IOWA STATE UNIVERSITY
Department of Electrical and Computer Engineering

Lecture 36: Security I

Agenda

- Security I
  - Basic Concepts
  - Information Leakage Channels
  - Cryptography
  - Authentication

Basic Concepts

- Classic Goals & Threats
  - Confidentiality
    - Having secrete data remain secret
  - Integrity
    - Unauthorized users should not be able to modify data
  - Availability
    - Nobody can disturb the system to make it unusable

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

Basic Concepts

- Trusted Computing Base (TCB)
  - the set of hardware and software necessary for enforcing all security rules
    - E.g., most hardware, part of OS kernel, user-level program with superuser privilege
  - should be minimal
    - E.g., MINIX 3 has about 10,000 lines of code in the kenrel, orders of magnitude less than Linux
      - Easier to be correct
      - Potentially offer higher security

Basic Concepts

- Protection Domains
  - A computer system contains resources (“objects”) that need to be protected
    - E.g., hardware (CPU, memory, HDD, ...) or software (processes, files, ...)
    - Each object has a unique name and a finite set of operations
      - E.g., read()/write() a file named /foo/bar
  - Domain: a set of [object, rights] pairs
    - a right means permission to perform one of the operations
    - a domain may correspond to different entities
      - E.g., a user or a group of users

Basic Concepts

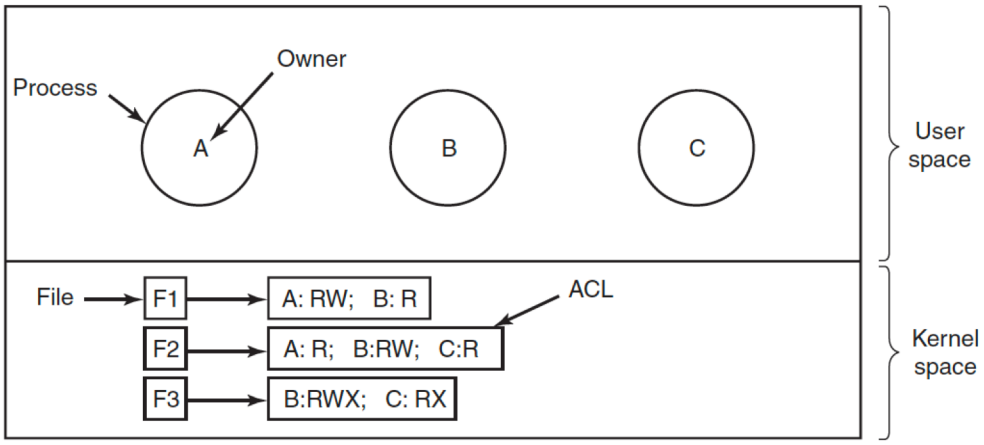
- Protection Domains (cont')
  - Protection matrix
    - Keep track of domains and the associated objects/rights in a matrix

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

    - problem: many cells are empty in a large matrix
      - waste storage space

Basic Concepts

- Access Control List (ACL)
  - slice up the matrix by columns
  - associate with each object an (ordered) list containing all the domains that may access the object, and how
  - E.g., three processes from three different users A/B/C (subjects) and three files (objects)



Basic Concepts

- Access Control List (ACL) (cont')
  - groups of users have group names and can be included in ACLs
    - groups are also called "roles"
      - e.g., system administrators, super users
    - E.g., two ACLs with groups

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

Basic Concepts

- Access Control List (ACL) (cont')
  - E.g., Linux file ACL
    - set file permission: **chmod()**

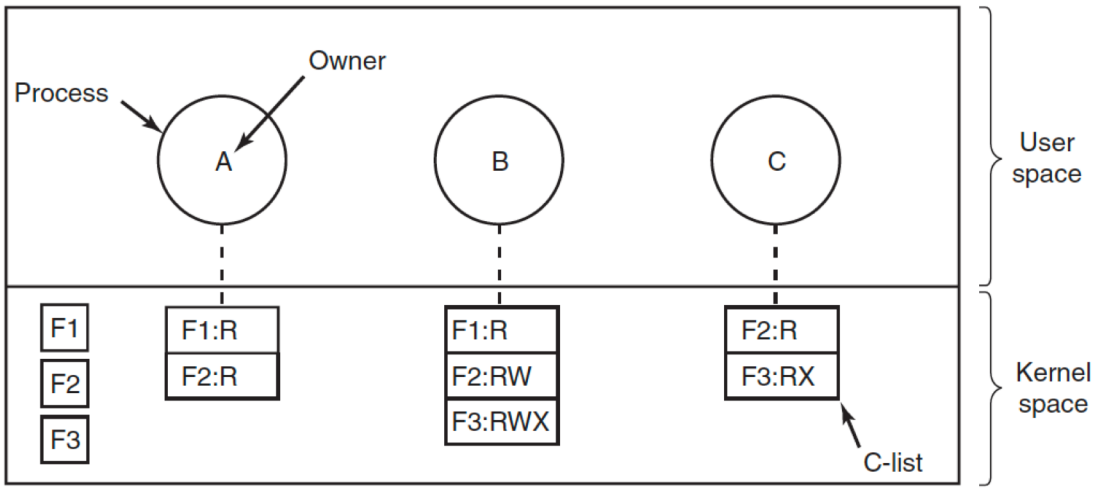
```
% ls -lR
.:
total 2
drwxr-x--x  2 mike    adm    1024 Dec 17 13:34 A
drwxr-----  2 mike    adm    1024 Dec 17 13:34 B

./A:
total 1
-rw-rw-rw-  1 mike    adm     593 Dec 17 13:34 x

./B:
total 2
-r--rw-rw-  1 mike    adm     446 Dec 17 13:34 x
-rw----rw-  1 bob     adm     446 Dec 17 13:45 y
```

Basic Concepts

- Capability List (C-list)
  - slice up the matrix by rows
  - associated with each user/process a list of objects that may be accessed
    - individual items on a C-list are called **capabilities**
      - Each capability grants the owner certain rights on a certain object

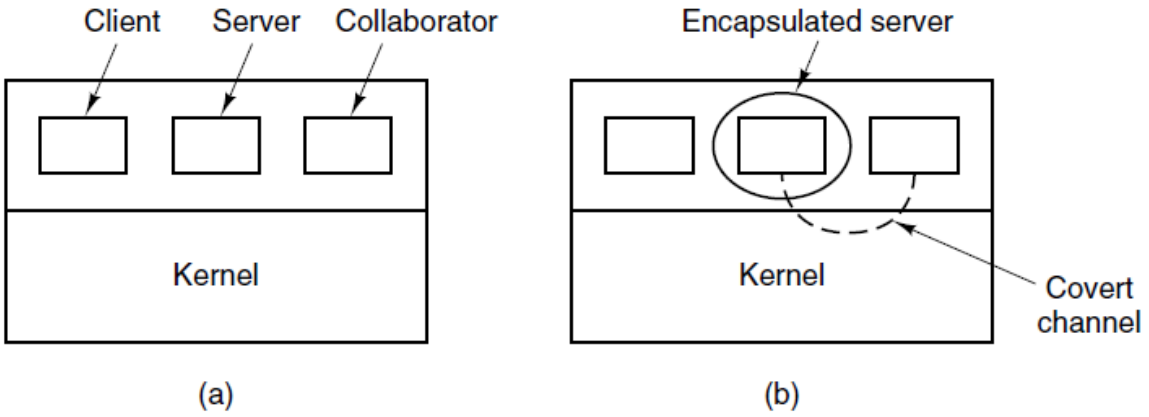


Agenda

- Security I
  - ~~Basic Concepts~~
  - Information Leakage Channels
  - Cryptography
  - Authentication

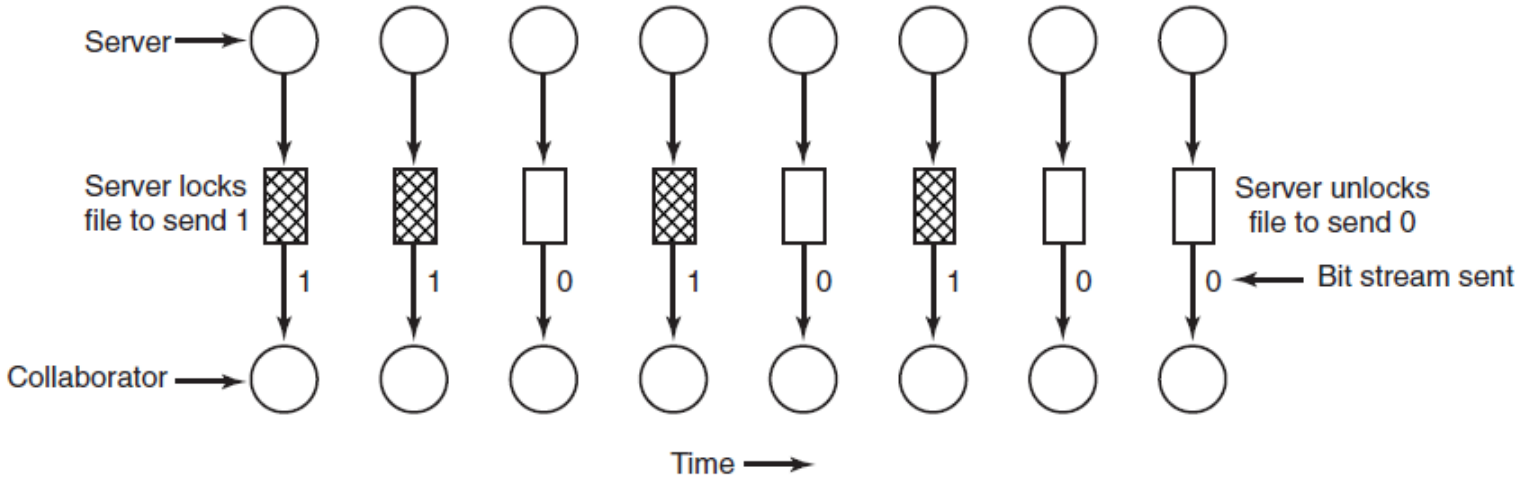
Information Leakage Channels

- Covert Channels
  - An insider process leaks information to an outsider process not normally allowed to access that information by using mechanisms that are not intended for communications
    - E.g., the encapsulated server can leak to the collaborator via covert channels



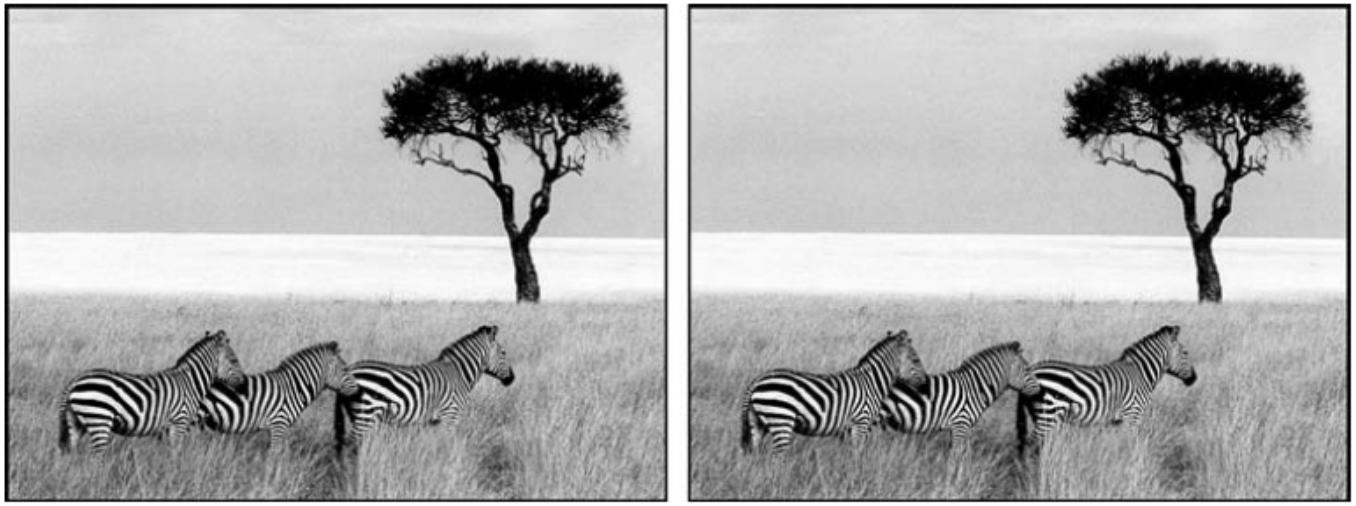
Information Leakage Channels

- Covert Channels (cont')
  - E.g., a covert channel using file locking



Information Leakage Channels

- Steganography
  - Hiding the existence of information
  - E.g., (a) Three zebras and a tree. (b) Three zebras, a tree, and the complete text of five plays by William Shakespeare.



(a) (b)

Agenda

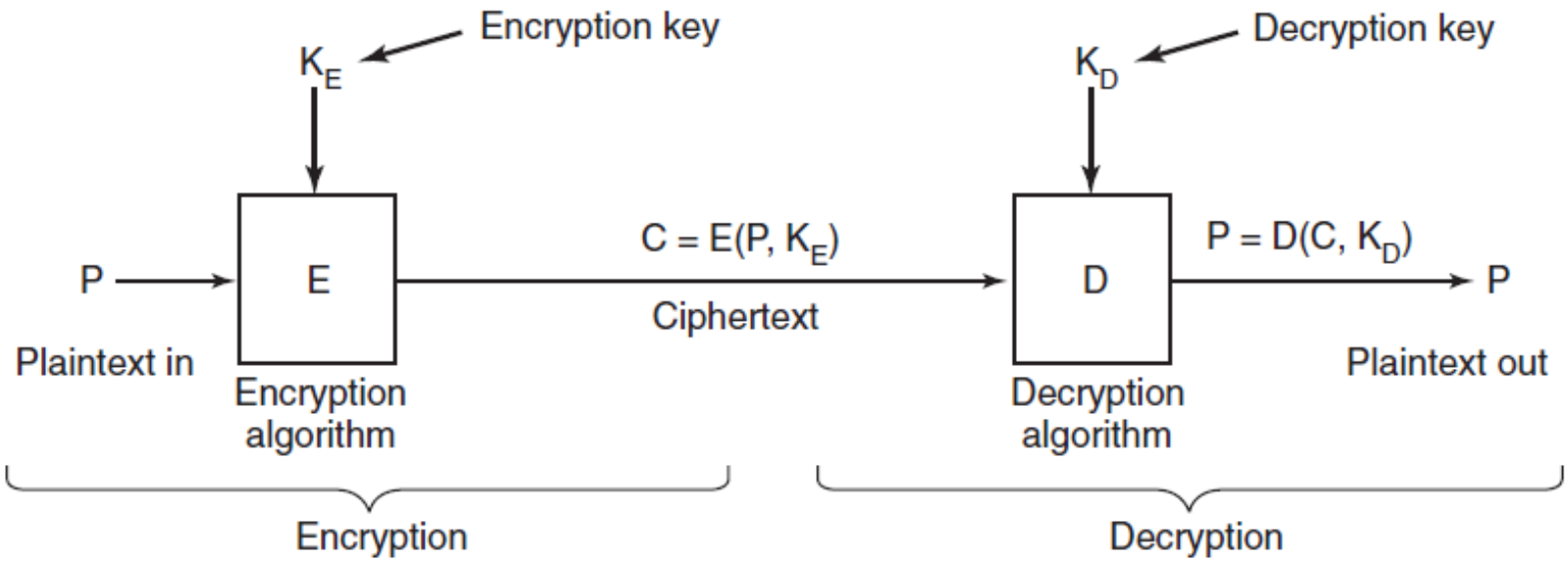
- Security I
  - ~~Basic Concepts~~
  - ~~Information Leakage Channels~~
  - Cryptography
  - Authentication

Cryptography

- Purpose
  - Take a message (or file), called the **plaintext**, and encrypt it into **ciphertext** in such a way that only authorized people know how to convert it back to plaintext
    - for unauthorized people, the ciphertext is just an incomprehensible sequence of bits
- The encryption & decryption algorithms are public
  - The secrecy depends on parameters to the algorithms called **keys**

Cryptography

- Relationship between the plaintext and the ciphertext



Cryptography

- Secret-Key Cryptography
  - Sender and receiver must both be in possession of the shared secret key
    - Also called “symmetric-key cryptography”
  - Efficient because the computation required to encrypt or decrypt a message is relatively manageable

Cryptography

- Secret-Key Cryptography
  - E.g., monoalphabetic substitution
    - An encryption algorithm in which each letter is replaced by a different letter.

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

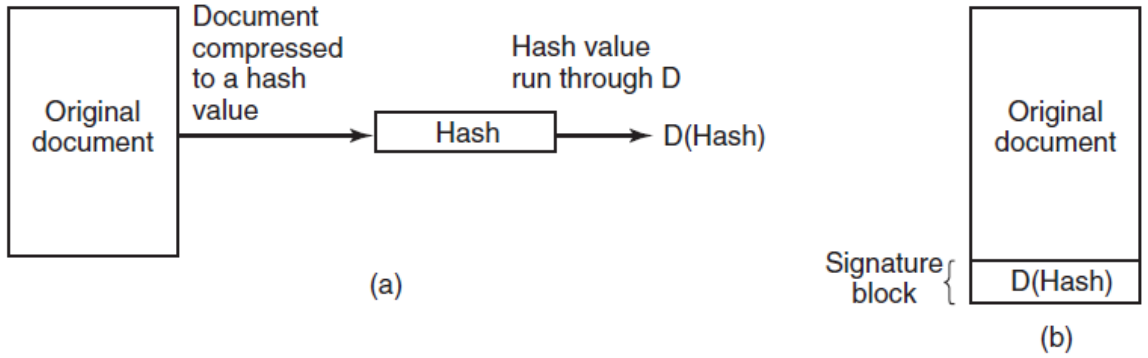
“ATTACK” ← → “QZZQEA”

Cryptography

- Public-Key Cryptography
  - Everyone picks a (public key, private key) pair and publishes the public key
    - Public key: encryption key
    - Private key: decryption key
  - Keys are generated automatically using an algorithm
    - E.g., RSA algorithm
    - Usually have some randomness or password fed into the algorithm as a seed
  - User X sends a secret message to User Y
    - X encrypts the message using Y's public key
    - Y decrypts the message using Y's secret key

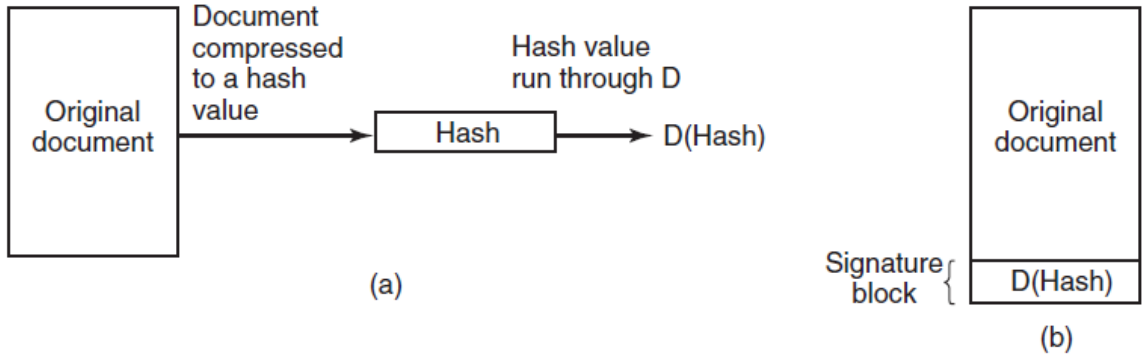
Cryptography

- Digital Signature
  - Sender signs digital documents in such a way that they cannot be repudiated by the sender later
    - run the document through a one-way cryptographic hashing algorithm (e.g., SHA-1) that is very hard to invert
    - sender applies her private key to the hash to get D(hash), i.e., signature block
    - Signature block is appended to the doc and send to the receiver



Cryptography

- Digital Signature
  - Receiver:
    - computes the hash of the document (e.g., using SHA-1)
    - applies the sender's public key to the signature block to get E(D(hash))
      - Canceling out the effect of D(hash) to get the hash back
    - If the computed hash does not match the hash from the signature block, then the document, the signature block, or both have been tampered

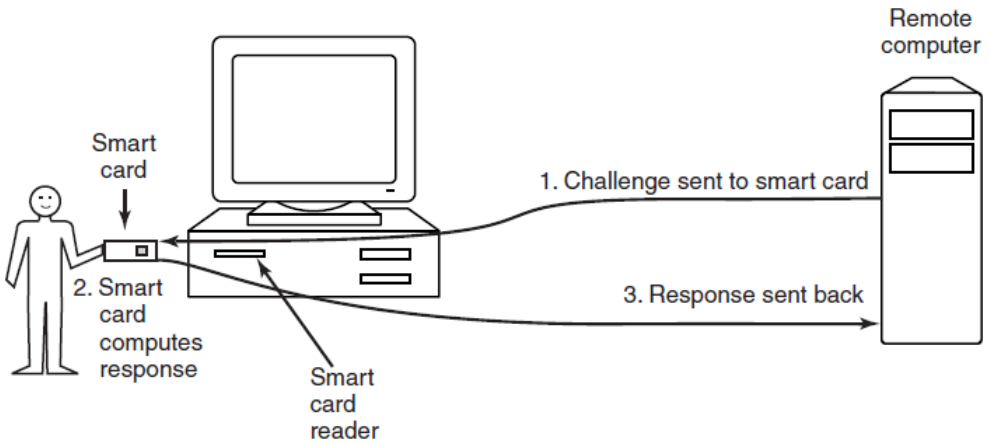


Agenda

- Security I
  - ~~Basic Concepts~~
  - ~~Information Leakage Channels~~
  - ~~Cryptography~~
  - Authentication

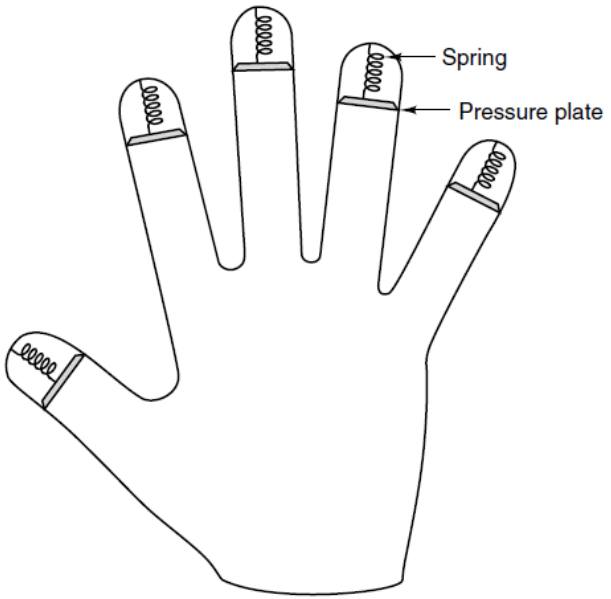
Authentication

- Prove the identity of a user
- Based on three general principles:
  - Something the user knows.
  - Something the user has.
  - Something the user is
- Common methods
  - Password
  - Hardware token
    - E.g., RSA SecurID
  - Software token
    - E.g., private key in a public-key cryptosystem



Authentication

- Common Methods
  - Biometrics
    - E.g., fingerprint



  - Multi-factor authentication
    - Combine multiple sources to verify identity
    - E.g., password + hardware token, password + security questions

Agenda

- ~~Security I~~
  - ~~Basic Concepts~~
  - ~~Information Leakage Channels~~
  - ~~Cryptography~~
  - ~~Authentication~~

Questions?

*acknowledgement: slides include content from “Modern Operating Systems” by A. Tanenbaum, “Operating Systems Concepts” by A. Silberschatz etc., “Operating Systems: Three Easy Pieces” by R. Arpaci-Dusseau etc., and anonymous pictures from internet.