Computer Security: Principles and Practice

Fourth Edition

By: William Stallings and Lawrie Brown

Chapter 4

Access Control

The 1-slide course summary of CH 1-3

CH1 - Introduction

- 3 Pillars of security: CIA
- Threats, Vulnerabilities, Attacks, Countermeasures
- More fine-grained services: I&A, Auth, Conf, Int, Non-rep, Avail

CH2 – Cryptohraphy

- Symmetric, Asymmetric, Hash

CH3 – I&A (first fine-grained service)

CH4…… Access control (2nd fine-grained service)

Access Control Definitions 1/2

NISTIR 7298 defines access control as:

"the process of granting or denying specific requests to: (1) obtain and use information and related information processing services; and (2) enter specific physical facilities"

Access Control Definitions 2/2

RFC 4949 defines access control as:

"a process by which use of system resources is regulated according to a security policy and is permitted only by authorized entities (users, programs, processes, or other systems) according to that policy"

Access Control Principles

- In a broad sense, all of computer security is concerned with access control

- RFC 4949 defines computer security as:

"measures that implement and assure security services in a computer system, particularly those that assure access control service"

Table 4.1
Access Control Security Requirements (SP 800-171)

	Basic Security Requirements
1	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).
2	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.

(Table is on page 107 in the textbook)

Table 4.1
Access Control Security Requirements (SP 800-171)

	Derived Security Requirements
3	Control the flow of CUI in accordance with approved authorizations.
4	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.
5	Employ the principle of least privilege, including for specific security functions and privileged accounts.
6	Use non-privileged accounts or roles when accessing nonsecurity functions.
7	Prevent non-privileged users from executing privileged functions and audit the execution of such functions.
8	Limit unsuccessful logon attempts.
9	Provide privacy and security notices consistent with applicable CUI rules.
10	Use session lock with pattern-hiding displays to prevent access and viewing of data after period of inactivity.
11	Terminate (automatically) a user session after a defined condition.

(Table is on page 107 in the textbook)

Table 4.1
Access Control Security Requirements (SP 800-171)

	Derived Security Requirements
12	Monitor and control remote access sessions.
13	Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.
14	Route remote access via managed access control points.
15	Authorize remote execution of privileged commands and remote access to security-relevant information.
16	Authorize wireless access prior to allowing such connections.
17	Protect wireless access using authentication and encryption.
18	Control connection of mobile devices.
19	Encrypt CUI on mobile devices.
20	Verify and control/limit connections to and use of external information systems.
21	Limit use of organizational portable storage devices on external information systems.
22	Control CUI posted or processed on publicly accessible information systems.

CUI = controlled unclassified information

(Table is on page 107 in the textbook)

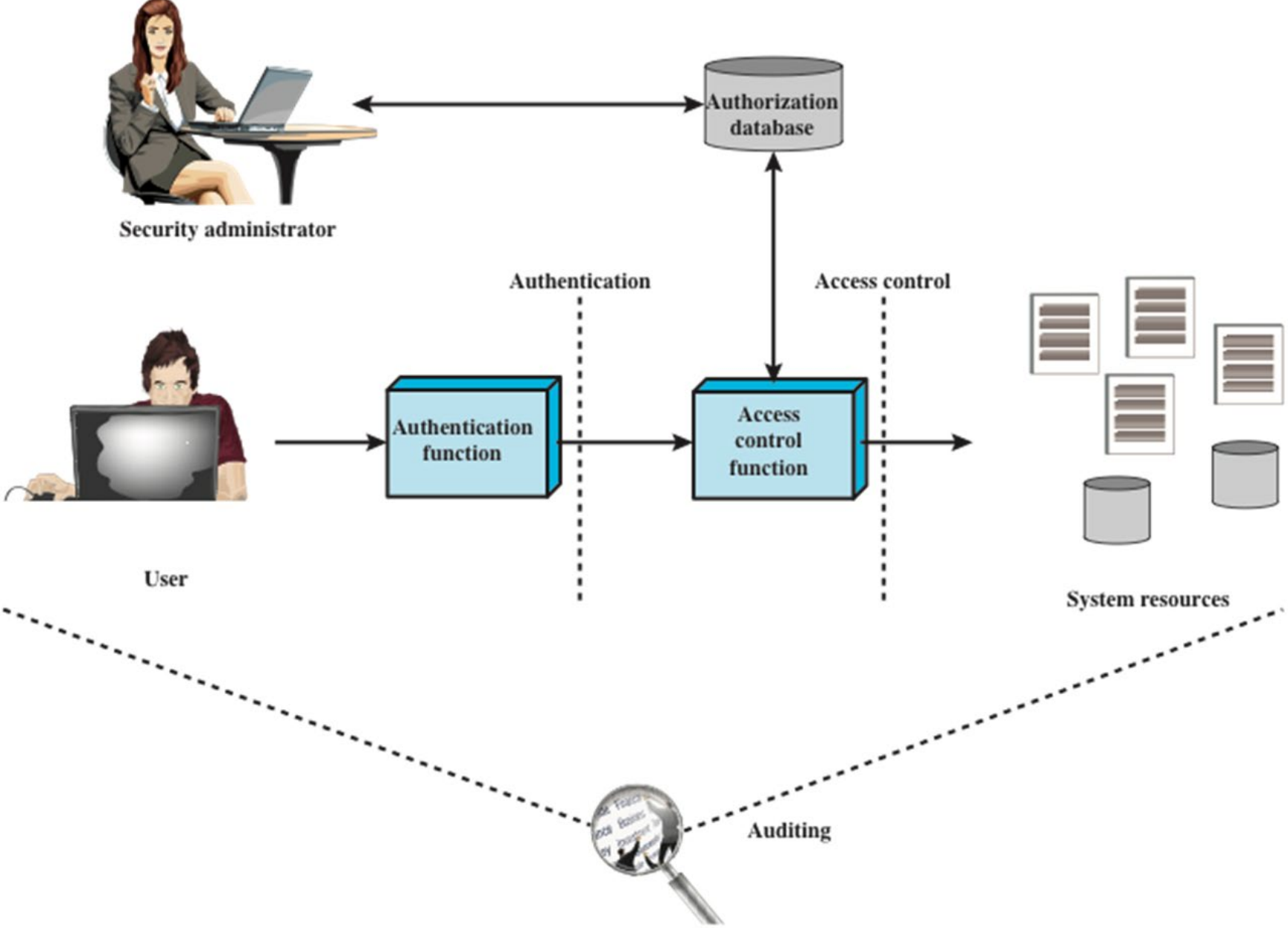


Figure 4.1 Relationship Among Access Control and Other Security Functions

Access Control Policies

- Discretionary access control (DAC)
  - Controls access based on the identity of the requestor and on access rules (authorizations) stating what requestors are (or are not) allowed to do
- Mandatory access control (MAC)
  - Controls access based on comparing security labels with security clearances
- Role-based access control (RBAC)
  - Controls access based on the roles that users have within the system and on rules stating what accesses are allowed to users in given roles
- Attribute-based access control (ABAC)
  - Controls access based on attributes of the user, the resource to be accessed, and current environmental conditions
  - E.g. time, department, ownership etc.

Subjects, Objects, and Access Rights

Subject

An entity capable of accessing objects

Three classes
- Owner
- Group
- World

Object

A resource to which access is controlled

Entity used to contain and/or receive information

Access right

Describes the way in which a subject may access an object

Could include:
- Read
- Write
- Execute
- Delete
- Create
- Search

Discretionary Access Control (DAC)

- Scheme in which an entity may be granted access rights that permit the entity to enable another entity to access some resource
- Often provided using an access matrix
  - One dimension consists of identified subjects that may attempt data access to the resources
  - The other dimension lists the objects that may be accessed
  - Each entry in the matrix indicates the access rights of a particular subject for a particular object

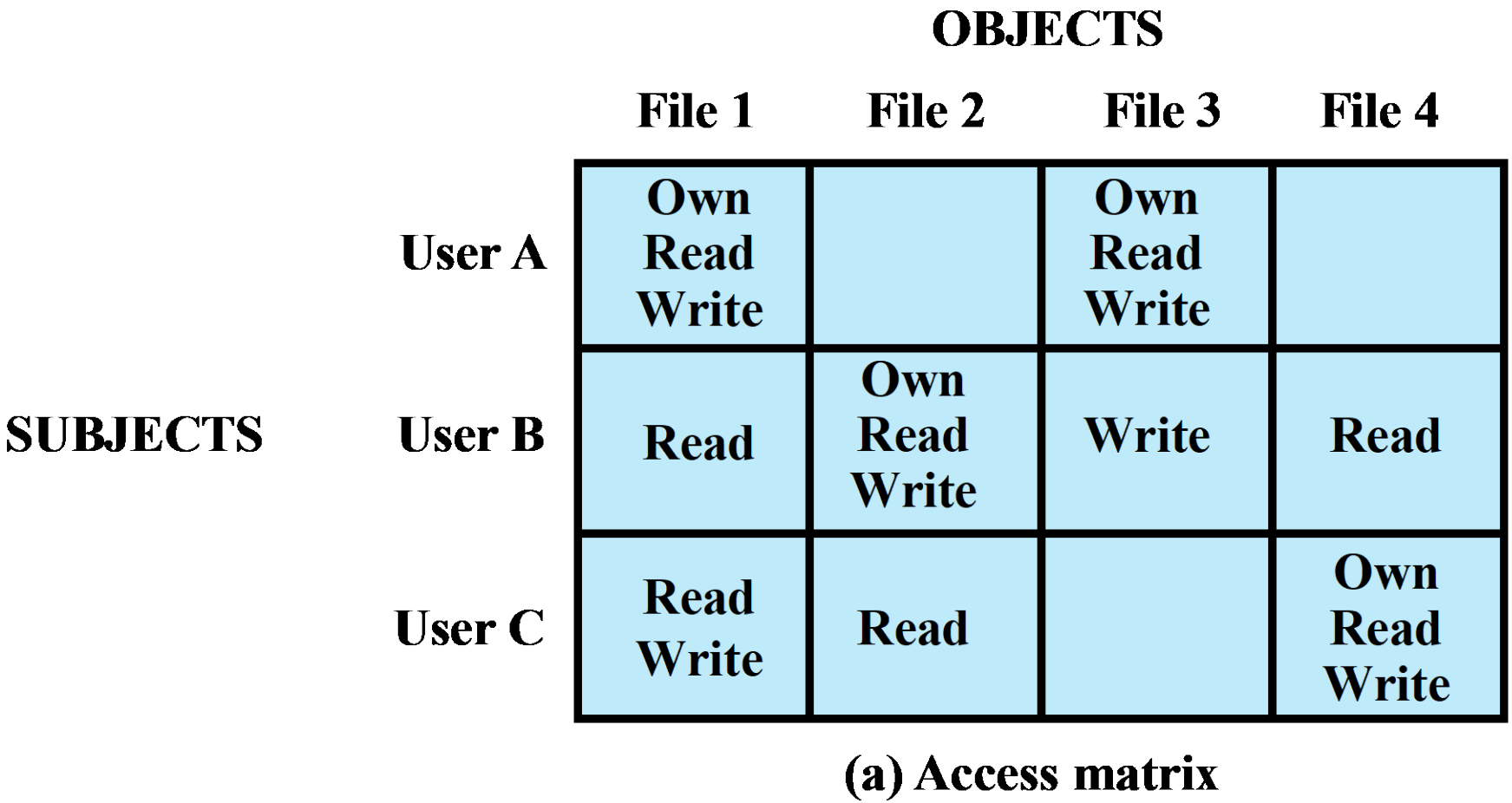
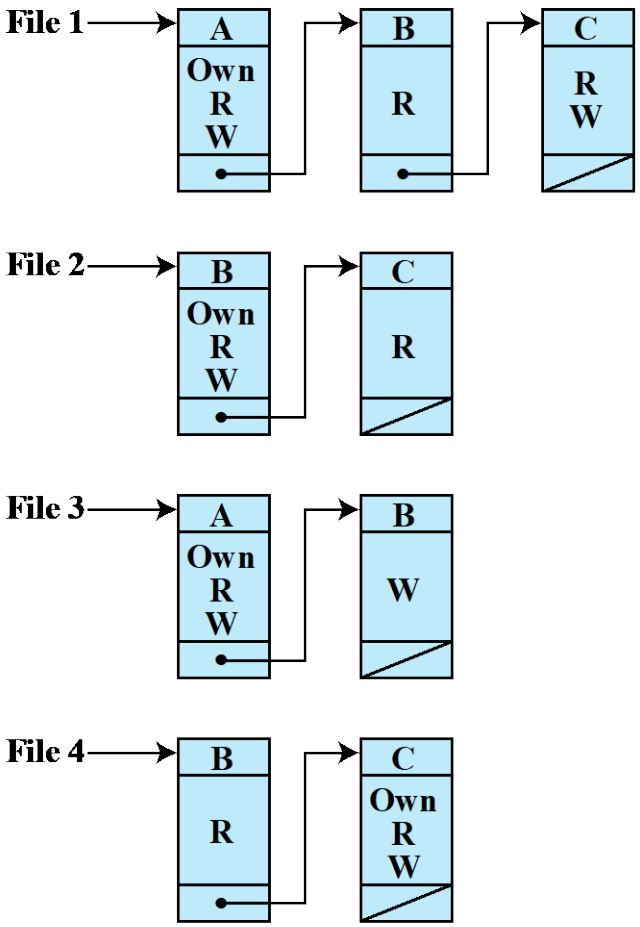
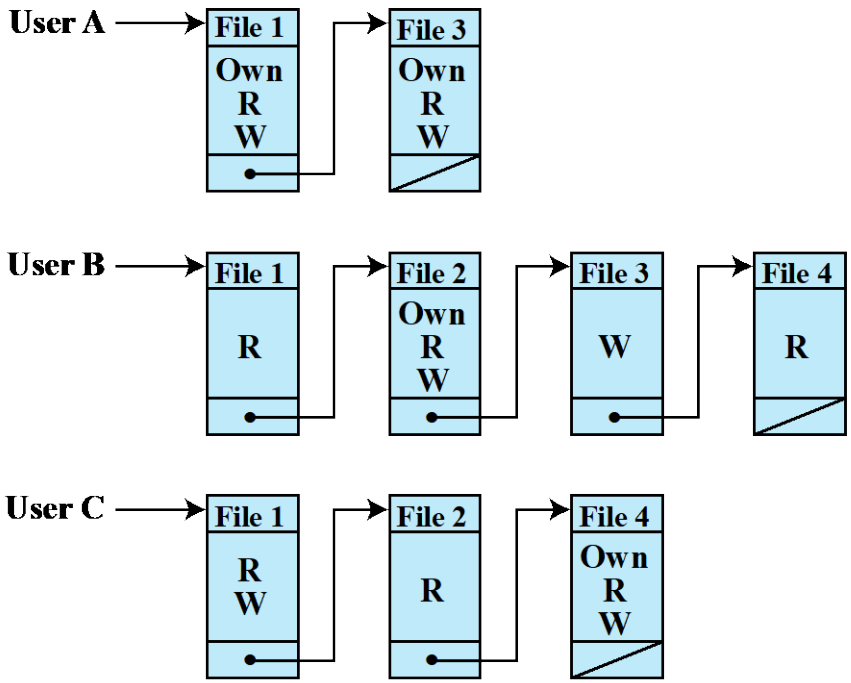


Figure 4.2 Example of Access Control Structures



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



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

Figure 4.2 Example of Access Control Structures

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
C	Read	File 1
C	Write	File 1
C	Read	File 2
C	Own	File 4
C	Read	File 4
C	Write	File 4

Table 4.2

Authorization Table for Files in Figure 4.2

(Table is on page 113 in the textbook)

		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

UNIX File Access Control

UNIX files are administered using inodes (index nodes)

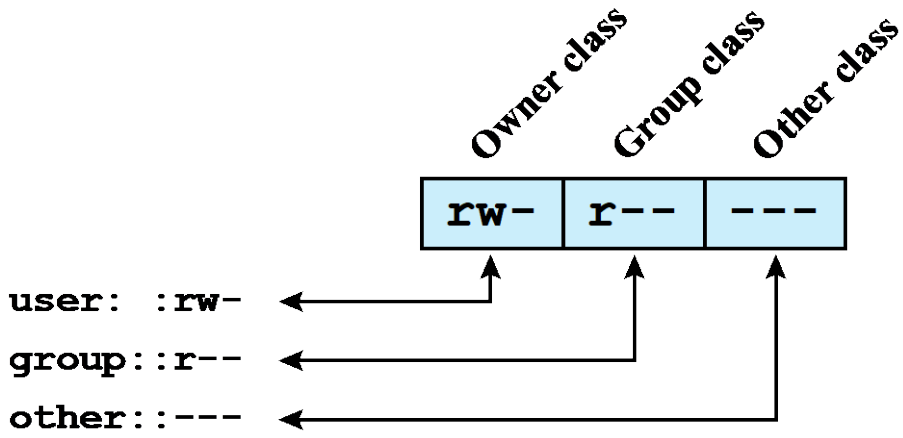
- Control structures with key information needed for a particular file
- Several file names may be associated with a single inode
- An active inode is associated with exactly one file
- File attributes, permissions and control information are sorted in the inode
- On the disk there is an inode table, or inode list, that contains the inodes of all the files in the file system
- When a file is opened its inode is brought into main memory and stored in a memory resident inode table

Directories are structured in a hierarchical tree

- May contain files and/or other directories
- Contains file names plus pointers to associated inodes

UNIX
File Access Control

- Unique user identification number (user ID)
- Member of a primary group identified by a group ID
- Belongs to a specific group
- 12 protection bits
  - Specify read, write, and execute permission for the owner of the file, members of the group and all other users
- The owner ID, group ID, and protection bits are part of the file's inode



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

Figure 4.5 UNIX File Access Control

Access Control Lists (ACLs) in UNIX

Modern UNIX systems support ACLs

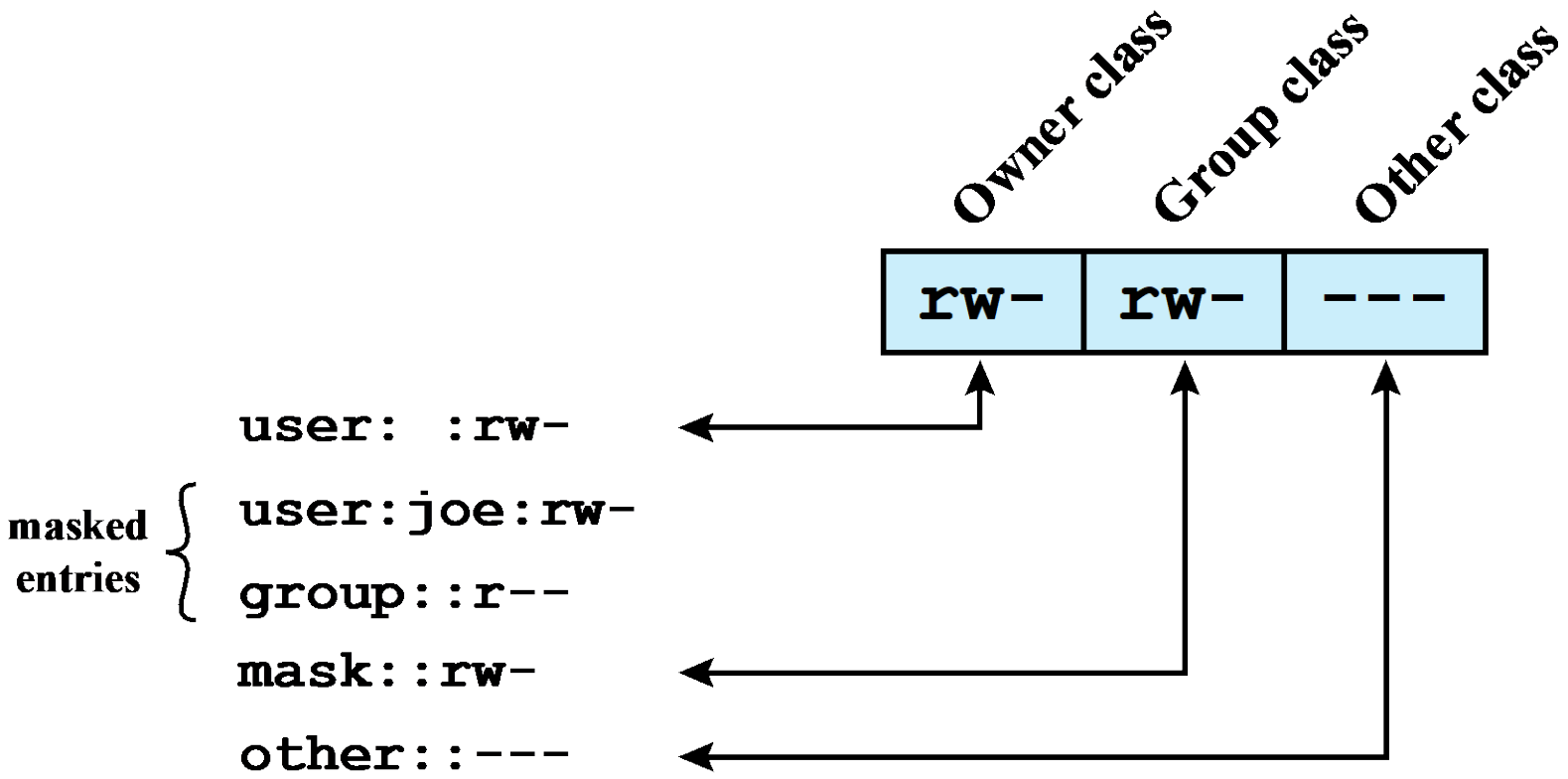
- FreeBSD, OpenBSD, Linux, Solaris

FreeBSD

- Setfacl command assigns a list of UNIX user IDs and groups
- Any number of users and groups can be associated with a file
- Read, write, execute protection bits
- A file does not need to have an ACL
- Includes an additional protection bit that indicates whether the file has an extended ACL

When a process requests access to a file system object, two steps are performed:

- Step 1 selects the most appropriate ACL
- Step 2 checks if the matching entry contains sufficient permissions



(b) Extended access control list

Figure 4.5 UNIX File Access Control

Access Control Policies

- Discretionary access control (DAC)
  - Controls access based on the identity of the requestor and on access rules (authorizations) stating what requestors are (or are not) allowed to do
- Mandatory access control (MAC)
  - Controls access based on comparing security labels with security clearances
- Role-based access control (RBAC)
  - Controls access based on the roles that users have within the system and on rules stating what accesses are allowed to users in given roles
- Attribute-based access control (ABAC)
  - Controls access based on attributes of the user, the resource to be accessed, and current environmental conditions
  - E.g. time, department, ownership etc.

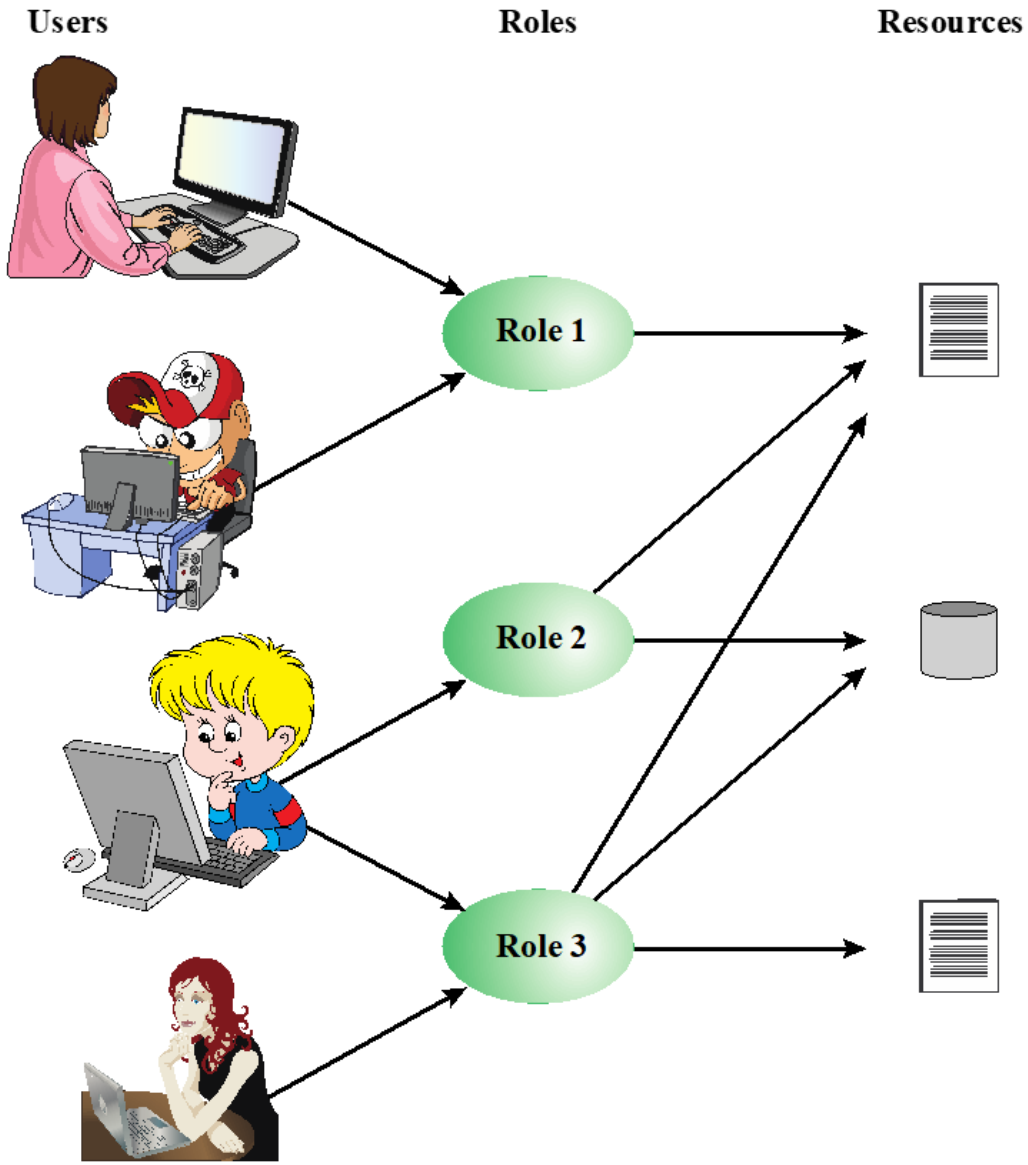
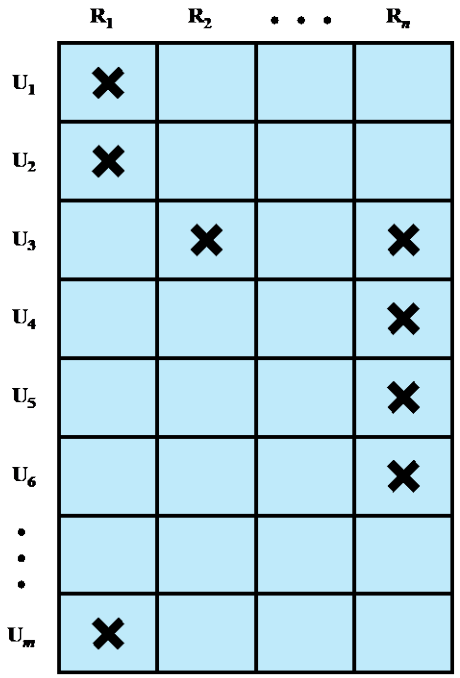


Figure 4.6 Users, Roles, and Resources



OBJECTS

ROLES	R_1	R_2	R_n	F_1	F_1	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 4.7 Access Control Matrix Representation of RBAC

Attribute-Based Access Control (ABAC)

Can define authorizations that express conditions on properties of both the resource and the subject

Strength is its flexibility and expressive power

Main obstacle to its adoption: concern about the negative performance impact of evaluating predicates on both resource and user properties for each access

Web services have been pioneering technologies through the introduction of the eXtensible Access Control Markup Language (XACML)

There is considerable interest in applying the model to cloud services

ABAC Model: Attributes

Subject attributes

- A subject is an active entity that causes information to flow among objects or changes the system state
- Attributes define the identity and characteristics of the subject
- E.g. identifier, name, organization, job title, and so on, subject's role

Object attributes

- An object (or resource) is a passive information system-related entity containing or receiving information
- Objects have attributes that can be leverages to make access control decisions
- E.g. ownership, service taxonomy, or even Quality of Service (QoS)

Environment attributes

- Describe operational, technical, and even situational environment or context in which the information access occurs
- These attributes have so far been largely ignored in most access control policies
- current date and time, the current virus/hacker activities, and the network's security level (e.g., Internet vs. intranet)

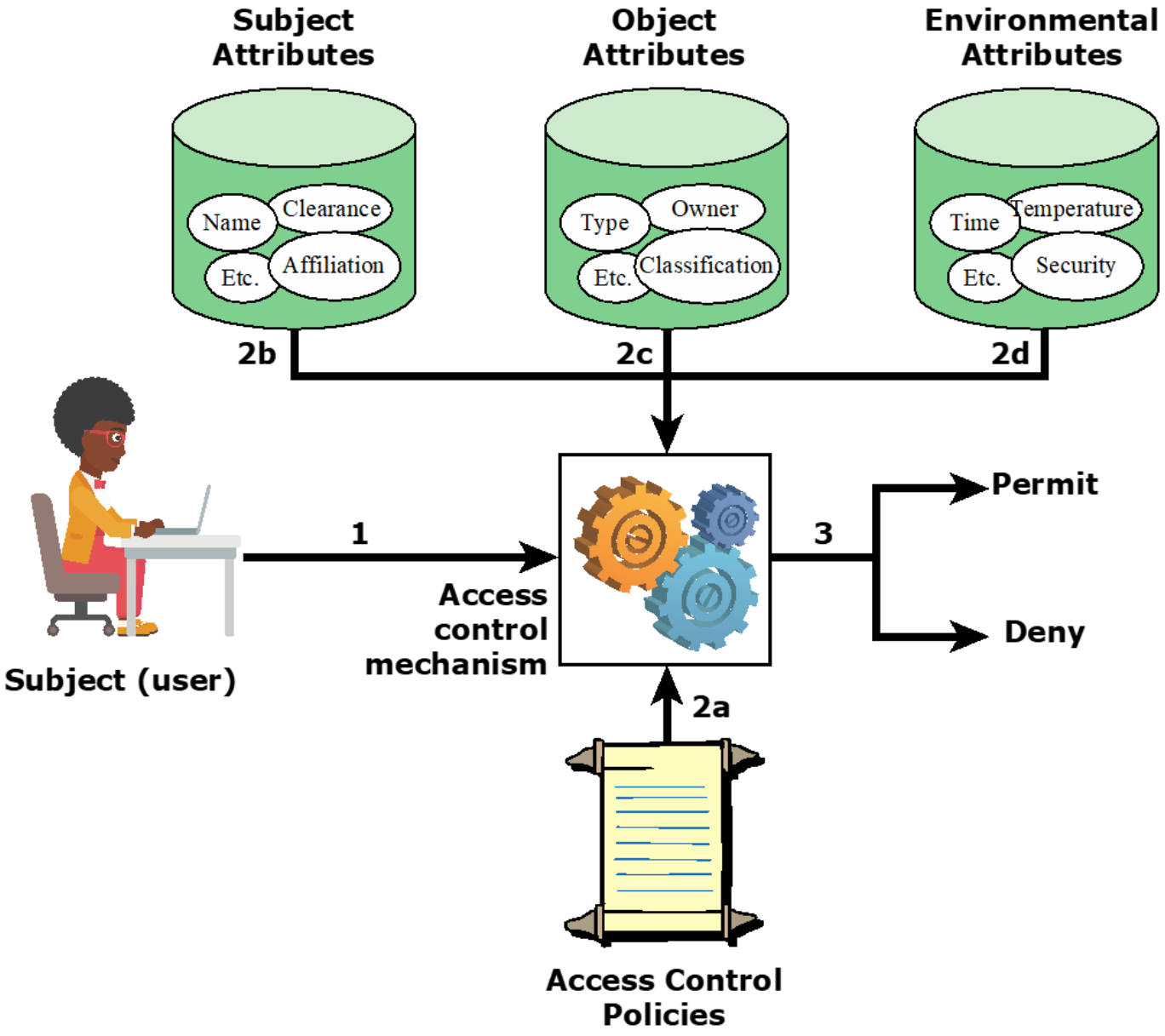


Figure 4.10 ABAC Scenario

ABAC Policies

A policy is a set of rules and relationships that govern allowable behavior within an organization, based on the privileges of subjects and how resources or objects are to be protected under which environment conditions

Typically written from the perspective of the object that needs protecting and the privileges available to subjects

Privileges represent the authorized behavior of a subject and are defined by an authority and embodied in a policy

Other terms commonly used instead of privileges are: rights, authorizations, and entitlements

Identity, Credential, and Access Management (ICAM)

- A comprehensive approach to managing and implementing digital identities, credentials, and access control
- Developed by the U.S. government
- Designed to:
  - Create trusted digital identity representations of individuals and nonperson entities (NPEs)
  - Bind those identities to credentials that may serve as a proxy for the individual of NPE in access transactions
    - A credential is an object or data structure that authoritatively binds an identity to a token possessed and controlled by a subscriber
  - Use the credentials to provide authorized access to an agency's resources

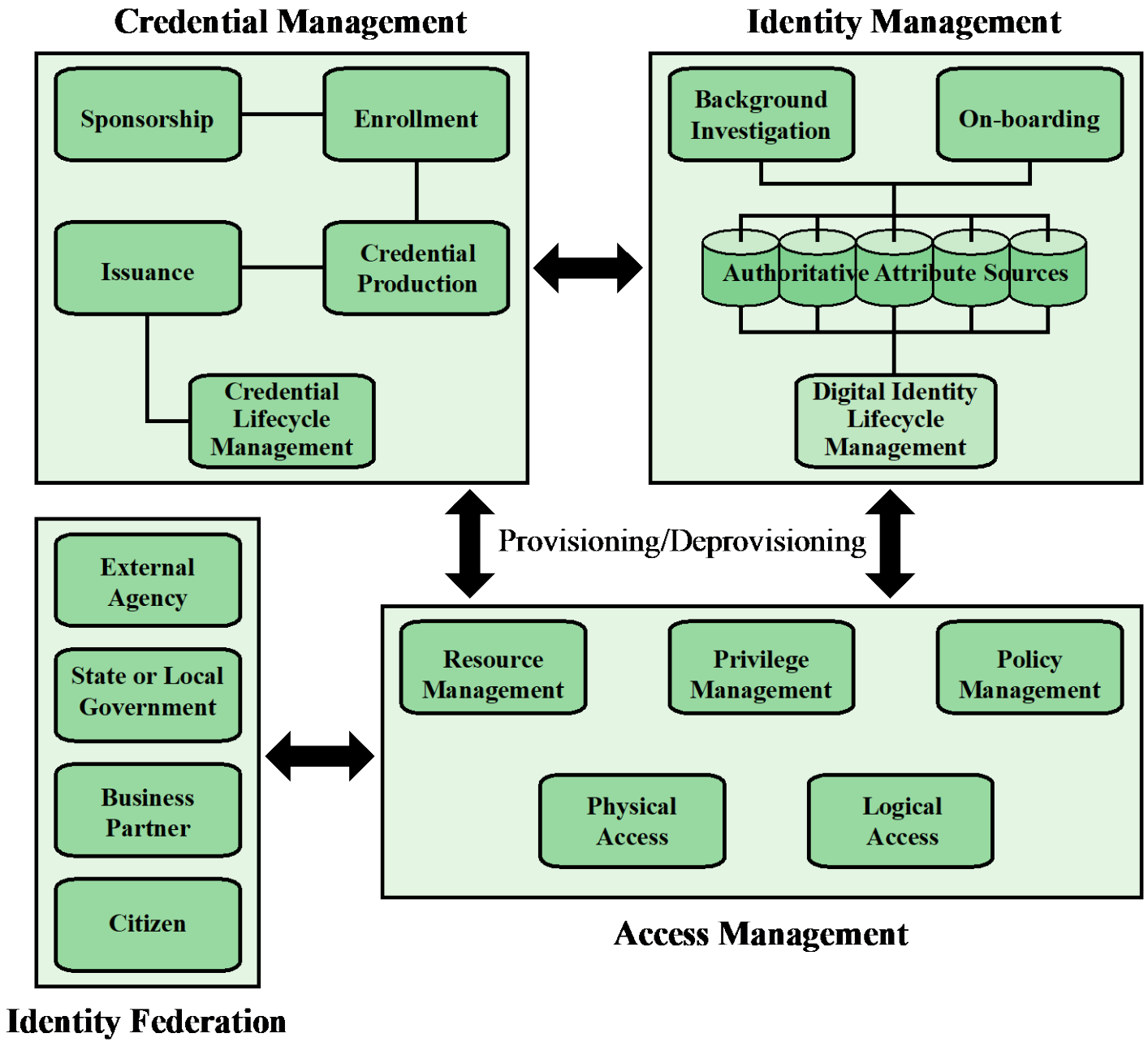


Figure 4.12 Identity, Credential, and Access Management (ICAM)

Identity Management

- Concerned with assigning attributes to a digital identity and connecting that digital identity to an individual or NPE
- Goal is to establish a trustworthy digital identity that is independent of a specific application or context
- Most common approach to access control for applications and programs is to create a digital representation of an identity for the specific use of the application or program
- Maintenance and protection of the identity itself is treated as secondary to the mission associated with the application
- Final element is lifecycle management which includes:
  - Mechanisms, policies, and procedures for protecting personal identity information
  - Controlling access to identity data
  - Techniques for sharing authoritative identity data with applications that need it
  - Revocation of an enterprise identity

Credential Management

The management of the life cycle of the credential

Examples of credentials are smart cards, private/public cryptographic keys, and digital certificates

Encompasses five logical components:

An authorized individual sponsors an individual or entity for a credential to establish the need for the credential

Credential Management

Encompasses five logical components:

The sponsored individual enrolls for the credential

- Process typically consists of identity proofing and the capture of biographic and biometric data
- This step may also involve incorporating authoritative attribute data, maintained by the identity management component

A credential is produced

- Depending on the credential type, production may involve encryption, the use of a digital signature, the production of a smart card or other functions

The credential is issued to the individual or NPE

A credential must be maintained over its life cycle

- Might include revocation, reissuance/replacement, reenrollment, expiration, personal identification number (PIN) reset, suspension, or reinstatement

Access Management

Deals with the management and control of the ways entities are granted access to resources

Covers both logical and physical access

May be internal to a system or an external element

Purpose is to ensure that the proper identity verification is made when an individual attempts to access a security sensitive building, computer systems, or data

Three support elements are needed for an enterprise-wide access control facility:

- Resource management
- Privilege management
- Policy management

Three support elements are needed for an enterprise-wide access control facility:

Resource management

- Concerned with defining rules for a resource that requires access control
- Rules would include credential requirements and what user attributes, resource attributes, and environmental conditions are required for access of a given resource for a given function

Privilege management

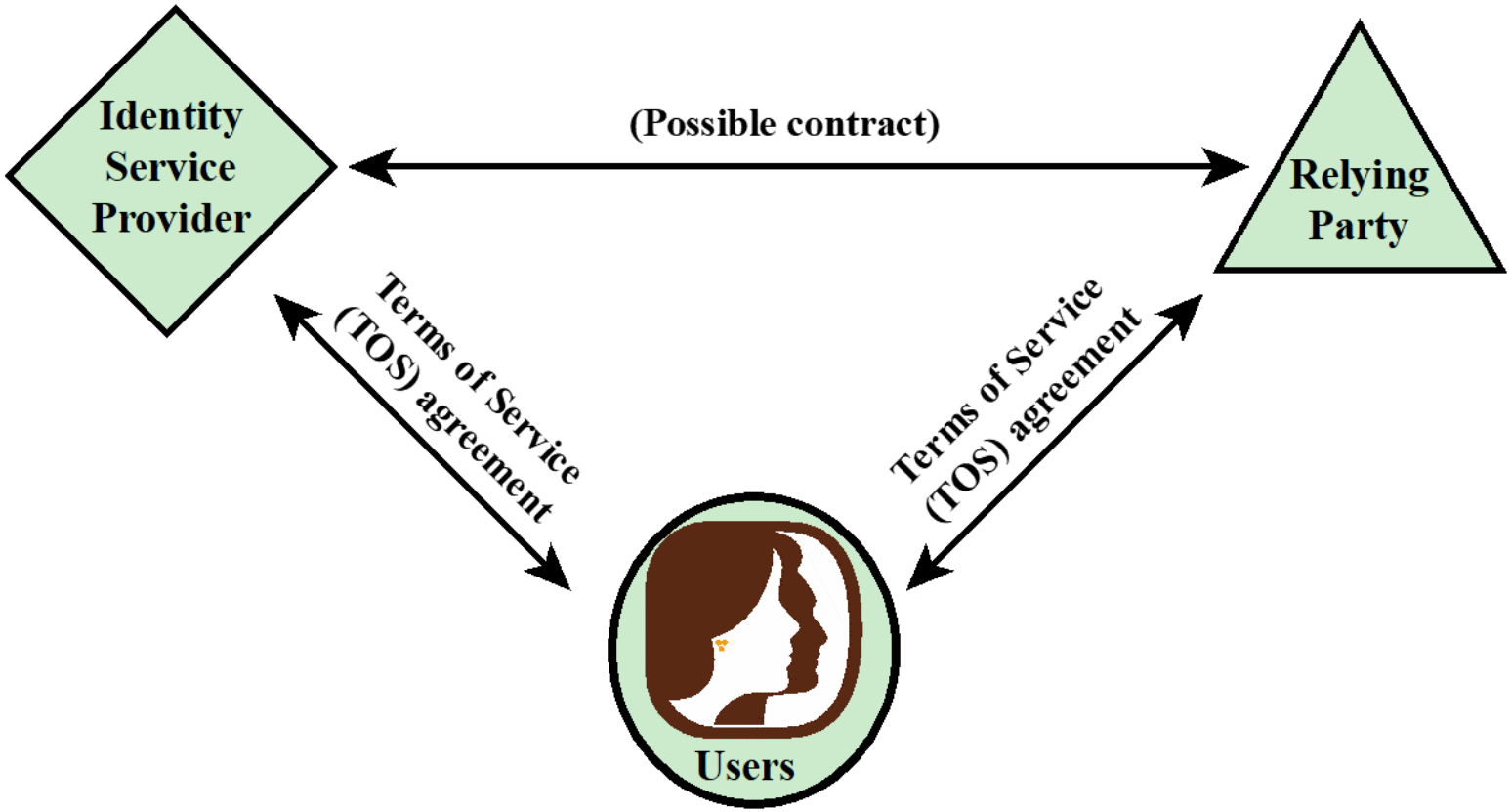
- Concerned with establishing and maintaining the entitlement or privilege attributes that comprise an individual's access profile
- These attributes represent features of an individual that can be used as the basis for determining access decisions to both physical and logical resources
- Privileges are considered attributes that can be linked to a digital identity

Policy management

- Governs what is allowable and unallowable in an access transaction

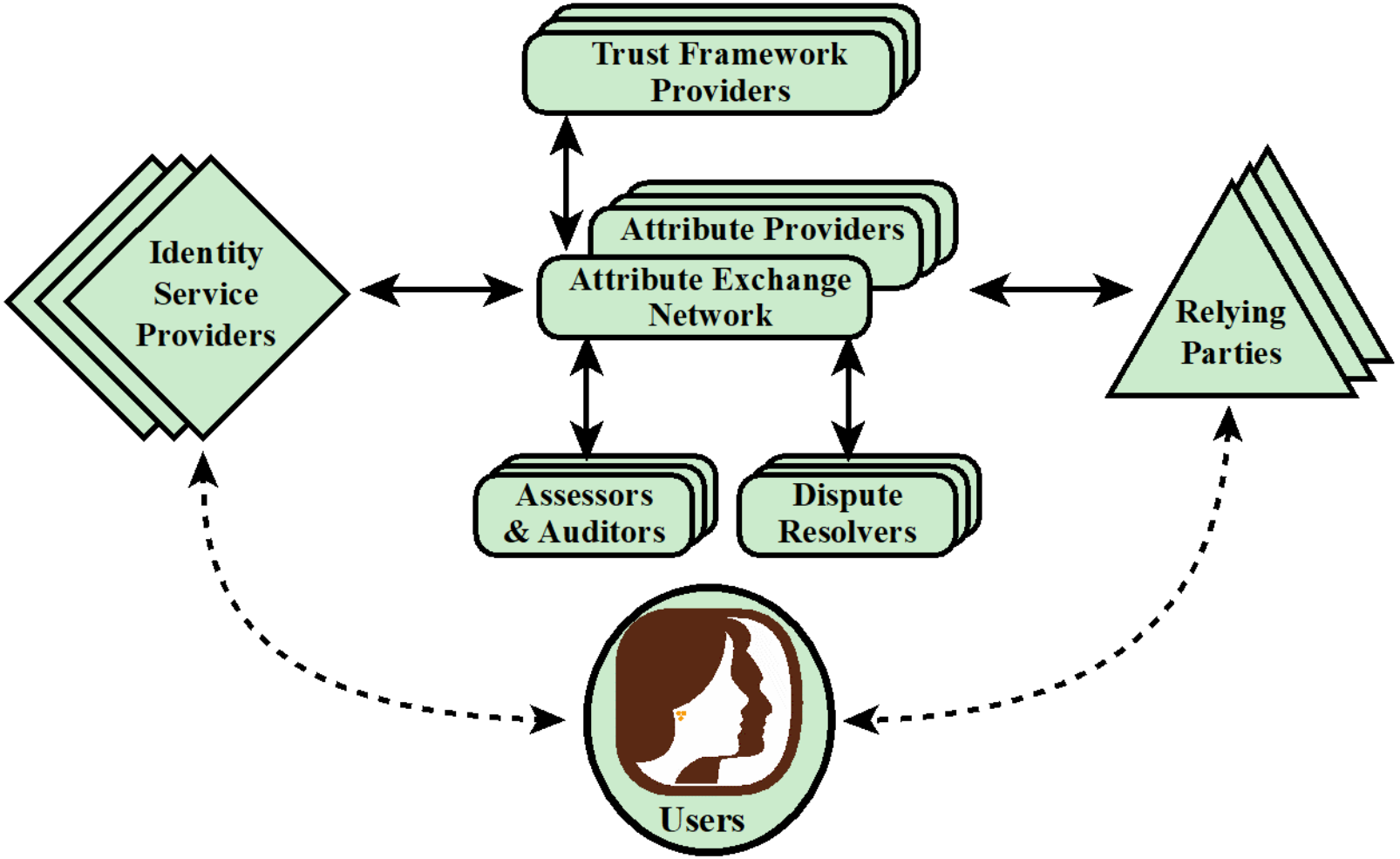
Identity Federation

- Term used to describe the technology, standards, policies, and processes that allow an organization to trust digital identities, identity attributes, and credentials created and issued by another organization
- Addresses two questions:
  - How do you trust identities of individuals from external organizations who need access to your systems
  - How do you vouch for identities of individuals in your organization when they need to collaborate with external organizations



(a) Traditional triangle of parties involved in an exchange of identity information

Figure 4.13 Identity Information Exchange Approaches



(B) Identity attribute exchange elements

Figure 4.13 Identity Information Exchange Approaches

Open Identity Trust Framework and others

OpenID

- An open standard that allows users to be authenticated by certain cooperating sites using a third party service

OIDF

- OpenID Foundation is an international nonprofit organization of individuals and companies committed to enabling, promoting, and protecting OpenID technologies

ICF

- Information Card Foundation is a nonprofit community of companies and individuals working together to evolve the Information Card ecosystem

OITF

- Open Identity Trust Framework is a standardized, open specification of a trust framework for identity and attribute exchange, developed jointly by OIDF and ICF

OIX

- Open Identity Exchange Corporation is an independent, neutral, international provider of certification trust frameworks conforming to the OITF model

AXN

- Attribute Exchange Network is an online Internet-scale gateway for identity service providers and relying parties to efficiently access user asserted, permissioned, and verified online identity attributes in high volumes at affordable costs

Table 4.5
Functions and Roles for Banking Example

(a) Functions and Official Positions

Role	Function	Official Position
A	financial analyst	Clerk
B	financial analyst	Group Manager
C	financial analyst	Head of Division
D	financial analyst	Junior
E	financial analyst	Senior
F	financial analyst	Specialist
G	financial analyst	Assistant
• • •	• • •	• • •
X	share technician	Clerk
Y	support e-commerce	Junior
Z	office banking	Head of Division

Table 4.5
Functions and Roles for Banking Example

(b) Permission Assignments

Role	Application	Access Right
A	money market instruments	1, 2, 3, 4
	derivatives trading	1, 2, 3, 7, 10, 12
	interest instruments	1, 4, 8, 12, 14, 16
B	money market instruments	1, 2, 3, 4, 7
	derivatives trading	1, 2, 3, 7, 10, 12, 14
	interest instruments	1, 4, 8, 12, 14, 16
	private consumer instruments	1, 2, 4, 7
• • •	• • •	• • •

(c) PA with Inheritance

Role	Application	Access Right
A	money market instruments	1, 2, 3, 4
	derivatives trading	1, 2, 3, 7, 10, 12
	interest instruments	1, 4, 8, 12, 14, 16
B	money market instruments	7
	derivatives trading	14
	private consumer instruments	1, 2, 4, 7
• • •	• • •	• • •

Summary

- Access control principles
  - Access control context
  - Access control policies
- Subjects, objects, and access rights
- Discretionary access control
  - Access control model
  - Protection domains
- UNIX file access control
  - Traditional UNIX file access control
  - Access control lists in UNIX
- Role-based access control
  - RBAC reference models
- Attribute-based access control
  - Attributes
  - ABAC logical architecture
  - ABAC policies
- Identity, credential, and access management
  - Identity management
  - Credential management
  - Access management
  - Identity federation
- Trust frameworks
  - Traditional identity exchange approach
  - Open identity trust framework
- Bank RBAC system

Practical 3

- Complete Problems 4.1 and 4.3 in your textbook.
- Submit your work in PDF online on the course website.
- Be warned about plagiarism!
- Submission deadline: Tuesday 27 August 2024, 09:00am
- Absolutely no late submissions will be allowed. No excuse of slow server, load shedding etc. No Doctor's note will be accepted unless you were booked off for the entire time from when the prac was released until its submission deadline.
- No email submissions will be accepted.

Problem 4.1

- For the DAC model discussed in Section 4.3, an alternative representation of the protection state is a directed graph. Each subject and each object in the protection state is represented by a node (a single node is used for an entity that is both subject and object). A directed line from a subject to an object indicates an access right, and the label on the link defines the access right.
- **a.** Draw a directed graph that corresponds to the access matrix of Figure 4.2a. See https://www.youtube.com/watch?v=by1zmpTxXIk if you do not know what a directed graph is.
- **b.** Draw a directed graph that corresponds to the access matrix of Figure 4.3.
- **c.** Is there a one-to-one correspondence between the directed graph representation
- and the access matrix representation? Explain.

Problem 4.3

- The VAX/VMS operating system makes use of four processor access modes to
- Facilitate the protection and sharing of system resources among processes. The access mode determines:
  - **Instruction execution privileges:** What instructions the processor may execute
  - **Memory access privileges:** Which locations in virtual memory the current instruction may access
- The four modes are as follows:
  - **Kernel:** Executes the kernel of the VMS operating system, which includes memory management, interrupt handling, and I/O operations
  - **Executive:** Executes many of the operating system service calls, including file and record (disk and tape) management routines
  - **Supervisor:** Executes other operating system services, such as responses to user commands
  - **User:** Executes user programs, plus utilities such as compilers, editors, linkers, and Debuggers

…Continued on next slide…

Problem 4.3 (Continued)

- A process executing in a less-privileged mode often needs to call a procedure that executes in a more-privileged mode; for example, a user program requires an operating system service. This call is achieved by using a change-mode (CHM) instruction, which causes an interrupt that transfers control to a routine at the new access mode. A return is made by executing the REI (return from exception or interrupt) instruction.
- **a.** A number of operating systems have two modes: kernel and user. What are the advantages and disadvantages of providing four modes instead of two?
- **b.** Can you make a case for even more than four modes?