Chapter 2
Toolbox: Authentication, Access Control, and Cryptography

Jun Li

lijun@cs.uoregon.edu

Learning Objectives

- Purposes and methods of authentication and access control
- Basic cryptography
  - Classic crypto
  - Public key crypto
  - Certificates, PKI, Digital Signature

1.

AUTHENTICATION

Determining who a person is

- Identification: the act of asserting who a person is
- Authentication: the act of proving that asserted identity: that the person is who she says she is.
- Identity are typically public or well known. Authentication should be private.

Authentication

- Something the user *knows*
  - e.g., passwords, pin, mother's maiden name, etc.
- Something the user *has*
  - e.g., ID, physical keys
- Something the user *is*
  - e.g., biometrics

Two or more forms can be combined.

Authentication Based on Password: Something You Know

- Password
- Attacking and protecting passwords
  - Dictionary attacks
  - Inferring passwords likely for a user
  - Guessing possible passwords
  - Defeating Concealment (textbook Page 49-50)
  - Exhaustive attack
- Good passwords
- Security Questions
  - only the right person should know the answer

Authentication Based on Biometrics: Something You Are

- Fingerprint, hand geometry, retina and iris, voice, handwriting, typing characteristics, face, blood vessels, facial features
- Problems: intrusive, costly, single point of failure, accuracy
- **False positive**: incorrectly confirming an identity
- **False negative**: incorrectly denying an identity

Authentication Based on Tokens: Something You Have

- Examples: key, badge, identity card, credit cards with a chip.
- Static tokens
  - Skimming attack: the use of a device to copy authentication data surreptitiously and relay it to an attacker
- Dynamic tokens
  - Token value changes
  - Ex.: SecureID Token

Federated Identity Management

- Federated Identity Manager
  - Figure 2-5
  - Act as a server for multiple applications
- Single Sign-On
  - Figure 2-6
  - An umbrella task that acts on behalf of the user

Multifactor Authentication

- Combining authentication information
- Two-factor authentication
- A tradeoff between security and inconvenience

2.

ACCESS CONTROL

Goals

- Check every access
- Enforce least privilege
- Verify acceptable usage
  - E.g., stack accesses can only be `push`, `pop`, `clear`

Challenges

- The number of access points may be large
- Maybe no central authority
- Many types of accesses

Access Control Matrix

- A great concept and logically powerful

	BIBLIOG	TEMP	F	HELP.TXT	C_COMP	LINKER	SYS_CLOCK	PRINTER
USER A	ORW	ORW	ORW	R	X	X	R	W
USER B	R	-	-	R	X	X	R	W
USER S	RW	-	R	R	X	X	R	W
USER T	-	-	-	R	X	X	R	W
SYS_MGR	-	-	-	RW	OX	OX	ORW	O
USER_SVCS	-	-	-	O	X	X	R	W

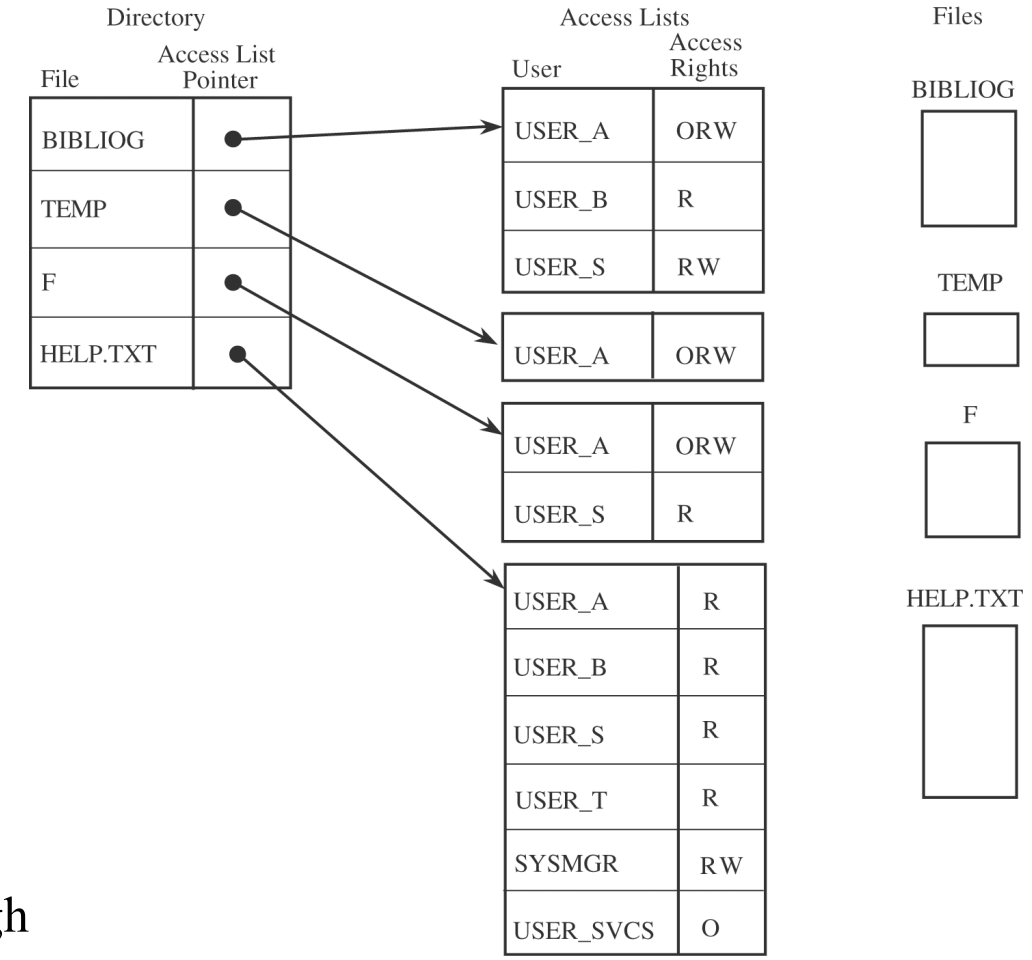
Control Methods

- Access Control Matrix
- Access Control List
- Directory

- Capability
- Procedure-Oriented Access Control
- Role-Based Access Control

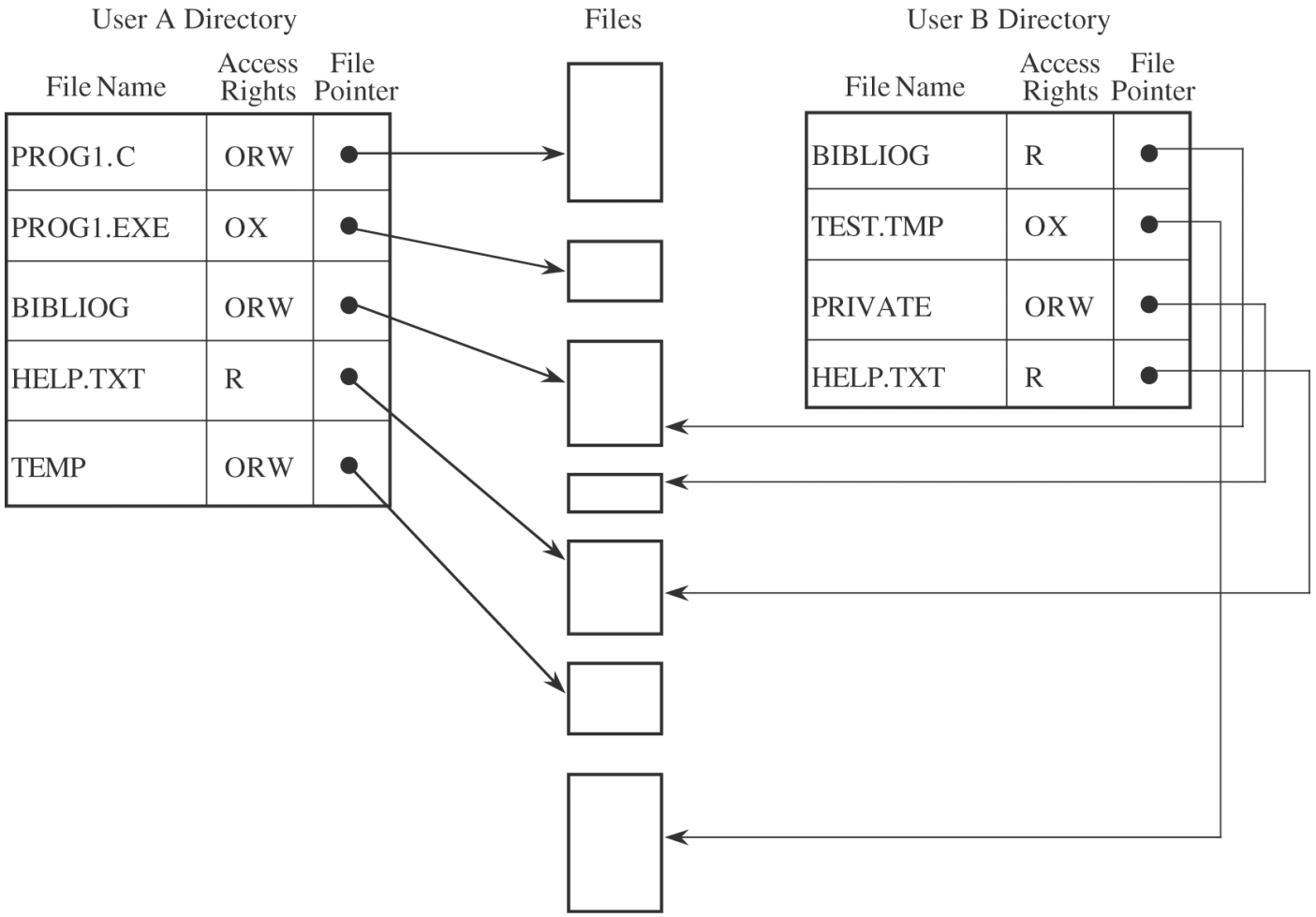
Access Control List

- One access control list per object
  - The column for the object in Access Control Matrix



Directory

- A directory per user (per subject)
  - The row for the user (subject) in Access Control Matrix



Capability

- A ticket giving permission to a subject to have a certain type of access to an object
- Must be unforgeable
- Held by OS, which only returns to the subject the pointer to the ticket
- Or, encrypted with a key only available to the access control mechanism

Procedure-Oriented Access Control

- Must go through a specific procedure (or more) to access an object
- You can think read/write/execute as special procedures

Role-Based Access Control

- Associate privileges with roles
- Control access by job demands, not by person

Discussion Questions

- What is the relationship between identification and authentication?
- What is the relationship between authentication and access control?
- What is the difference between ACL and Directory for access control?
- Directory vs. Capability?