CIS 4360
Secure Computer Systems
Access Control

Professor Qiang Zeng
Spring 2017
Previous Class

• Biometrics
  – Measurement and applications of human characteristics
• Applications
• Advantages and Disadvantages
• False rejection rate; false acceptance rate
• Case Studies
  – Fingerprint
  – Iris
Outline

• Concepts of Access Control
• Access Matrix, Access Control List, Capabilities
• Main Types of Access Control Policies
  – DAC
  – MAC
  – RBAC
Access Control

• **Access Control**: the process of restricting access to resources according to a security policy
  – A security policy regulates who can do what
  – Access control implements a security policy

• **Authorization**: the action of granting access

• Access Control usually starts from **Authentication**
  (i.e., verifying the identity of a user)
Examples of Access Control

• The Temple’s Blackboard system
• Operating Systems
• Database systems
• Governments
• Intelligence Departments
• …
Consider “Entering a Temple building” as an example, point out “Policy”, “Access Control”, “Authentication”, “Authorization”

Policy: only Temple students, faculty and employees or verified visitors are allowed to enter the building.

Access Control: the process of restricting people who can enter the building.

Authentication: verifying the identity of a person.

Authorization: allowing a person to enter the building.
Concepts

- **Subjects**: entities to access resources
  - Users, processes, threads

- **Objects**: resources whose access is controlled
  - Files, relations, memory

- **Access Rights**: actions that are taken
  - Read, Write, Execute, Delete, Create, Search
Goals of Access Control

• Confidentiality (Secrecy)
• Integrity
Question

To achieve confidentiality, is it sufficient by correctly restricting the read operation only?

It is insufficient. A malicious or buggy subject (e.g., a process) may read information from a sensitive file and then write to a file accessible by public

Sensitive Object -> Subject -> Non-sensitive object -> Public

Therefore, the access control has to regulate not only read but also write
Access (Control) Matrix

- An **Access Matrix** describes the rights of each subject with regard to each object in an Access Control system **at some point of time**
- But it does NOT model the rules by which rights are changed; thus, it is not equal with the access control policy
Access Matrix

<table>
<thead>
<tr>
<th>User</th>
<th>File 1</th>
<th>File 2</th>
<th>File 3</th>
<th>File 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>User A</td>
<td>Own Read Write</td>
<td></td>
<td>Own Read Write</td>
<td></td>
</tr>
<tr>
<td>User B</td>
<td>Read</td>
<td>Own Read Write</td>
<td>Write</td>
<td>Read</td>
</tr>
<tr>
<td>User C</td>
<td>Read Write</td>
<td>Read</td>
<td></td>
<td>Own Read Write</td>
</tr>
</tbody>
</table>

Disadvantage: it does not scale well
Three Ways to Express the Access Matrix

• One Access Tuple per cell:
  – <subject, object, rights>
  – E.g., <Bob, File2, read/write>

• One Access Control List per object (column)

• One Capability List per subject (row)
Access Control Lists

• An ACL is a list of subjects and their rights to an object
• One ACL per object
• It is difficult to find out all files accessible by a given user
• Widely used in Unix/Linux/Windows
Access Control Lists in Unix

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

• A Capability List is the list of objects accessible by a subject and the corresponding rights
Capability in real-world

- int fd = open("/etc/passwd", O_RDWR);
- fd is an index into the process’s file descriptor table, which can be regarded as a runtime capability list
- Each file descriptor is a capability
  - For all subsequent read/write/seek operations, one critical parameter being passed is “fd”
- It is unforgeable by a user program, as the file descriptor table is stored in kernel space
Types of Access Control Policies

• Discretionary Access Control (DAC)
• Mandatory Access Control (MAC)
• Role-Based Access Control (RBAC)
• …
Discretionary Access Control (DAC)

- DAC means subjects themselves can grant rights to other subjects
  - E.g., in Unix/Linux, the owner of a file can set up and change the ACL of the file
- Convenient but cannot achieve the goals of confidentiality and integrity
  - Subjects make decisions about access permissions; the decisions may be bad decisions
Question

There are two ACLs defined in a DAC system, File 1: <Alice: write, Bob: read>, File 2: <Bob: write, Charlie: read>. The confidentiality goal is that “Alice does not leak info to Charlie”. Can this goal be achieved here?

No. Alice -> File1 -> Bob -> File2 -> Charlie
MAC

- A *mandatory access control (MAC)* policy is a means of assigning access rights based on regulations by a central authority.
- The underlying philosophy is that the information in a file belongs to the organization rather than the file owner. So it should be the organization who assigns access rights and regulates the information flow.
A Simple Example of MAC

• In Military department, there are four levels of clearance
  – Unclassified
  – Confidential
  – Secret
  – Top Secret

• Assume you, as an employee, created a file labeled as <“Secret”, Nuclear>
  – You are not allowed to decide who can access the file
  – People who have the “Secret” or “Top Secret” clearance and the Nuclear duty can access the file
Role Based Access Control (RBAC)

- In the real world, especially in enterprises, the responsibilities of a person change dynamically
  - In a large company, every day many people change their jobs
  - Is there a convenient way to access control?
- Role Based Access Control assign access rights to **roles** rather than **subjects**
- A *role* is a job function or title and can be translated to rights in a RBAC system
The Principle of Least Privilege

• A user can be assigned with multiple roles
• But when a user logs in, she can only activate one role
• This complies with the Principle of Least Privilege. That is, one is granted rights just needed to finish the intended task
Figure 4.6  Users, Roles, and Resources
Role vs. Group

• A role is a job title, while a group is a set of users
• A user can have zero or one active role at any given time, but can belong to many groups at any time
Summary

• Concepts
  – Access Control
  – Subject, Object

• Goals of Access Control
  – Confidentiality
  – Integrity

• Access Matrix
  – View of Columns: Access Control Lists
  – View of Rows: Capability Lists

• Types of Access Control Policies
  – DAC
  – MAC
  – RBAC
Writing Assignments

• In which scenarios DAC, MAC and RBAC should be used, respectively?
• Does RBAC belong to DAC or MAC?