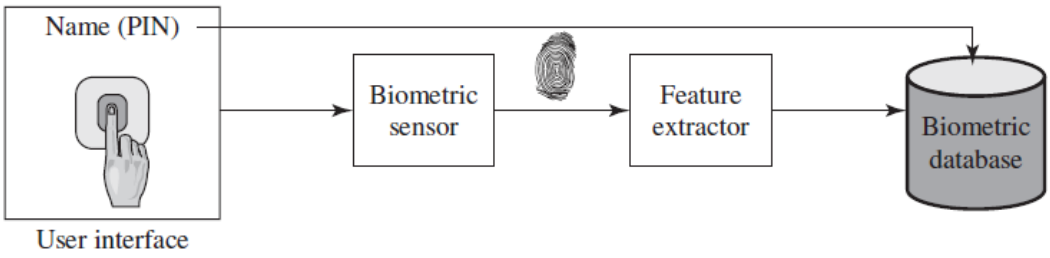
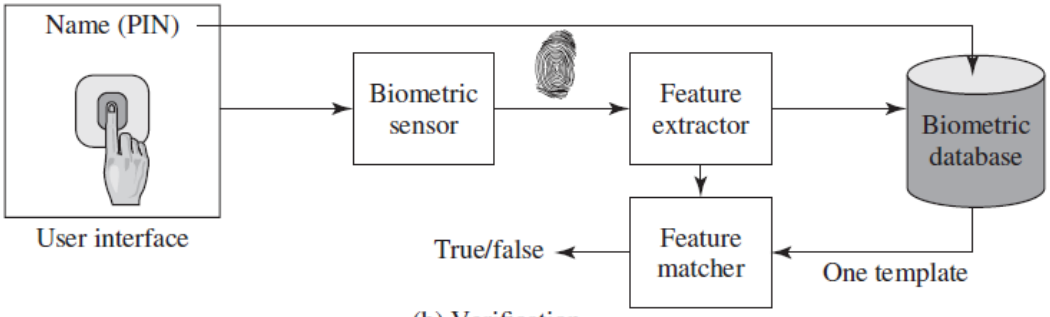


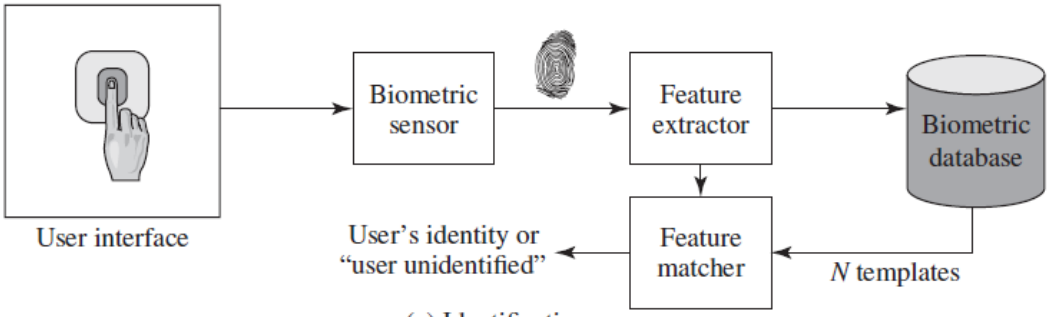
Figure 3.8 Cost Versus Accuracy of Various Biometric Characteristics in User Authentication Schemes



(a) Enrollment



(b) Verification



(c) Identification

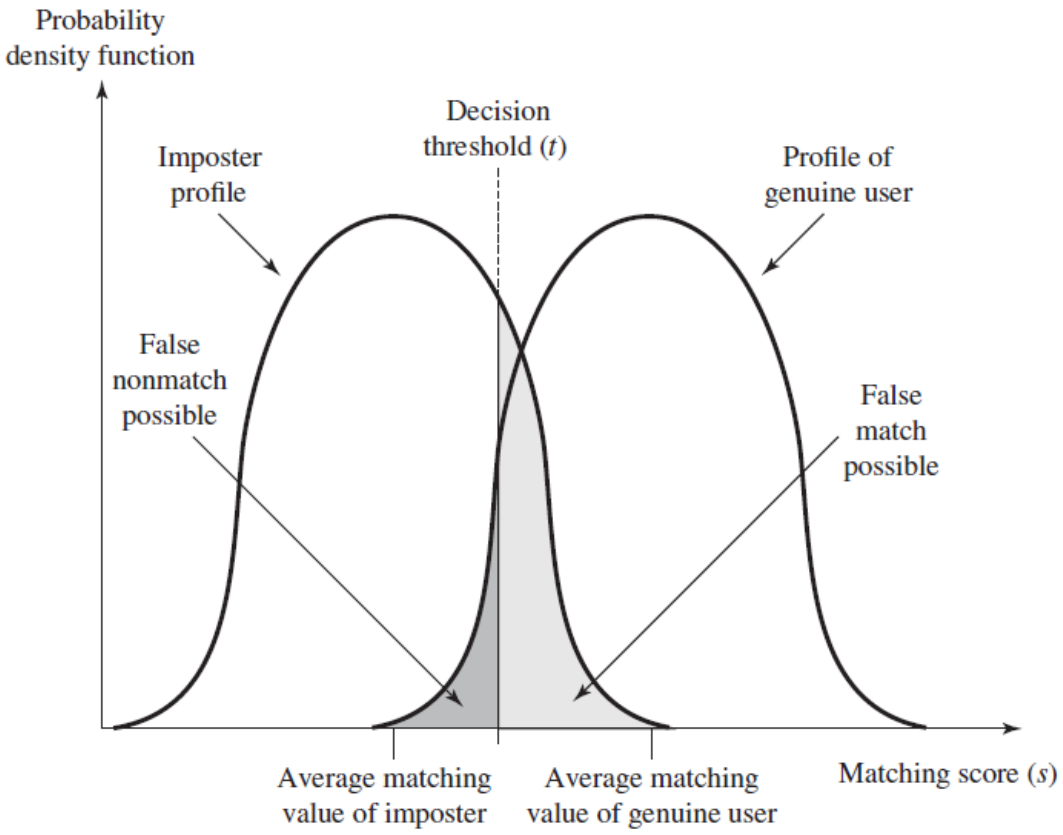


Figure 3.10 Profiles of a Biometric Characteristic of an Imposter and an Authorized User In this depiction, the comparison between the presented feature and a reference feature is reduced to a single numeric value. If the input value (s) is greater than a preassigned threshold (t), a match is declared.

Chap 4

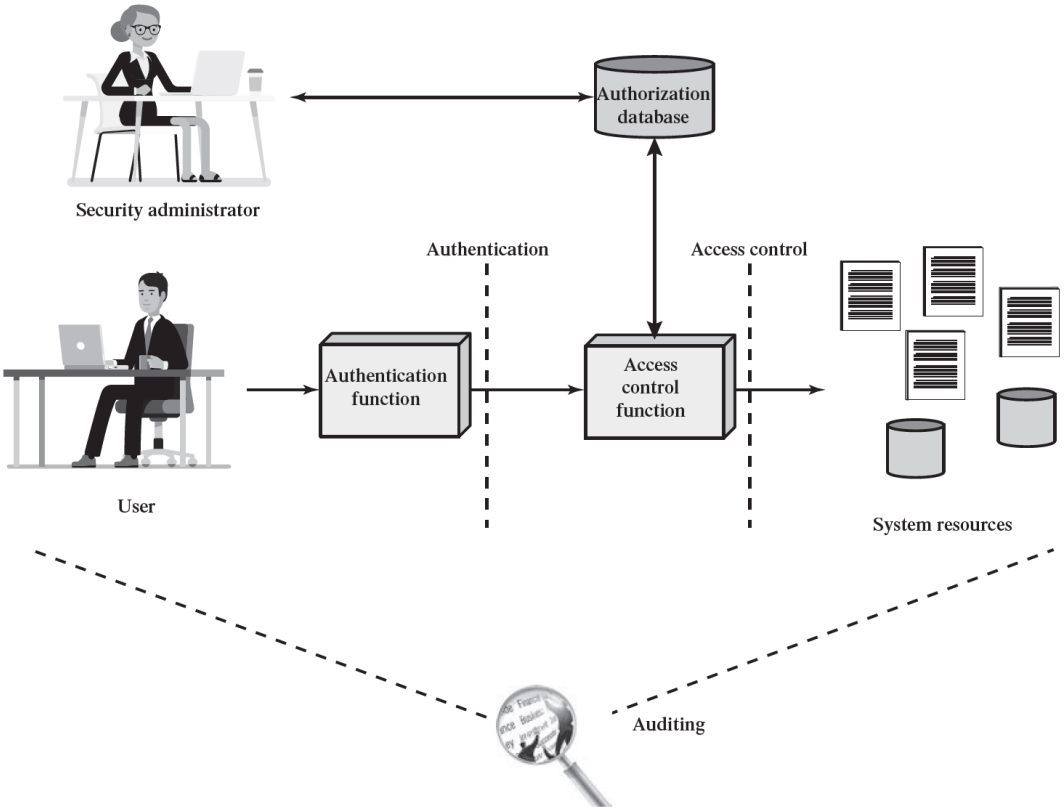


Figure 4.1 **Relationship Among Access Control and Other Security Functions**
Source: Based on [SAND94].

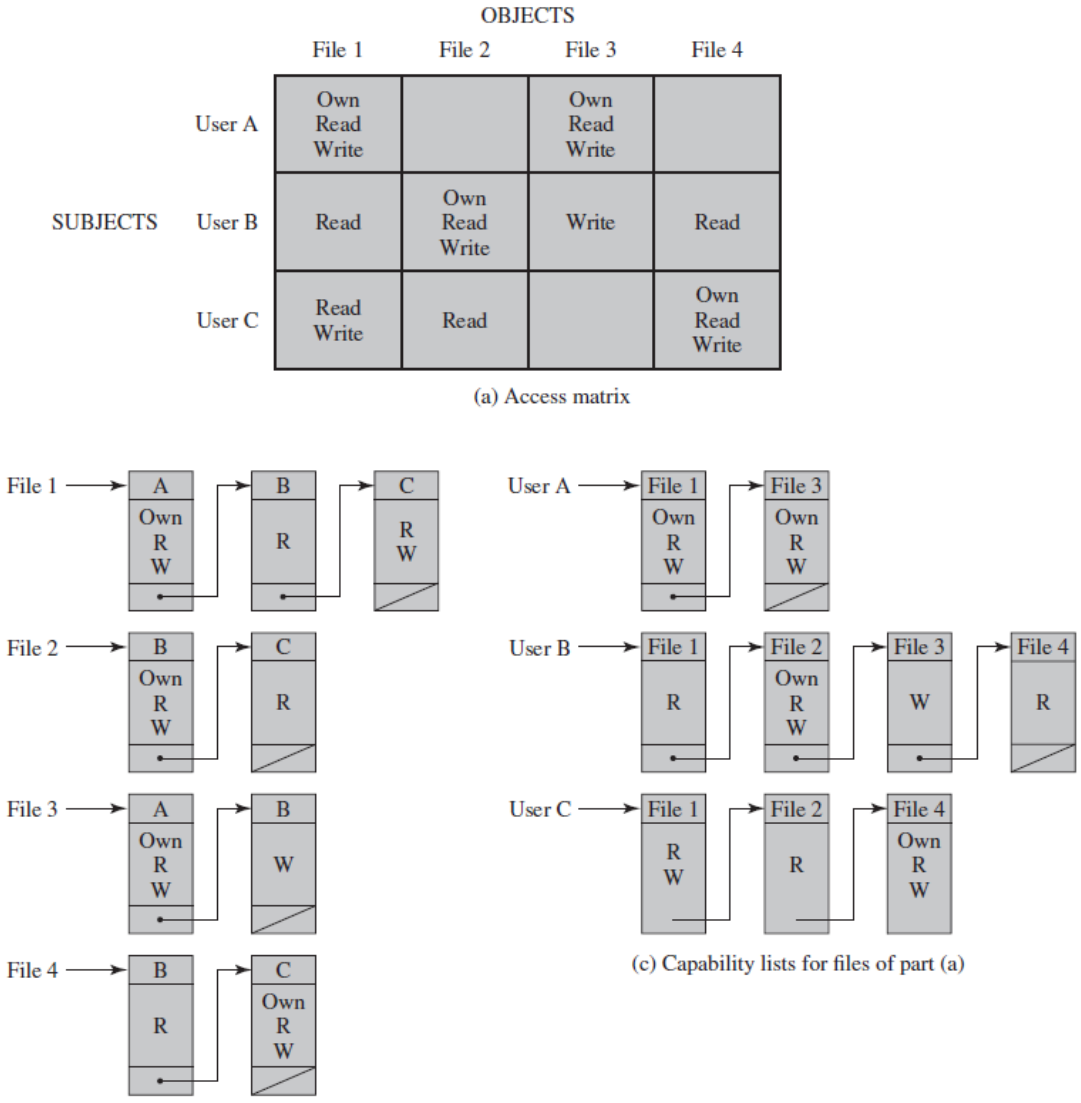


Figure 4.2 **Example of Access Control Structures**

		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**

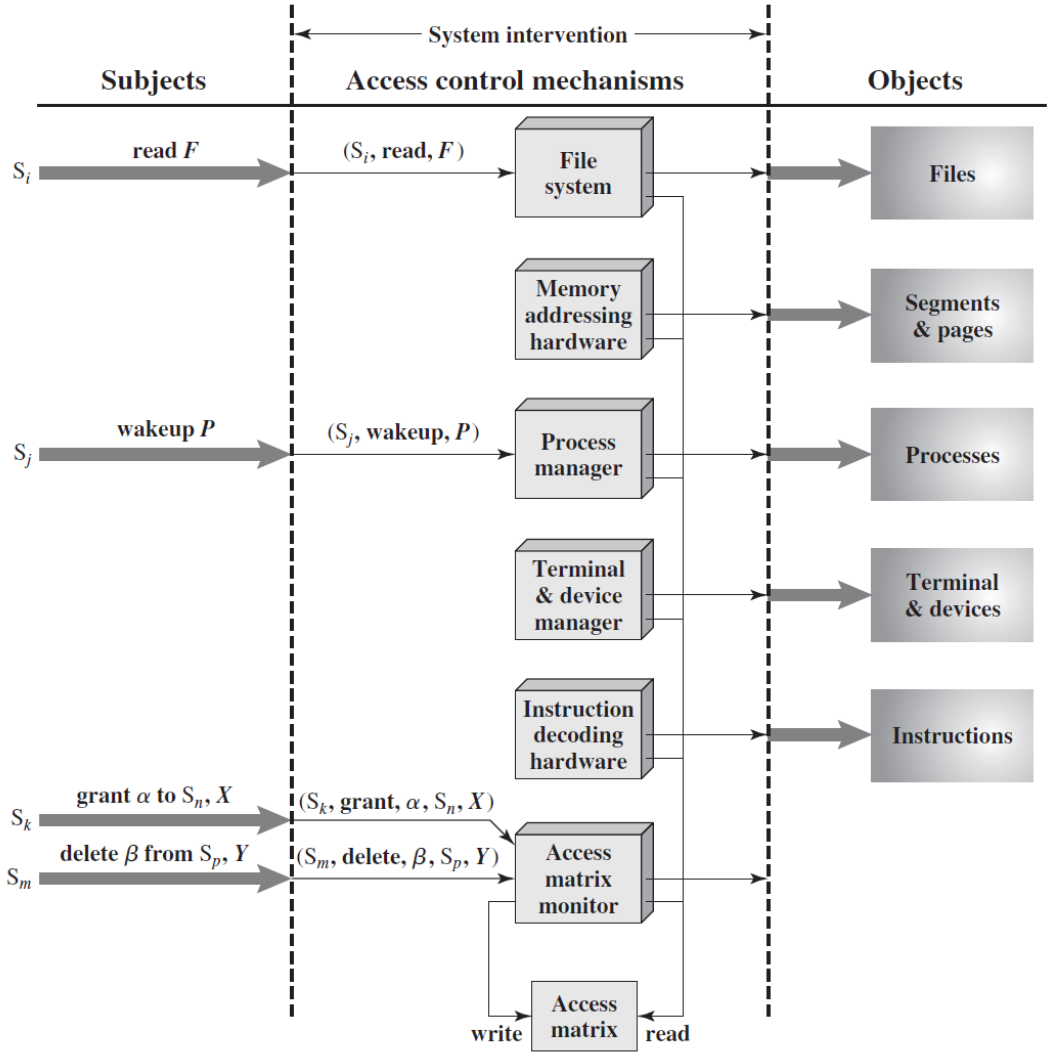
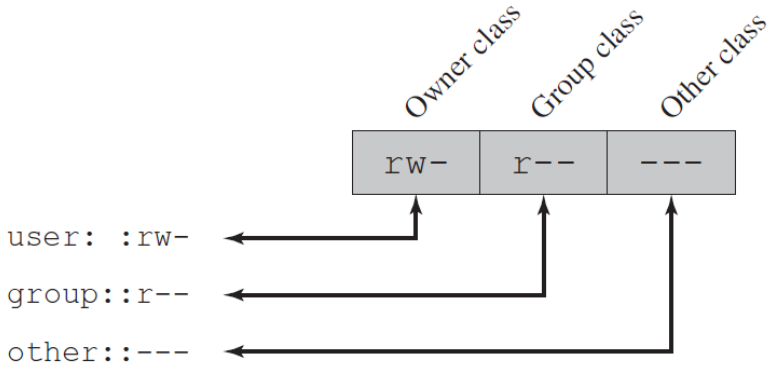
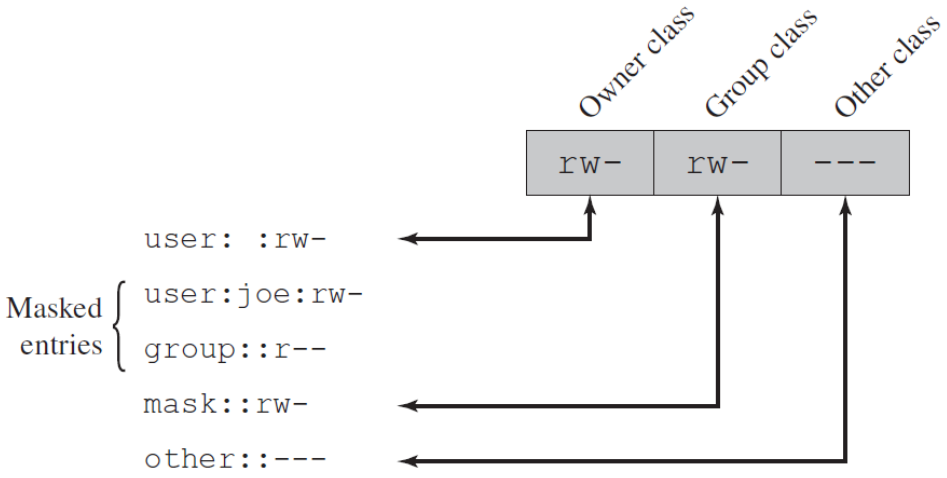


Figure 4.4 **An Organization of the Access Control Function**



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



(b) Extended access control list

Figure 4.5 **UNIX File Access Control**

		OBJECTS							
		R_1	R_2	R_n	F_1	F_2	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			

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

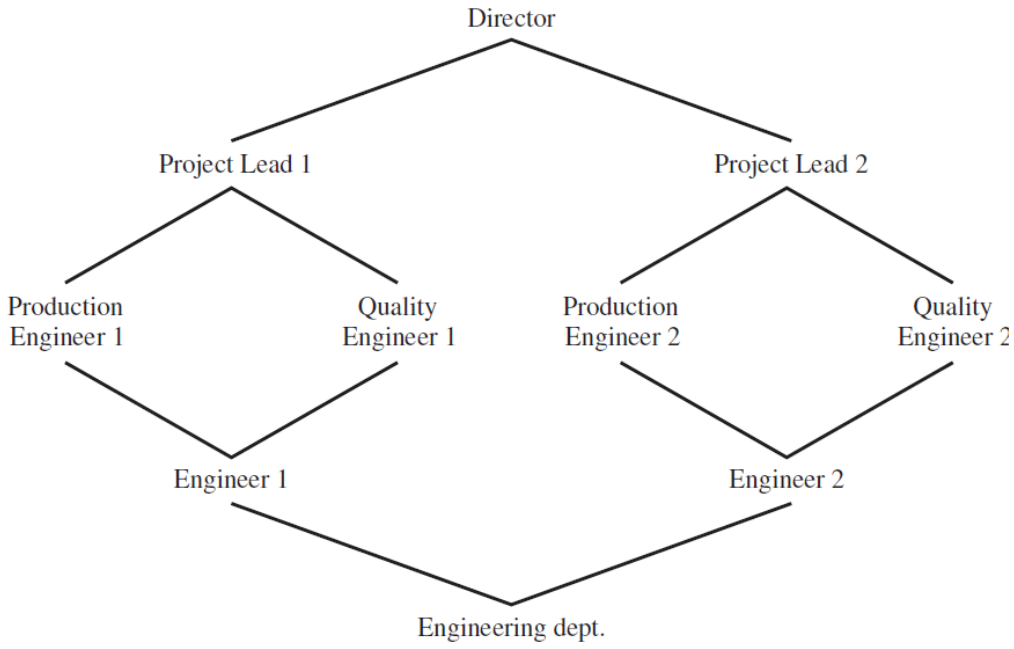


Figure 4.9 **Example of Role Hierarchy**

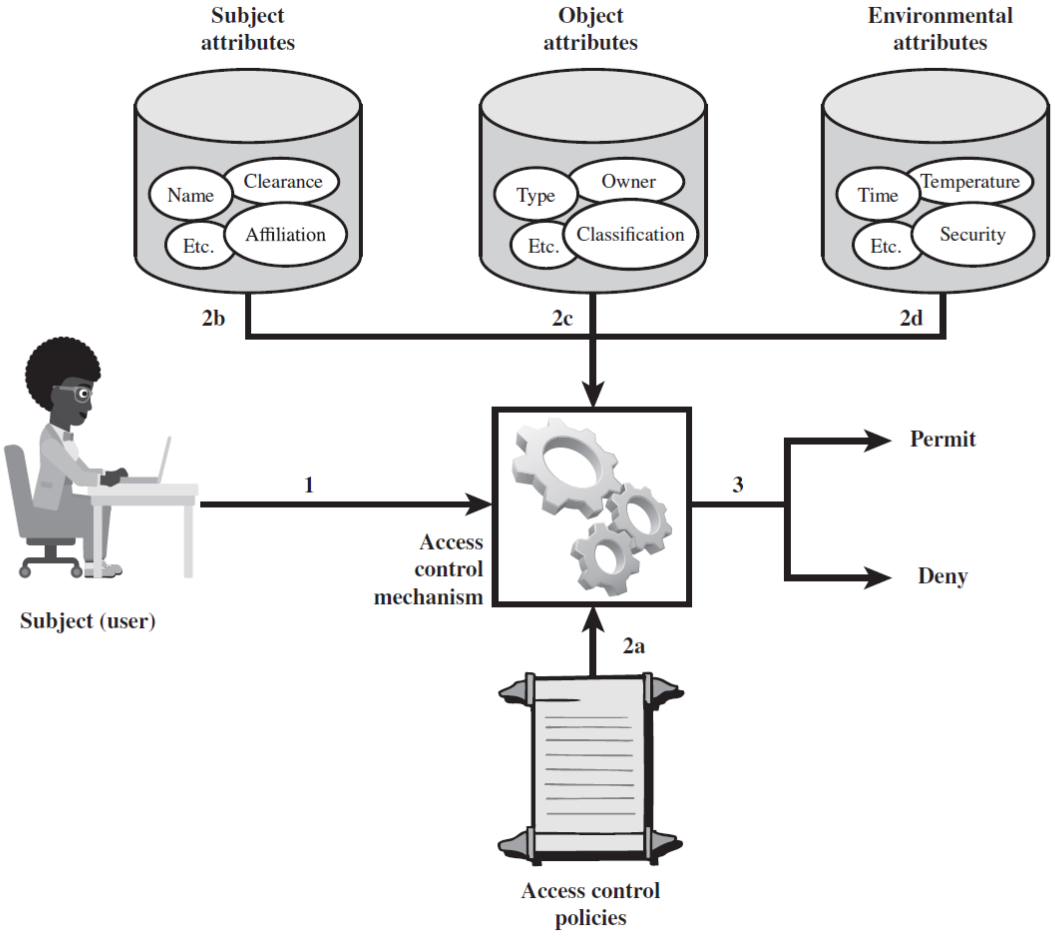
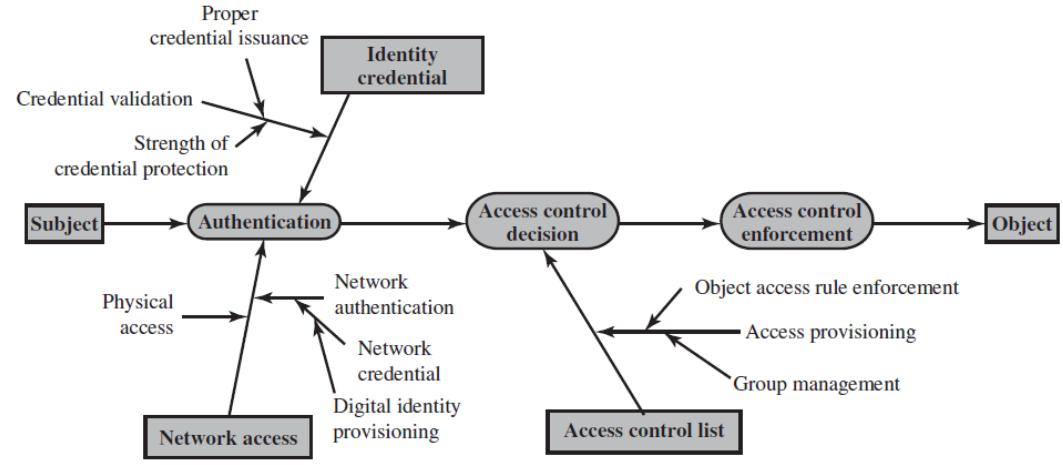
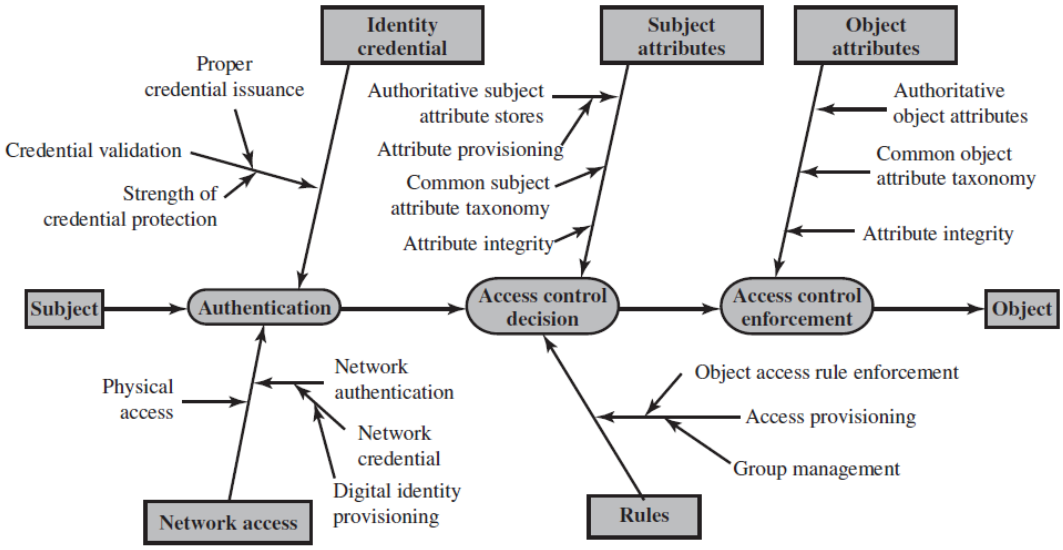


Figure 4.10 **ABAC Scenario**



(a) ACL Trust Chain



(b) ABAC Trust Chain

Figure 4.11 ACL and ABAC Trust Relationships

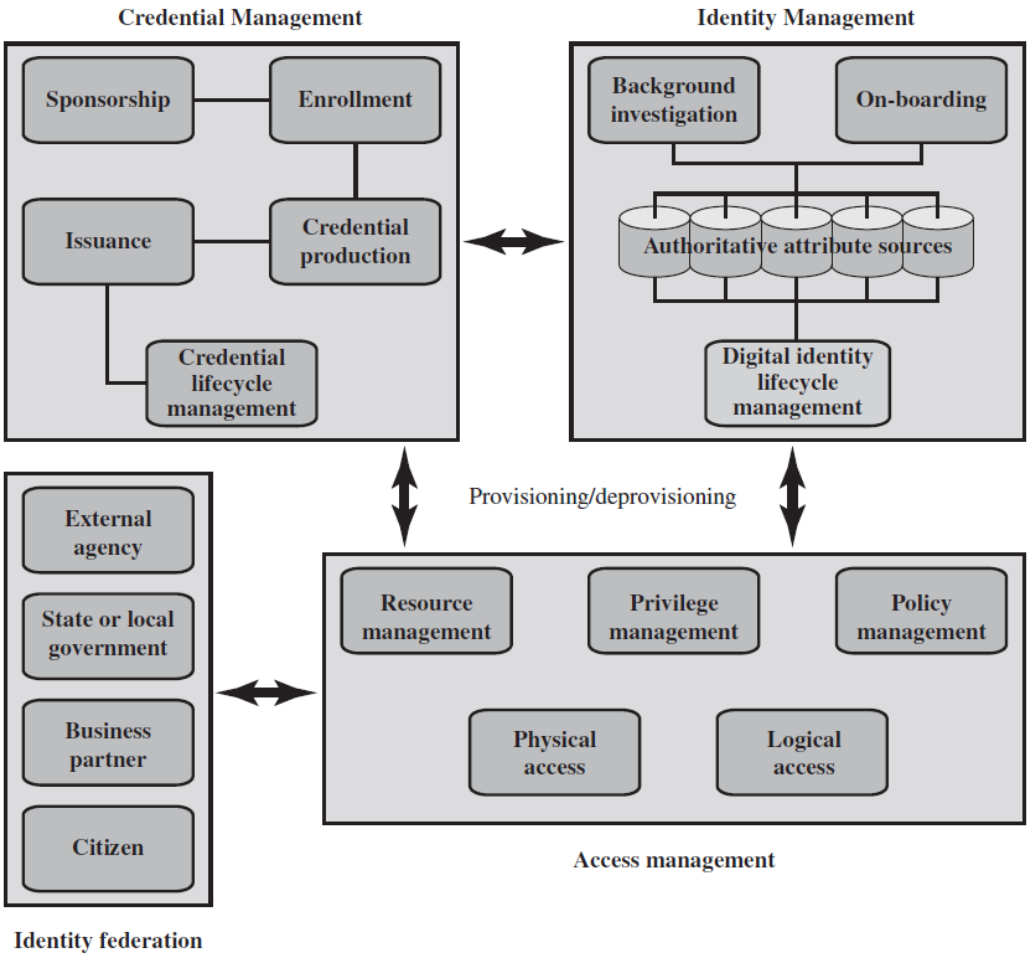


Figure 4.12 **Identity, Credential, and Access Management (ICAM)**

Chap 5

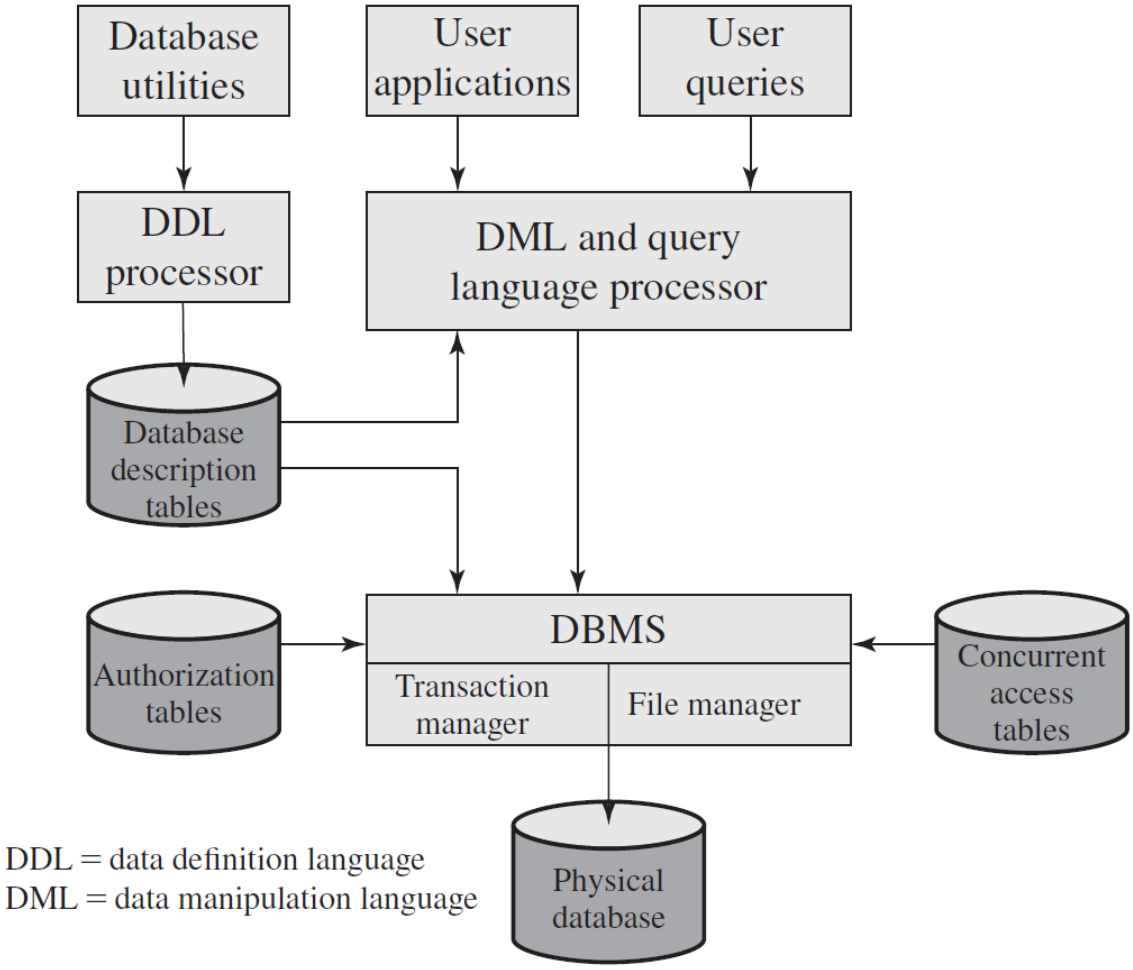


Figure 5.1 **DBMS Architecture**

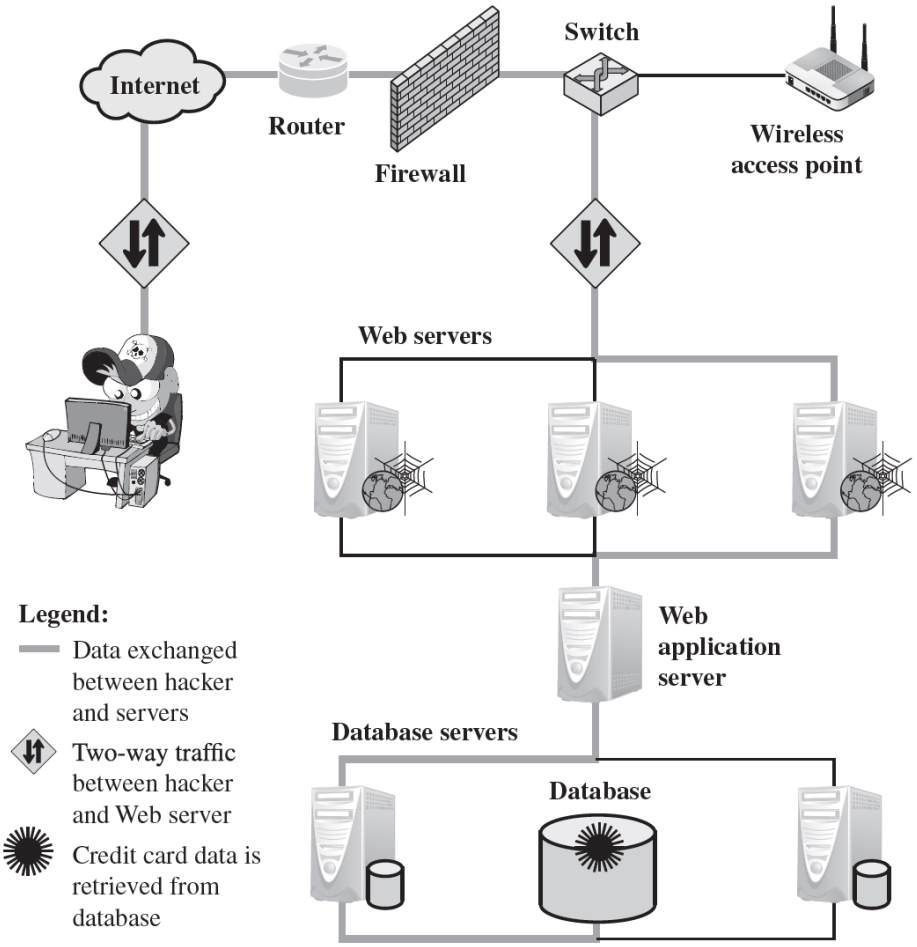


Figure 5.5 **Typical SQL Injection Attack**

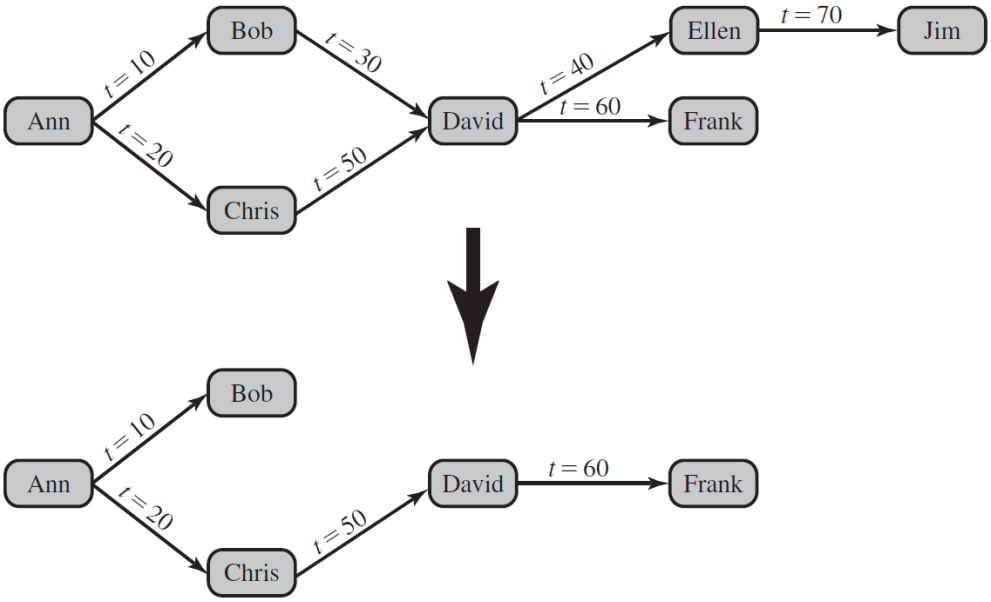


Figure 5.6 **Bob Revokes Privilege from David**

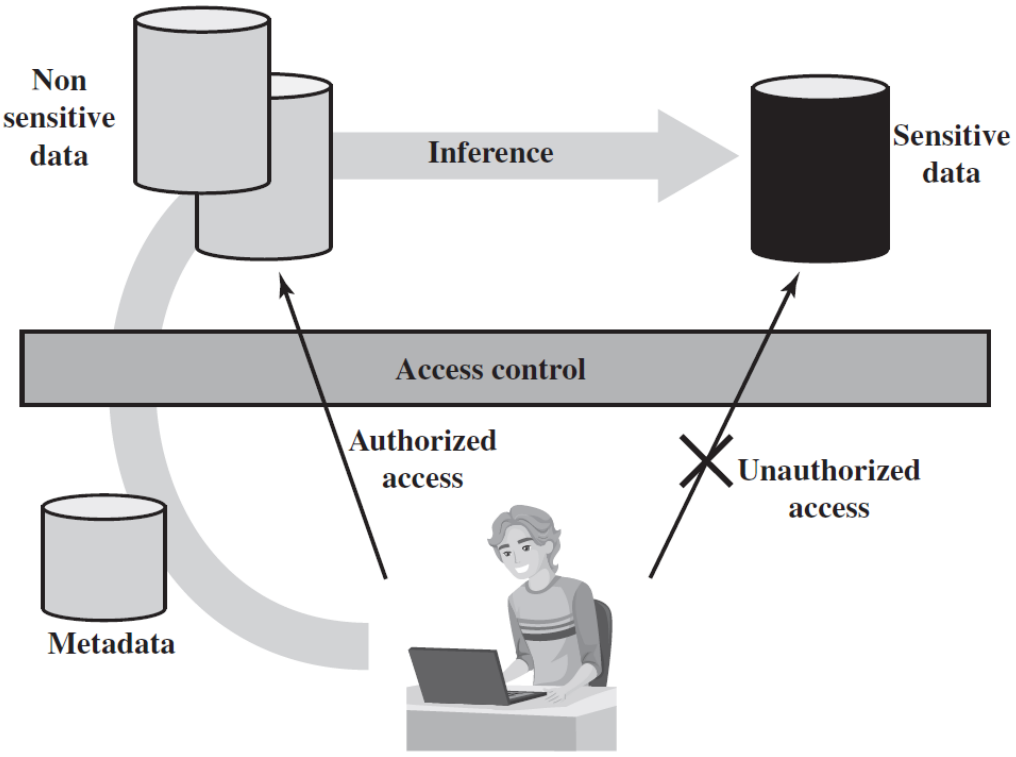


Figure 5.7 **Indirect Information Access via Inference Channel**

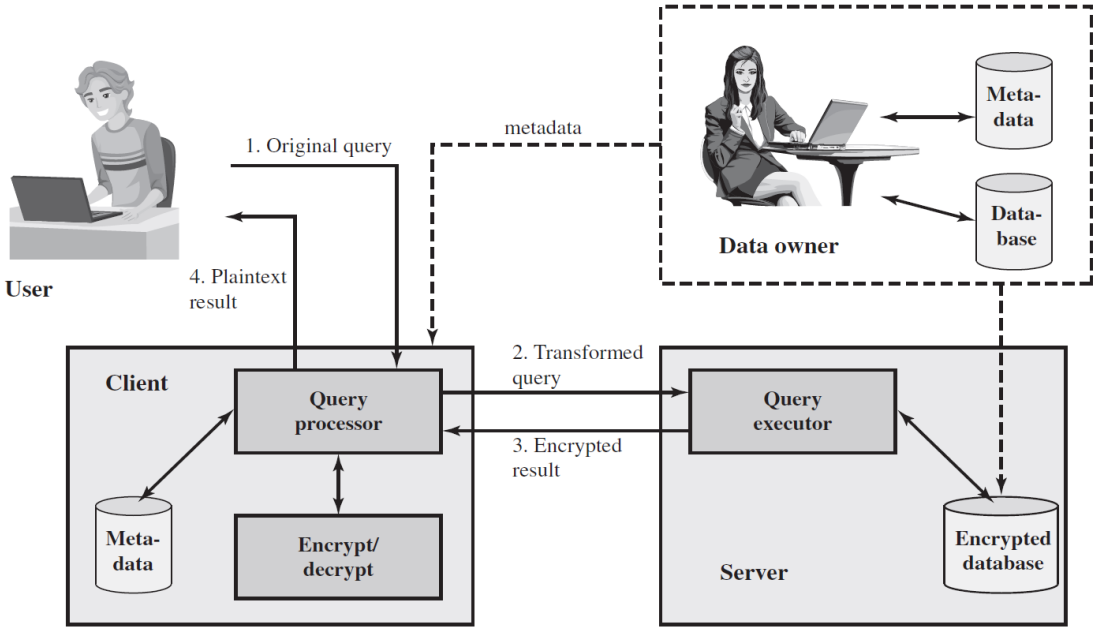


Figure 5.9 **A Database Encryption Scheme**

Chap 6

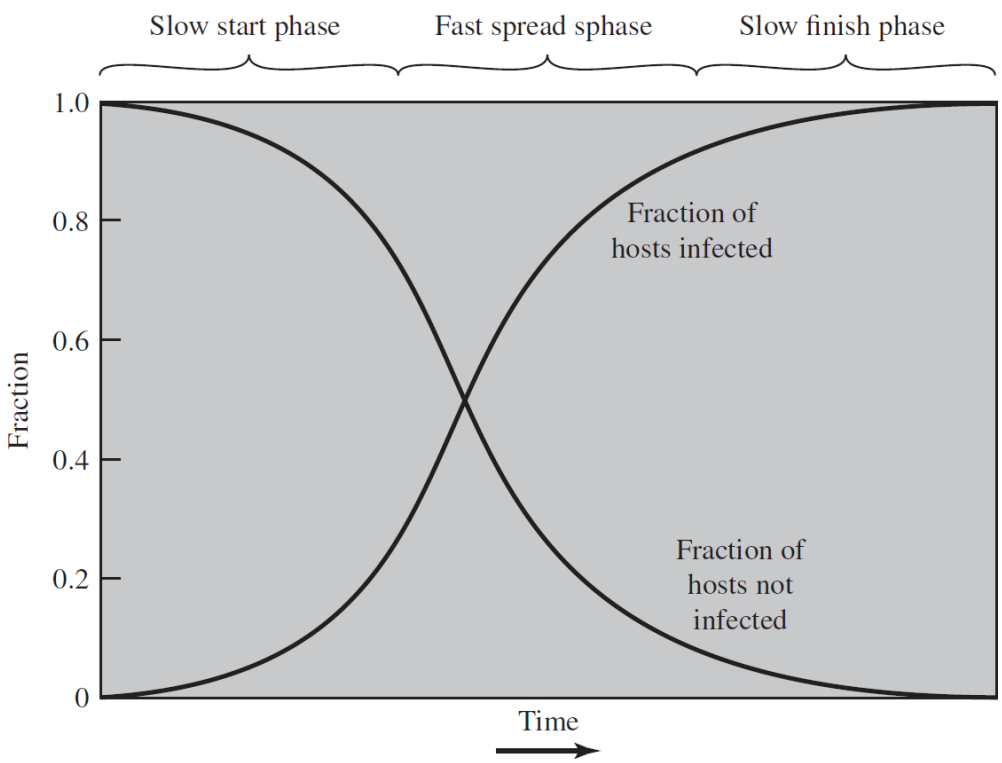


Figure 6.2 **Worm Propagation Model**

Chap 8

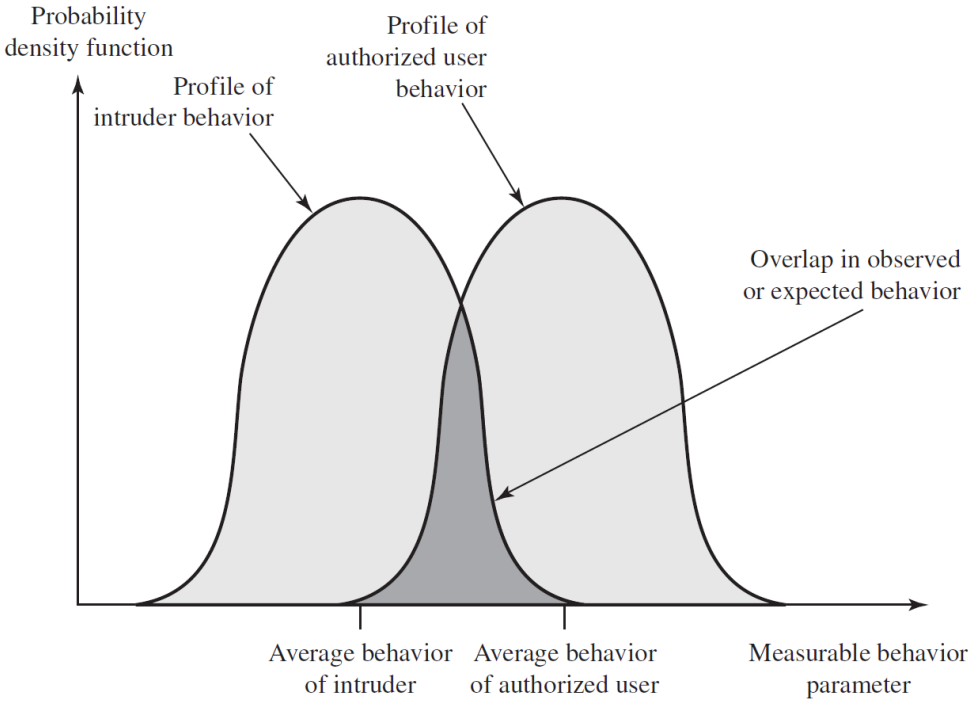


Figure 8.1 Profiles of Behavior of Intruders and Authorized Users

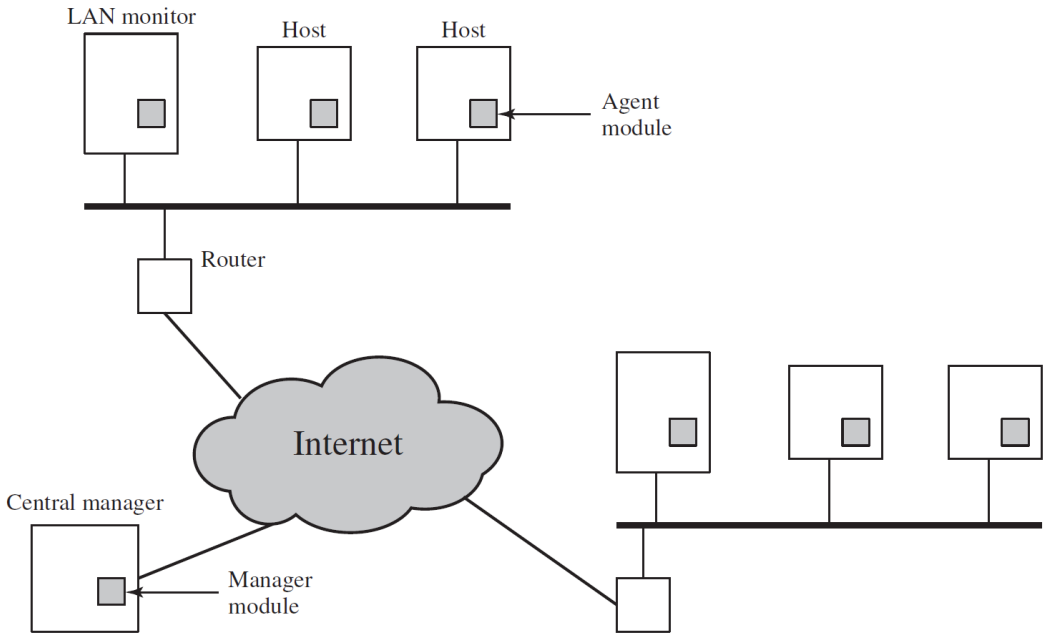


Figure 8.2 Architecture for Distributed Intrusion Detection

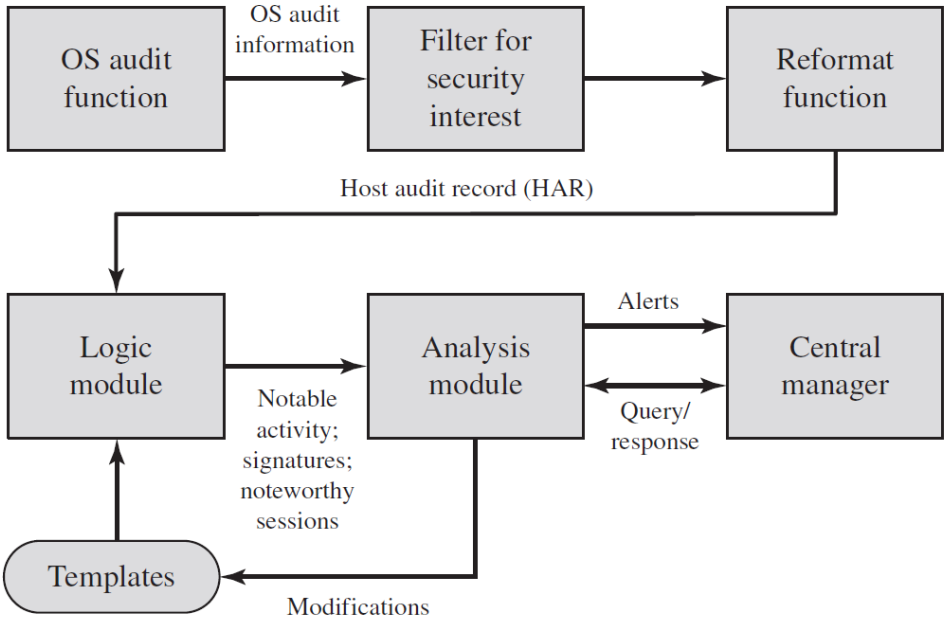


Figure 8.3 Agent Architecture

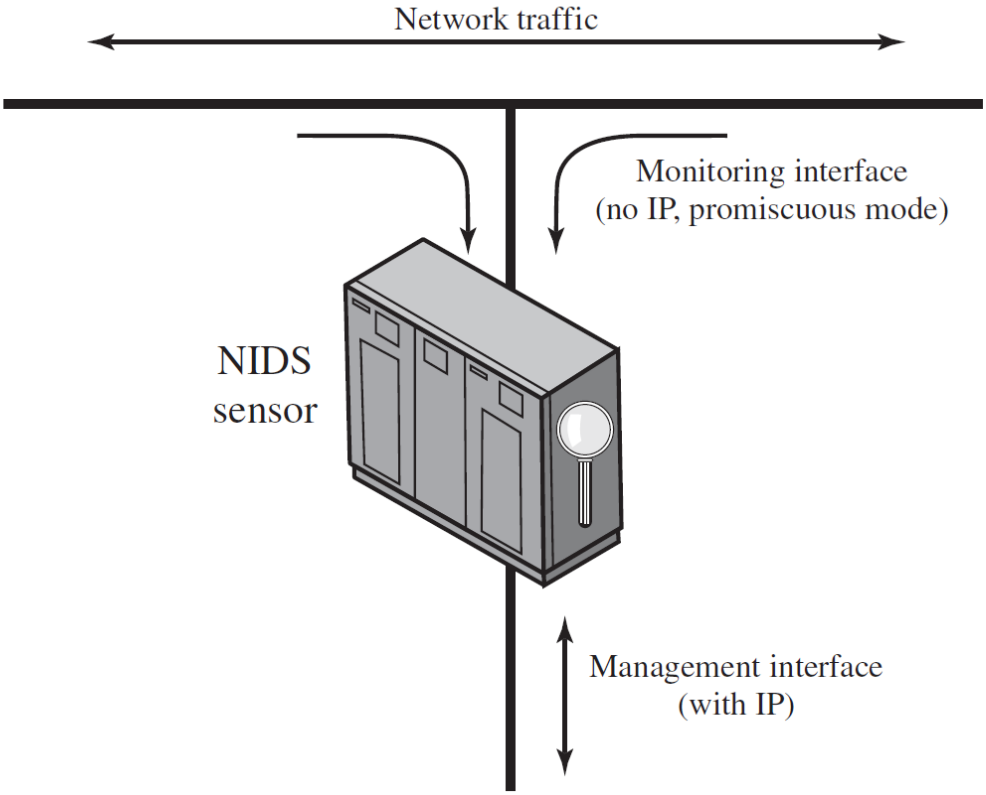
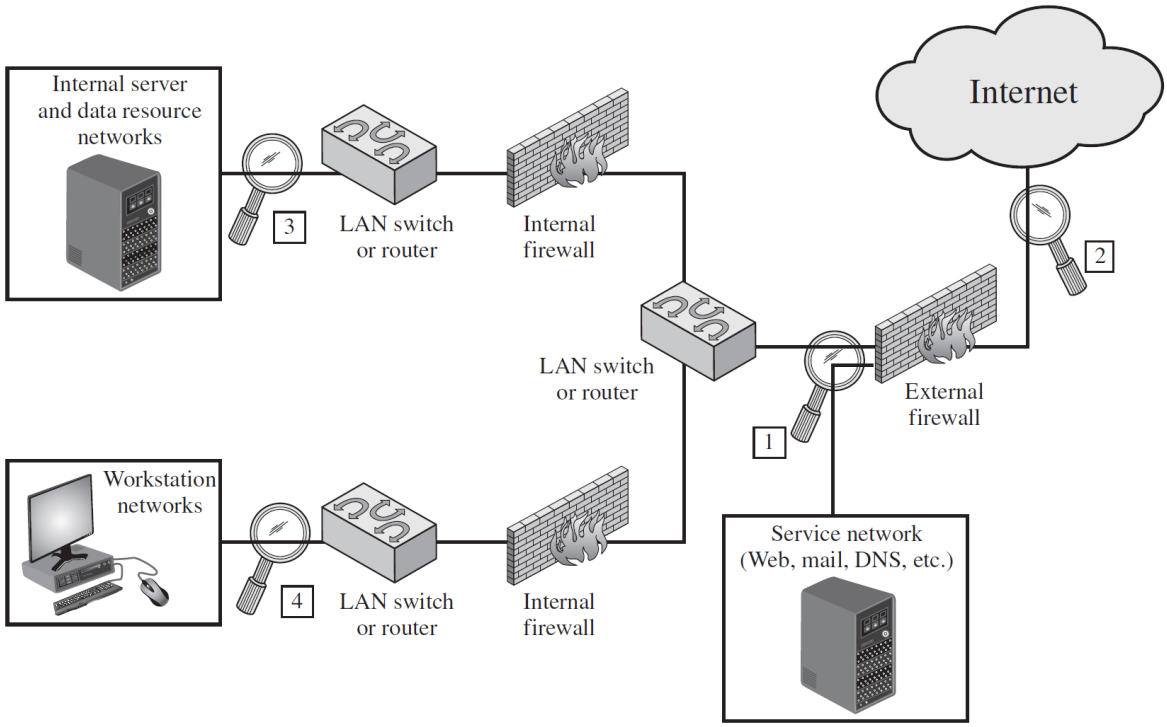
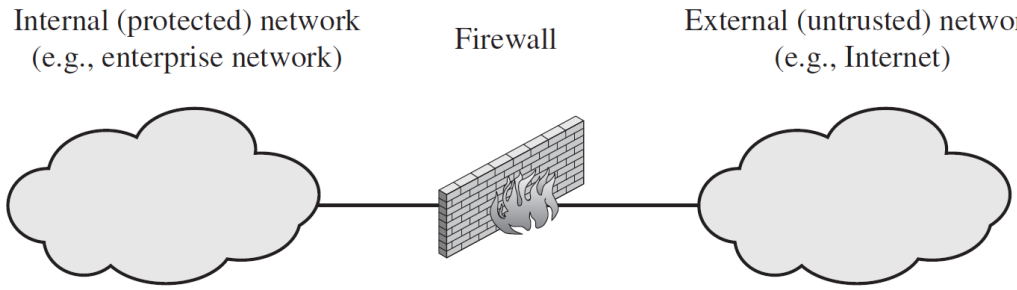


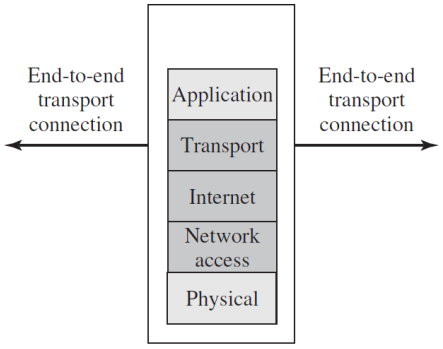
Figure 8.4 Passive NIDS Sensor

Source: Based on [CREM06].

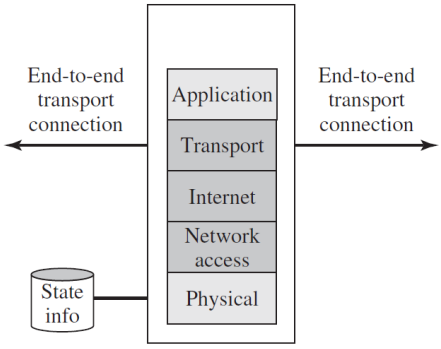




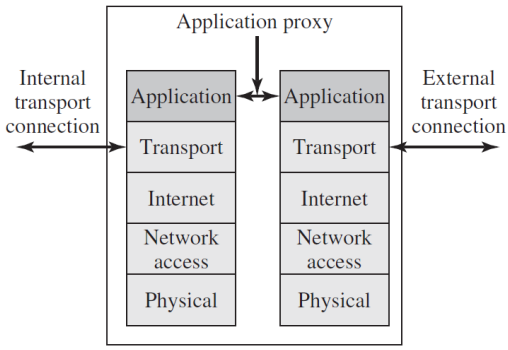
(a) General model



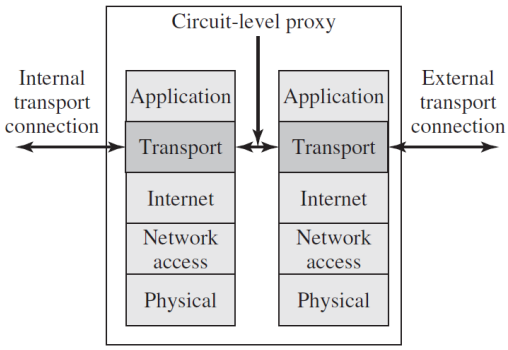
(b) Packet filtering firewall



(c) Stateful inspection firewall



(d) Application proxy firewall



(e) Circuit-level proxy firewall

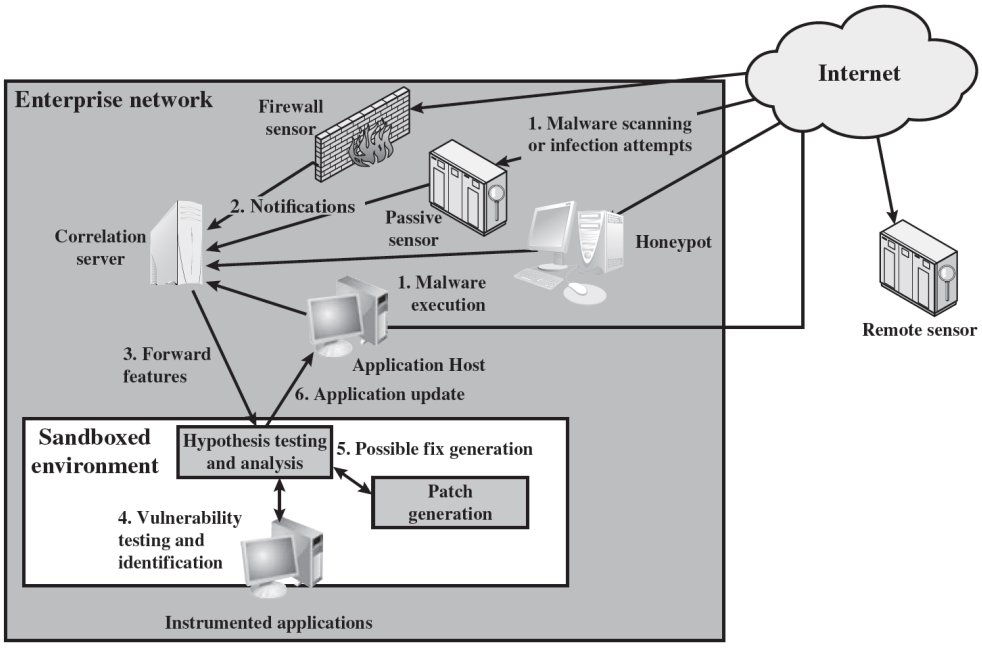


Figure 9.5 **Placement of Malware Monitors**
Source: Based on [SIDI05]. Sidiroglou, S., and Keromytis, A. "Countering Network Worms Through Automatic Patch Generation.", Columbia University, Figure 1, page 3, November-December 2005. http://www1.cs.columbia.edu/~angelos/Papers/2005/j6ker3.pdf IEEE.

Chap 14

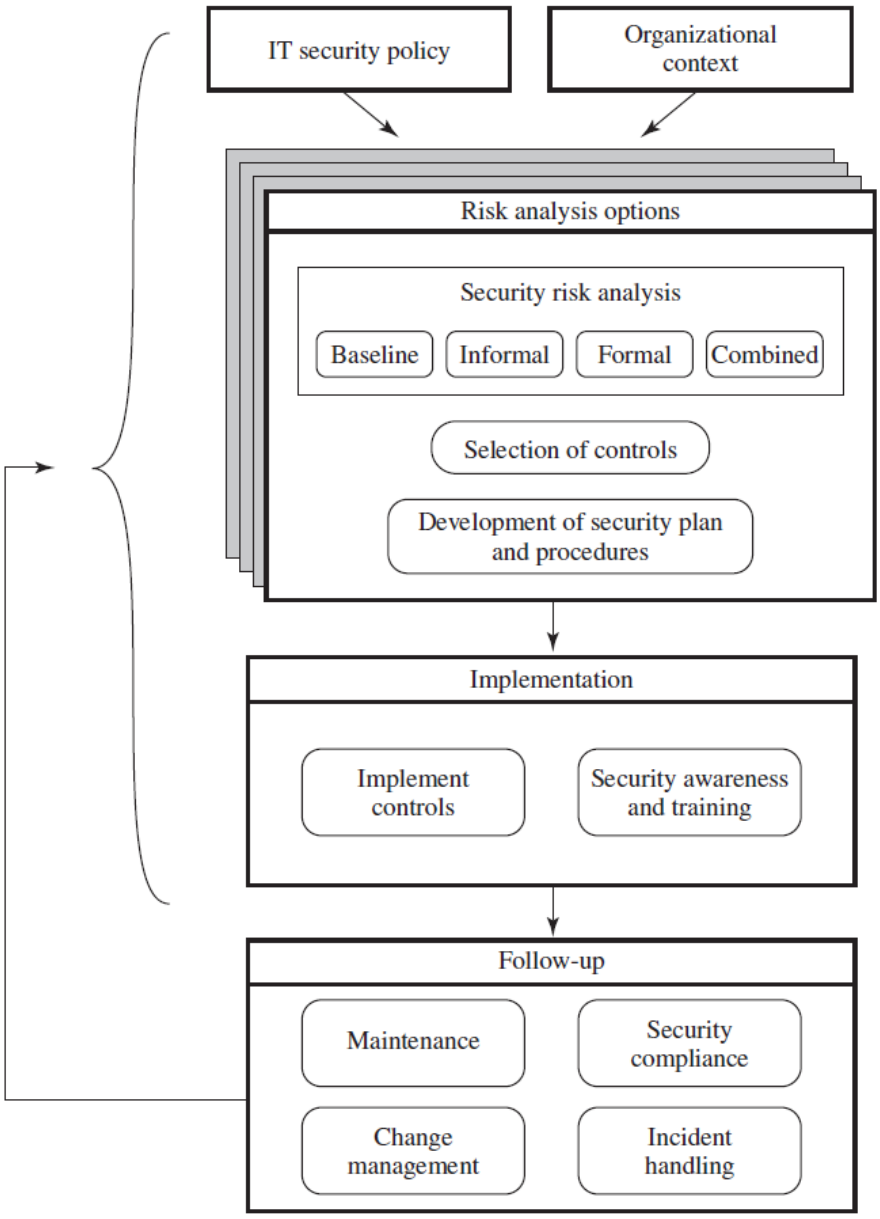


Figure 14.1 Overview of IT Security Management

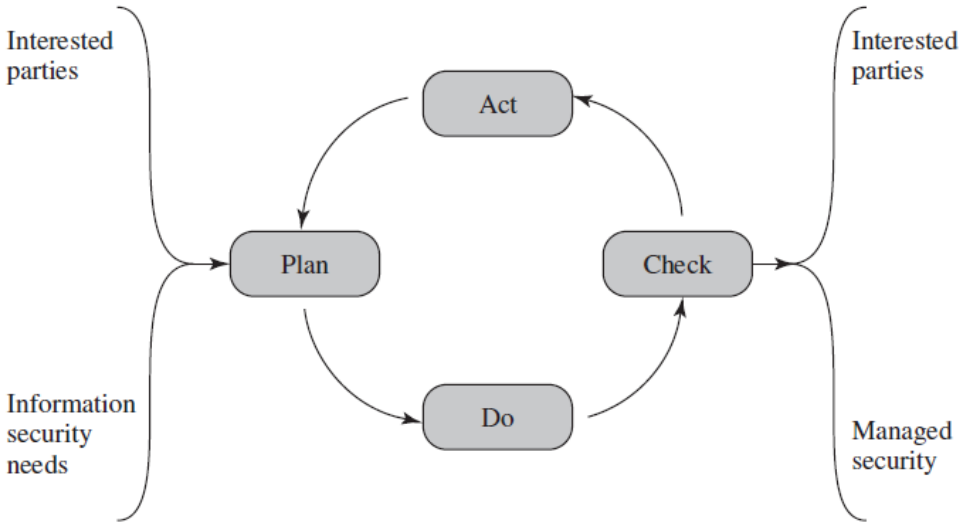


Figure 14.2 **The Plan-Do-Check-Act Process Model**

Plan: Establish security policy, objectives, processes, and procedures; perform risk assessment; develop risk treatment plan with appropriate selection of controls or acceptance of risk.

Do: Implement the risk treatment plan.

Check: Monitor and maintain the risk treatment plan.

Act: Maintain and improve the information security risk management process in response to incidents, review, or identified changes.

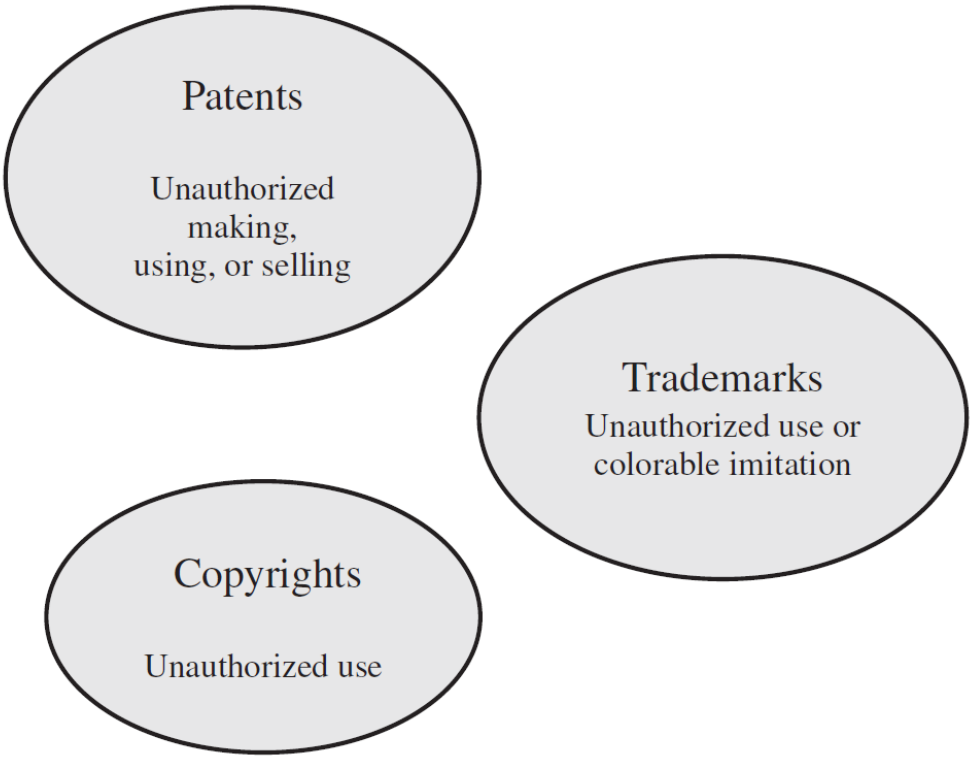


Figure 19.1 Intellectual Property Infringement

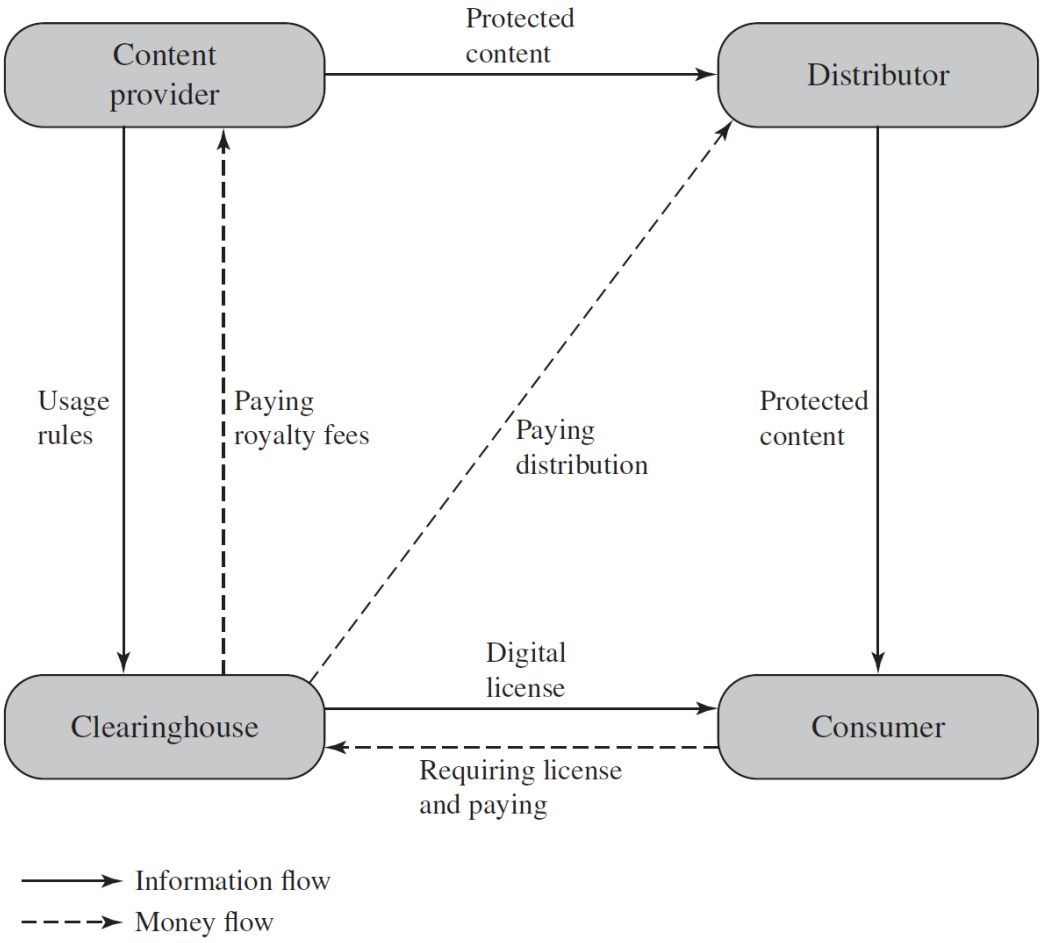


Figure 19.2 **DRM Components**

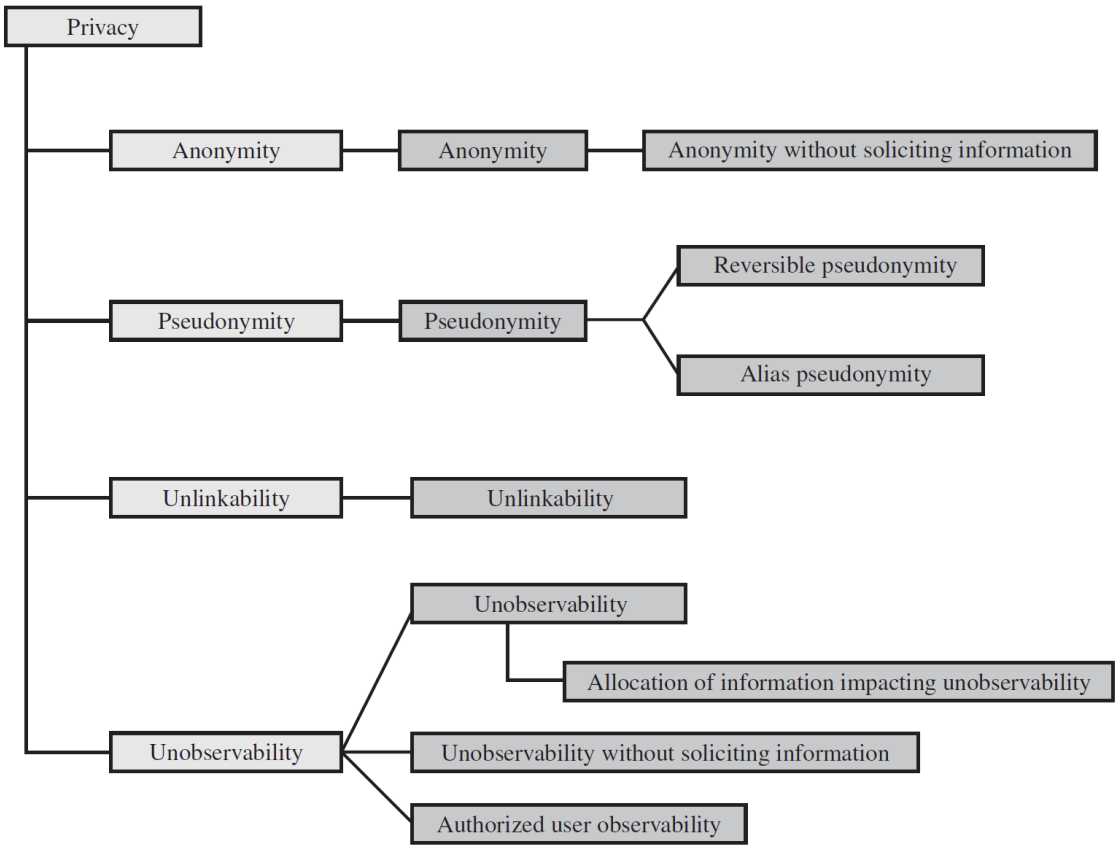


Figure 19.4 **Common Criteria Privacy Class Decomposition**

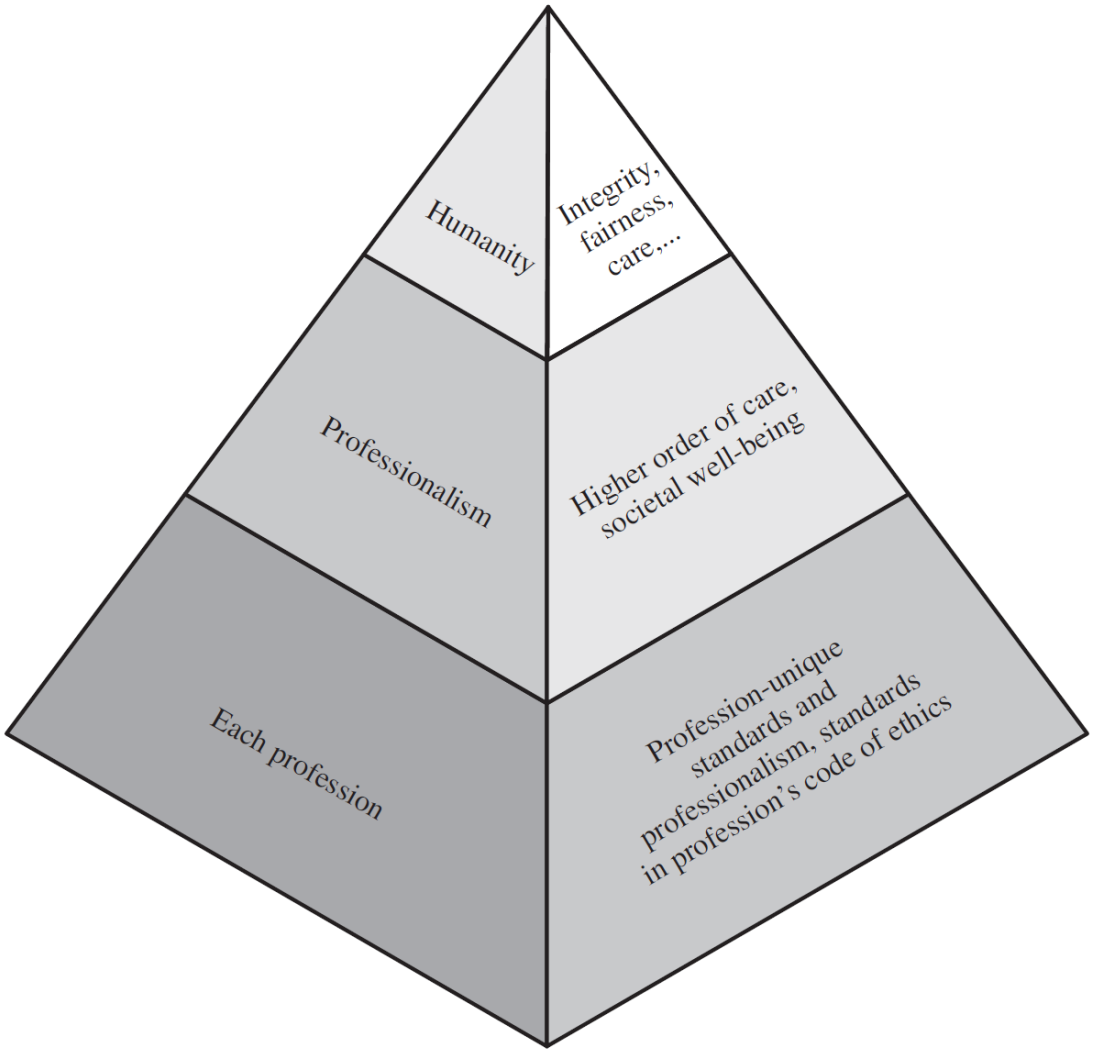


Figure 19.5 **The Ethical Hierarchy**