CSCI 360
Introduction to Operating Systems

Security

Humayun Kabir
Professor, CS, Vancouver Island University, BC, Canada

Outline

- Security Goals and Threats
- Protection Mechanisms
  - Protection Domain
  - Access Control List
  - Capabilities
- Security Models
- Cryptography and Digital Signature
- Authentication

The Security Goals and Threats

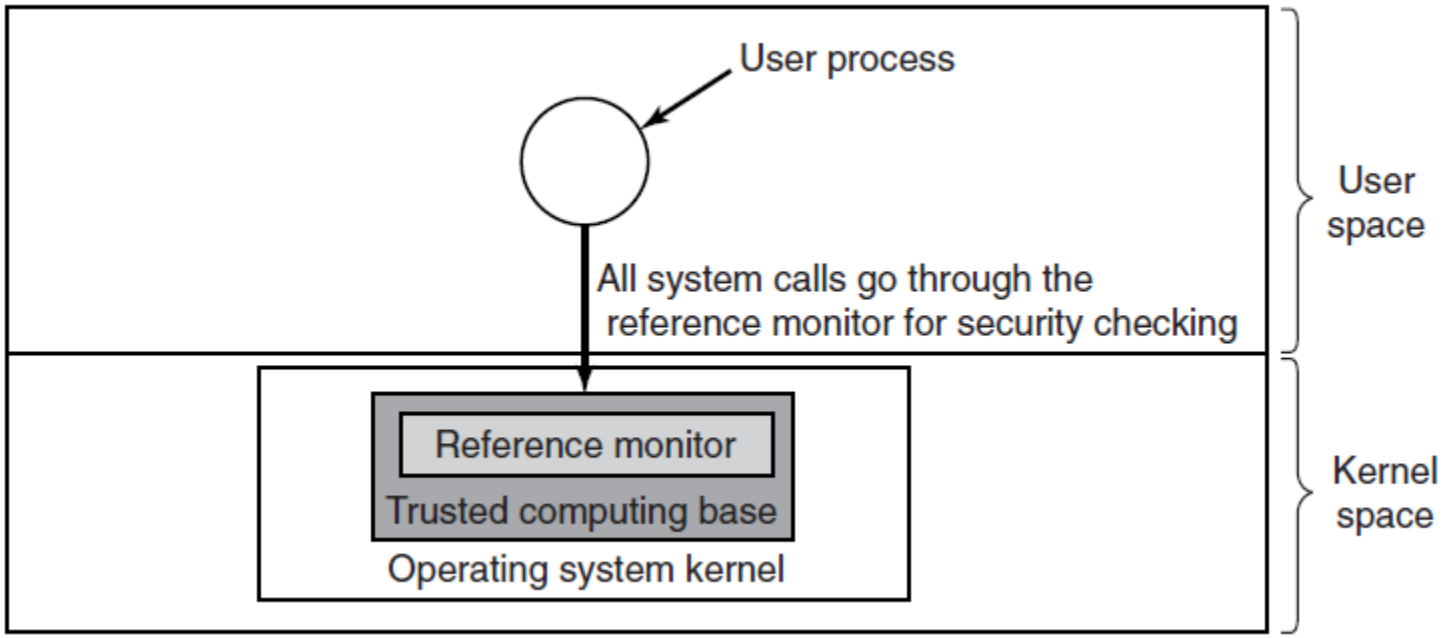
Goal	Threat
Confidentiality	Exposure of data
Integrity	Tampering with data
Availability	Denial of service

Can We Build Secure Systems?

Two questions concerning security:

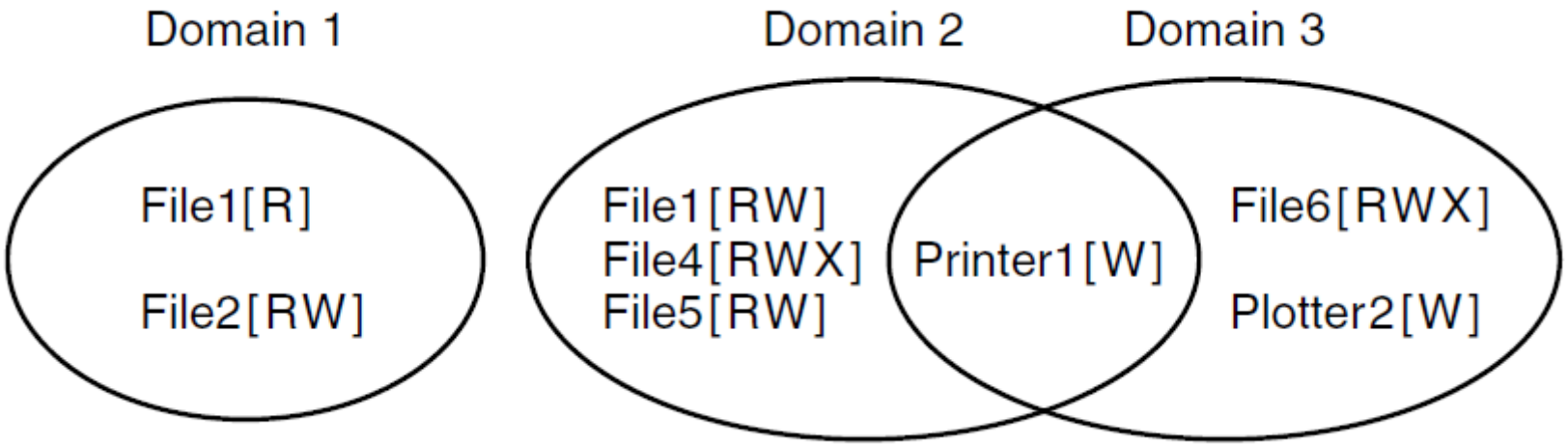
1. Is it possible to build a secure computer system?
2. If so, why is it not done?

Trusted Computing Base



A reference monitor.

Protection Domains



Three protection domains.

Protection Domains

Domain	Object							
	File1	File2	File3	File4	File5	File6	Printer1	Plotter2
1	Read	Read Write						
2			Read	Read Write Execute	Read Write		Write	
3						Read Write Execute	Write	Write

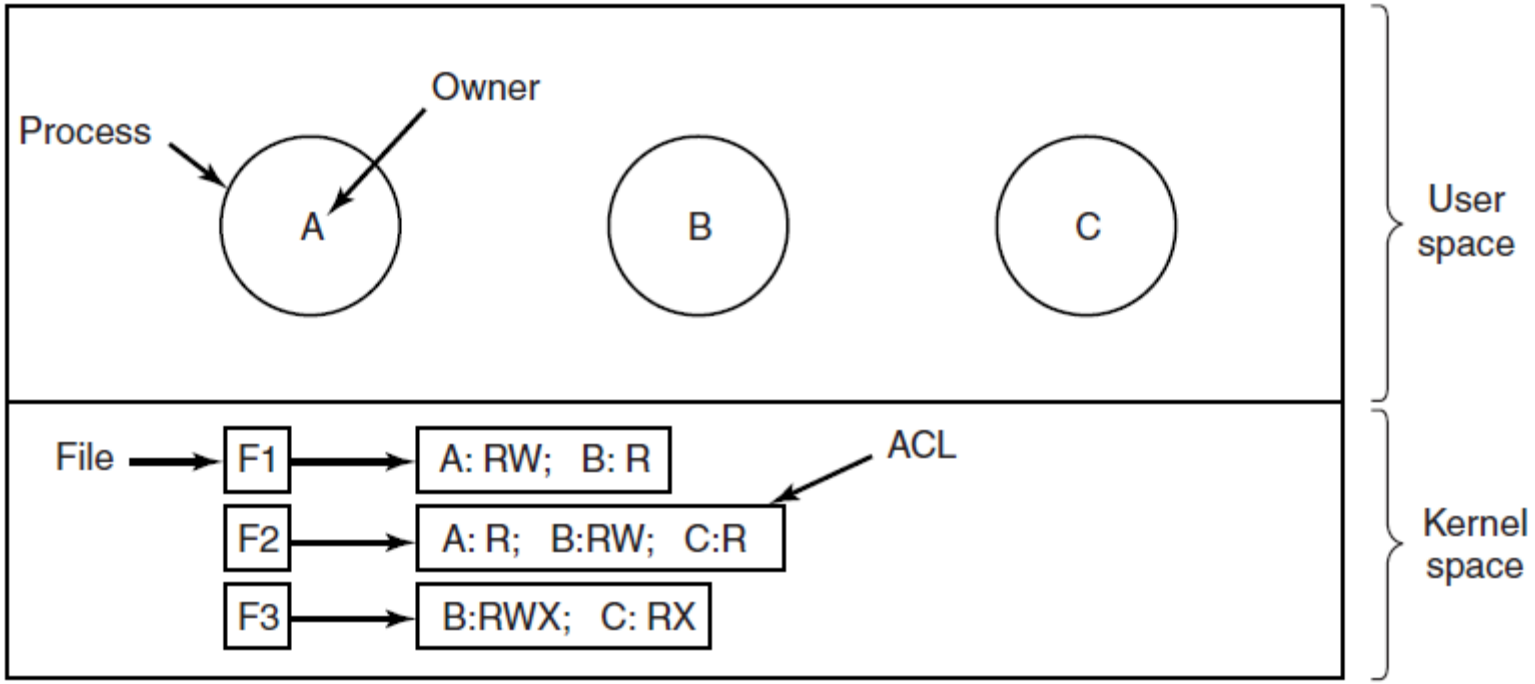
A protection matrix.

Protection Domains

Domain	Object									
	File1	File2	File3	File4	File5	File6	Printer1	Plotter2	Domain1	Domain2	Domain3
1	Read	Read Write								Enter	
2			Read	Read Write Execute	Read Write		Write				
3						Read Write Execute	Write	Write			

A protection matrix with domains as objects.

Access Control Lists



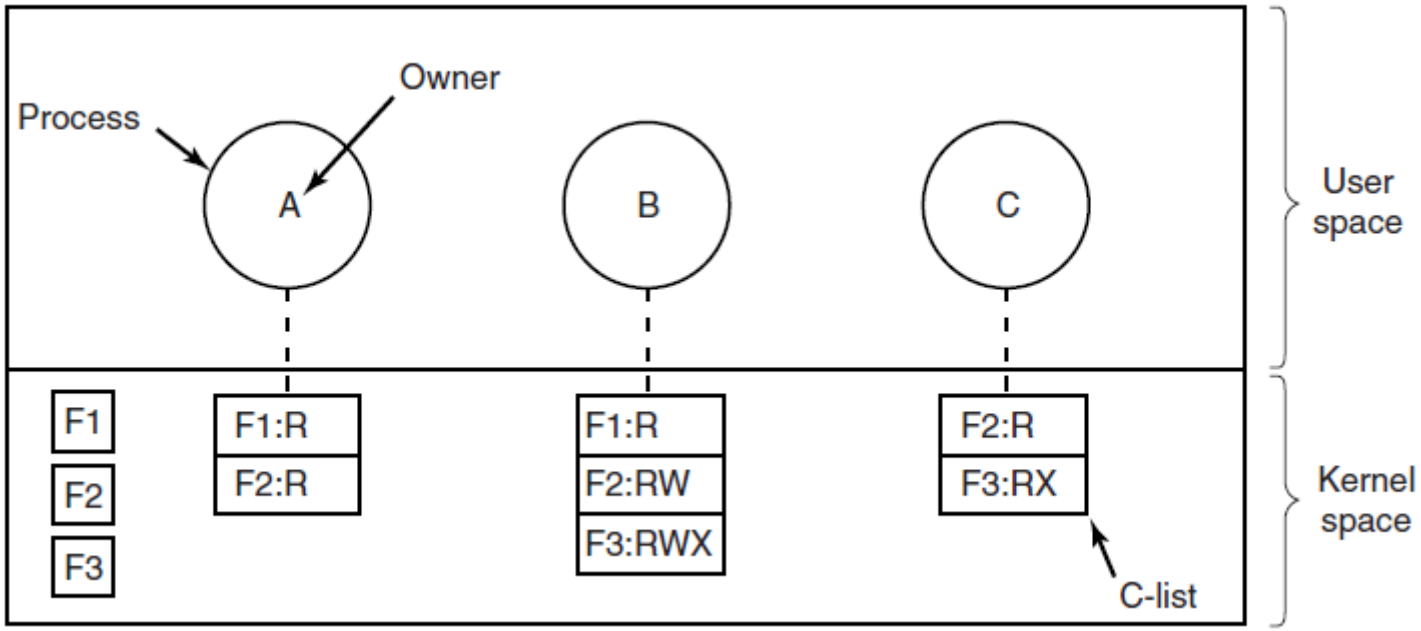
Use of access control lists to manage file access.

Access Control Lists

File	Access control list
Password	tana, sysadm: RW
Pigeon_data	bill, pigfan: RW; tana, pigfan: RW; ...

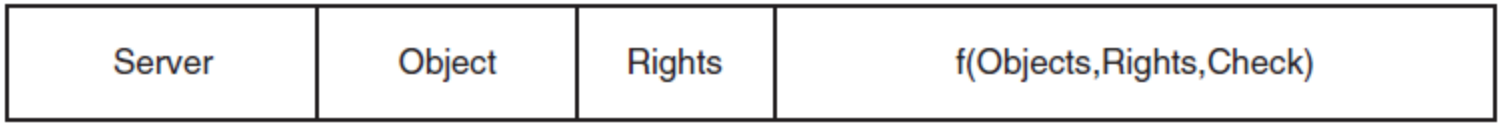
Two access control lists.

Capabilities



When capabilities are used, each process has a capability list.

Capabilities



A cryptographically protected capability.

Capabilities

Examples of generic rights:

1. Copy capability: create new capability for same object.
2. Copy object: create duplicate object with new capability.
3. Remove capability: delete entry from C-list; object unaffected.
4. Destroy object: permanently remove object and capability.

Formal Models of Secure Systems

	Objects		
	Compiler	Mailbox 7	Secret
Eric	Read Execute		
Henry	Read Execute	Read Write	
Robert	Read Execute		Read Write

(a)

	Objects		
	Compiler	Mailbox 7	Secret
Eric	Read Execute		
Henry	Read Execute	Read Write	
Robert	Read Execute	Read	Read Write

(b)

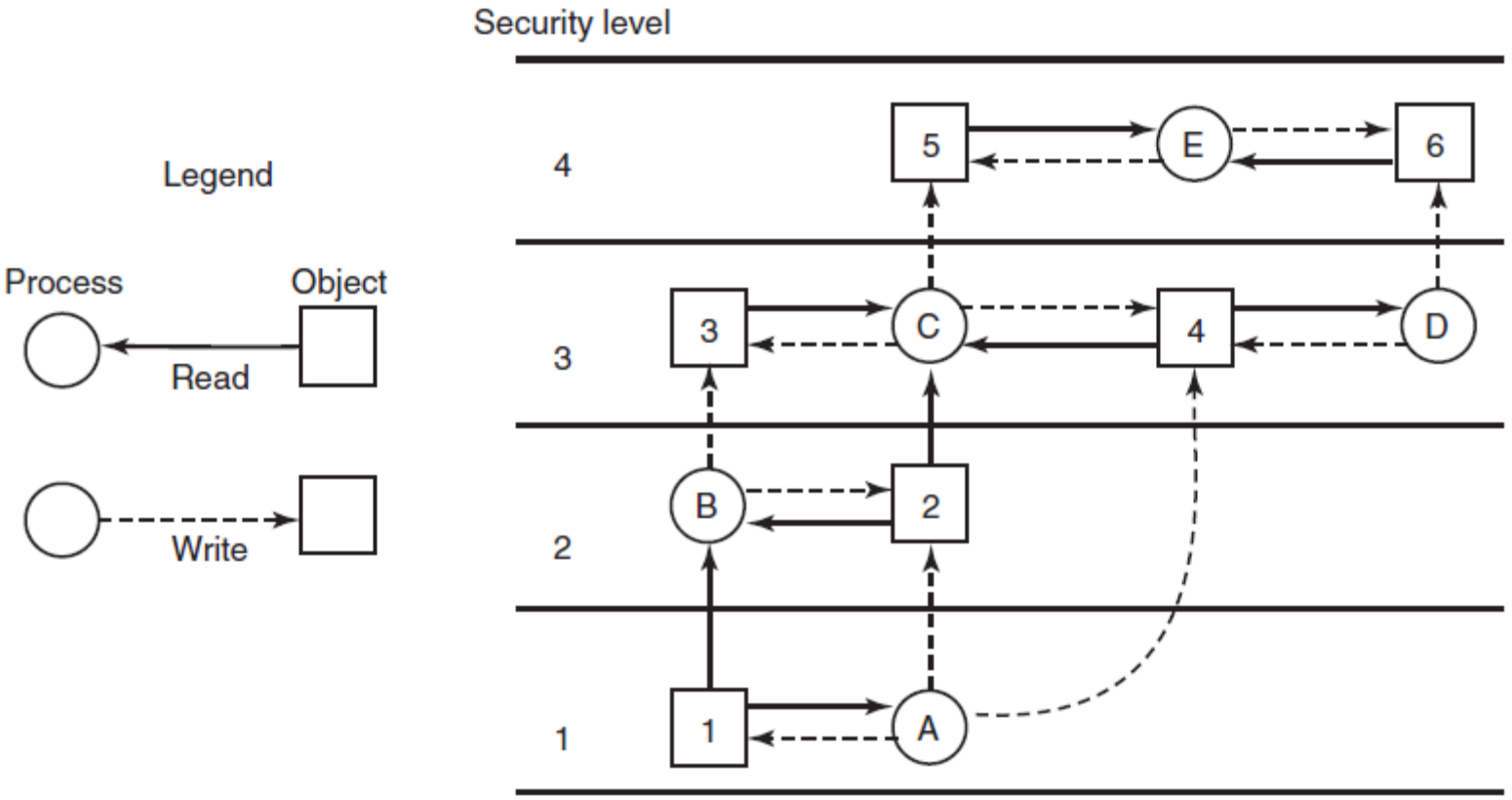
(a) An authorized state.
(b) An unauthorized state.

Multilevel Security
Bell-LaPadula Model

Bell-LaPadula Model rules for information flow:

1. The simple security property
   - Process running at security level k can read only objects at its level or lower
2. The * property
   - Process running at security level k can write only objects at its level or higher

Bell-LaPadula Model



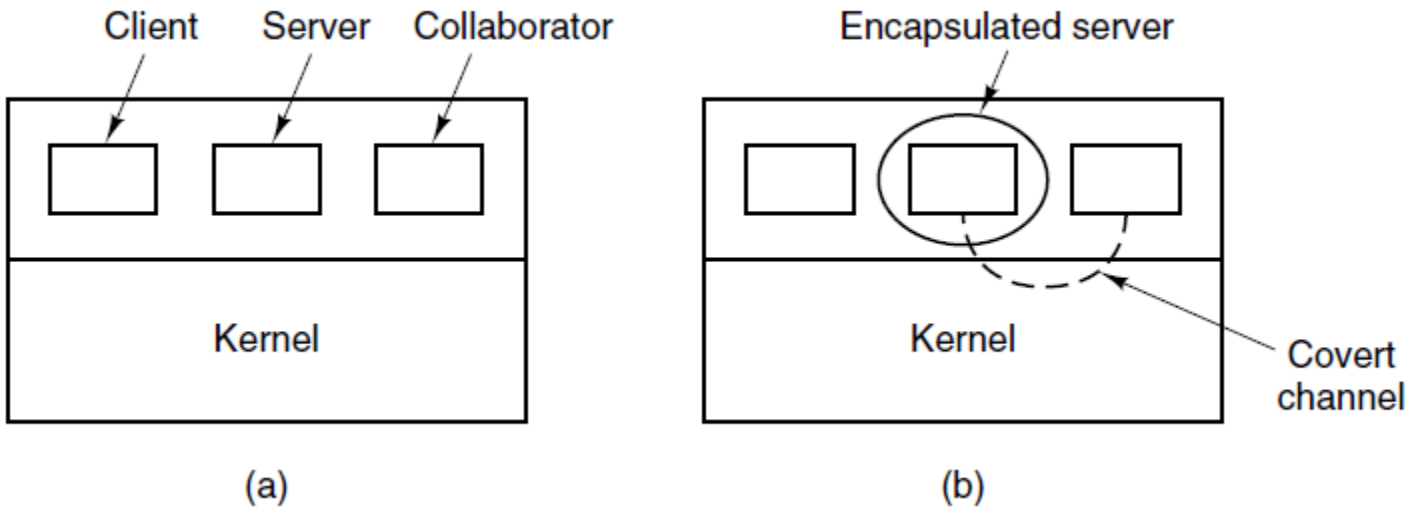
The Bell-LaPadula multilevel security model.

The Biba Model

To guarantee the integrity of the data:

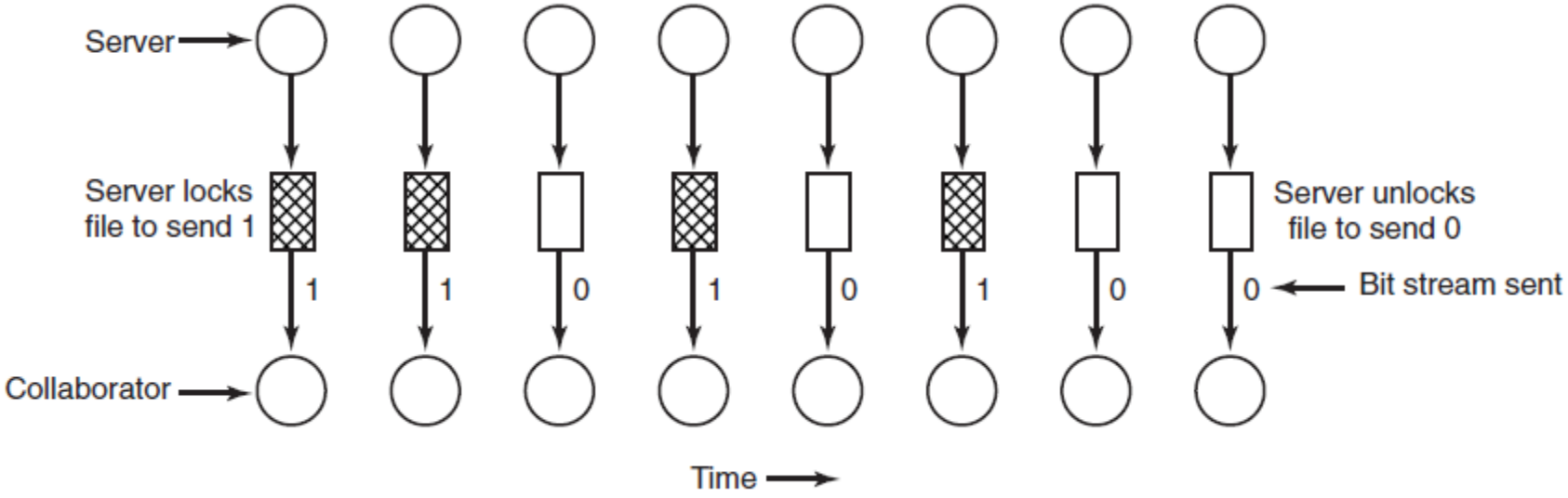
1. The simple integrity principle
   - process running at security level k can write only objects at its level or lower (no write up).
2. The integrity * property
   - process running at security level k can read only objects at its level or higher (no read down).

Covert Channels



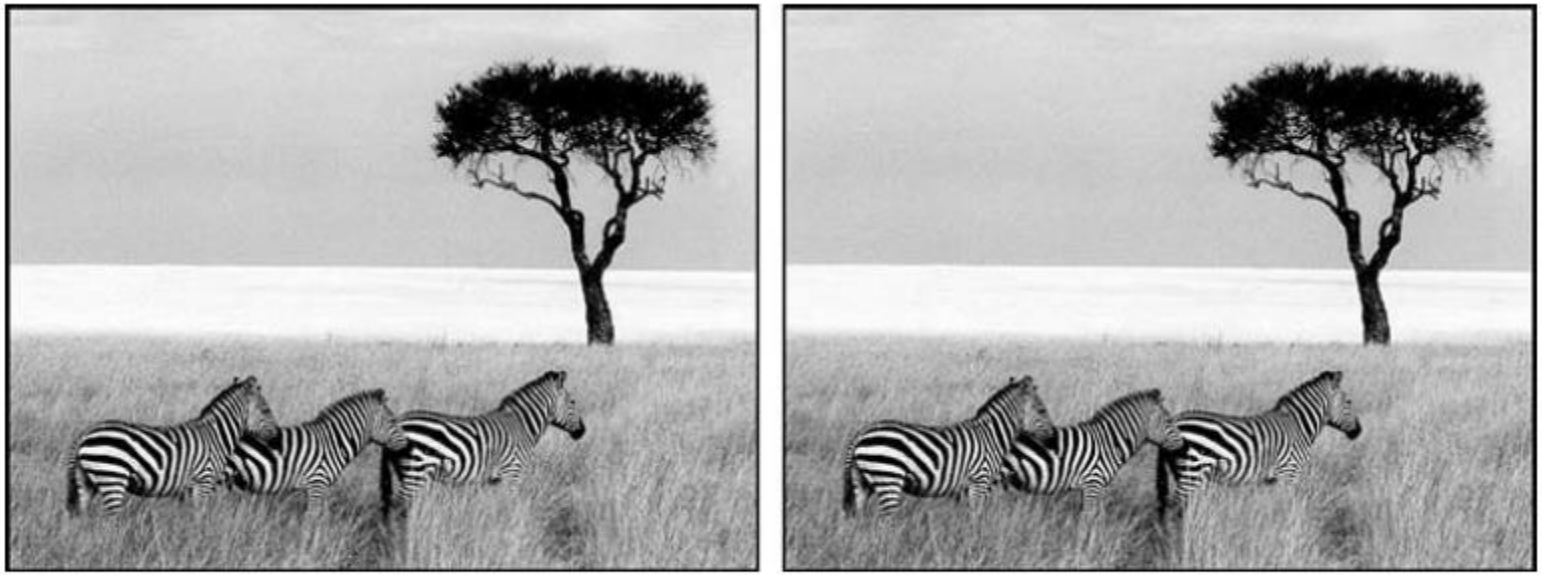
(a) The client, server, and collaborator processes. (b) The encapsulated server can still leak to the collaborator via covert channels.

Covert Channels



A covert channel using file locking.

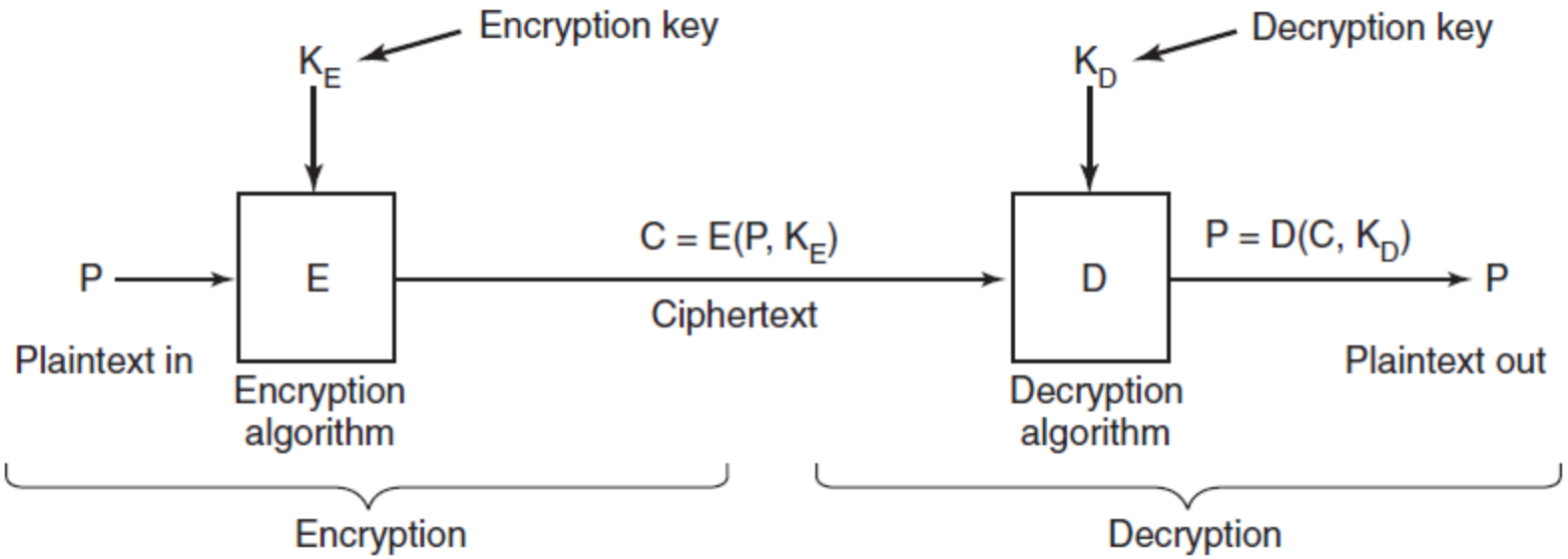
Steganography



(a) (b)

(a) Three zebras and a tree. (b) Three zebras, a tree, and the complete text of five plays by William Shakespeare.

Basics of Cryptography



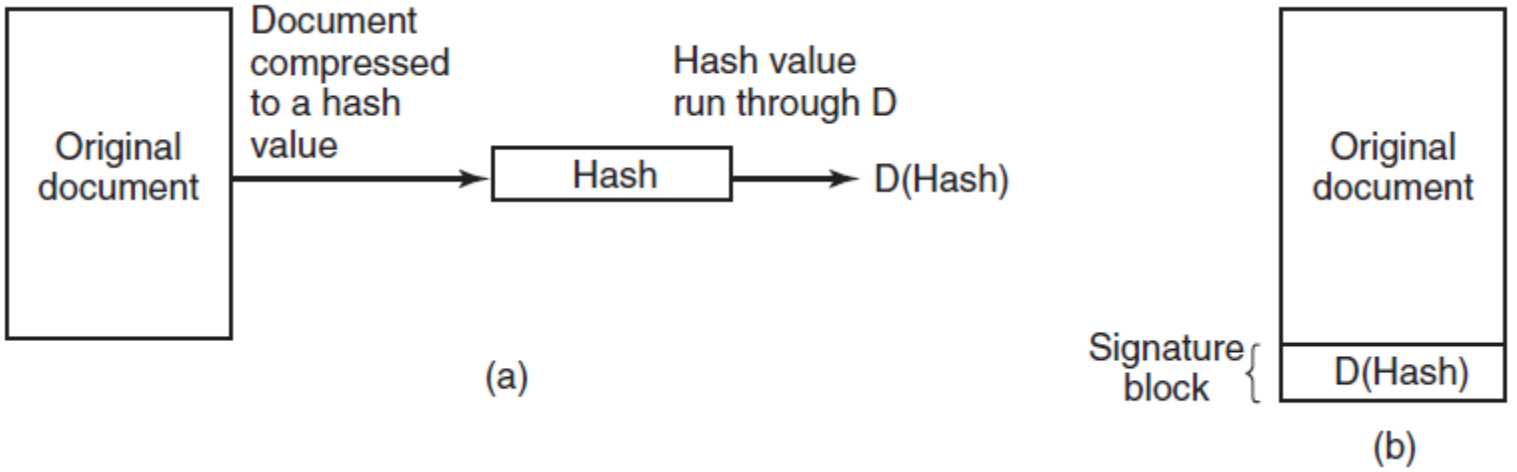
Relationship between the plaintext and the ciphertext.

Secret-Key Cryptography

plaintext:	A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
ciphertext:	Q W E R T Y U I O P A S D F G H J K L Z X C V B N M

An encryption algorithm in which each letter is replaced by a different letter.

Digital Signatures



(a) Computing a signature block.
(b) What the receiver gets.

Authentication

Methods of authenticating users when they attempt to log in based on one of three general principles:

1. Something the user knows.
2. Something the user has.
3. Something the user is.

Authentication

LOGIN: mitch
PASSWORD: FooBar!-7
SUCCESSFUL LOGIN

(a)

LOGIN: carol
INVALID LOGIN NAME
LOGIN:

(b)

LOGIN: carol
PASSWORD: Idunno
INVALID LOGIN
LOGIN:

(c)

(a) A successful login. (b) Login rejected after name is entered. (c) Login rejected after name and password are typed.

UNIX Password Security

Bobbie, 4238, e(Dog, 4238)
Tony, 2918, e(6%%TaeFF, 2918)
Laura, 6902, e(Shakespeare, 6902)
Mark, 1694, e(XaB#Bwcz, 1694)
Deborah, 1092, e(LordByron,1092)

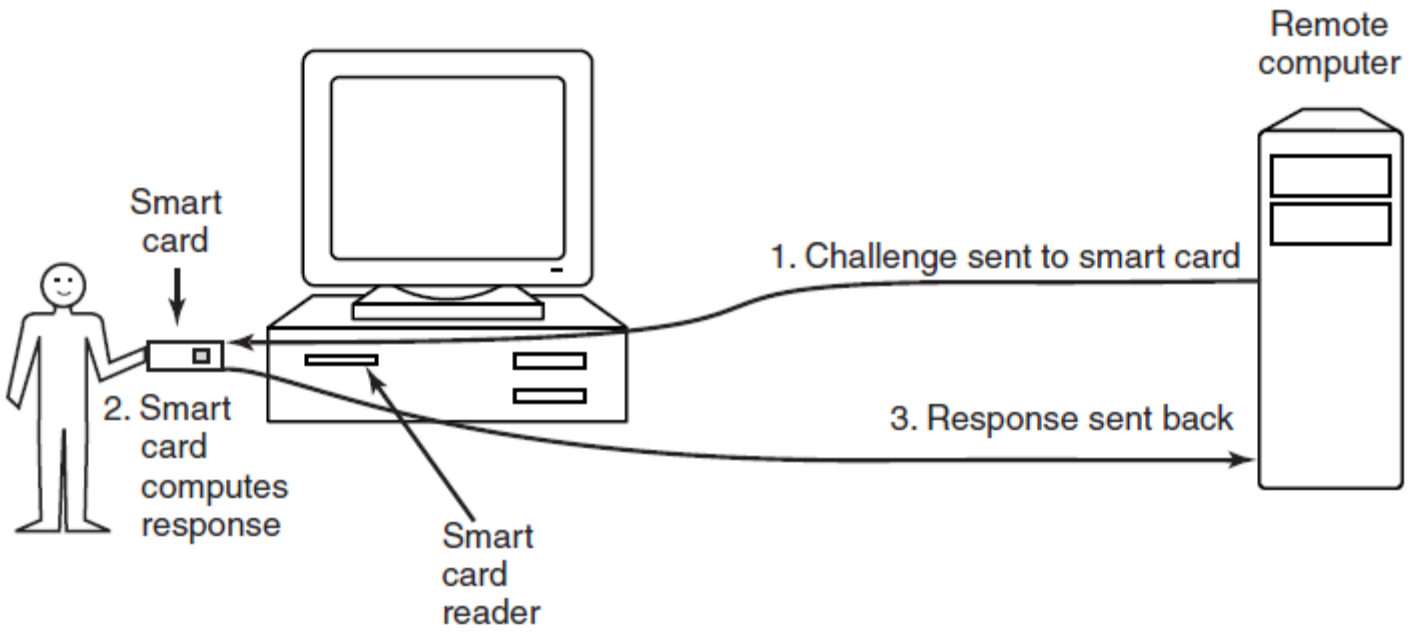
The use of salt to defeat precomputation of encrypted passwords.

Challenge-Response Authentication

Questions should be chosen so that the user does not need to write them down.
Examples:

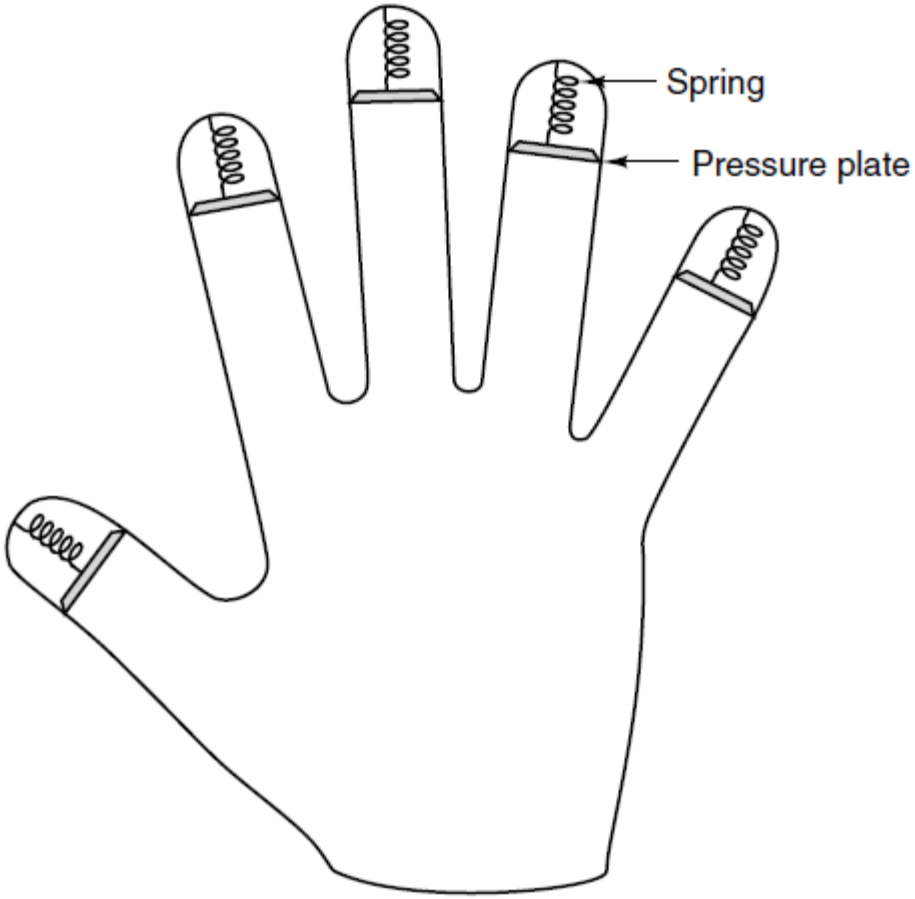
1. Who is Marjolein's sister?
2. On what street was your elementary school?
3. What did Mrs. Ellis teach?

Authentication Using a Physical Object



Use of a smart card for authentication.

Authentication Using Biometrics



A device for measuring finger length.

Summary

- Security Goals and Threats
- Protection Mechanisms
  - Protection Domain
  - Access Control List
  - Capabilities
- Security Models
- Cryptography and Digital Signature
- Authentication

End of CSCI 360