CS2107 Live Class Lec6: Access control

$_/|/|U_Ch@NgRu!$

May 11, 2021

Mu Changrui

1 Overview of Access Control

Computer system is also a layered structure: Example of each layer:

Applications
Services
Operating System
OS Kernel
Hardware

- Applications: Browser
- Service: Java Virtual Machine
- Operating System : IOS
- OS Kernel: system calls to handle memory
- hardware: CPU

2 Security Boundary/Perimeter

A security boundary is a boundary as such

- The parts of the system that can malfunction without compromising the protection mechanism lie outside this
- The parts of the system that can be used to disable the protection mechanism lie within the perimeter

System security is quite different from network security. The main concern in system security is that there are many subjects accessing the objects and boundaries need to be had between them.

The object can be data and file whereas the subject can be users

3 Access Control Model

Access control is the selective restriction of access of access to a place or other resources
Access control model gives a way to specify and enforce such restriction on the subject, objects and actions
There are four parties in access control models:

- Principal, or subject
- Operation
- Reference Monitor
- Object

In general, a principal wants to access an object with some operation. The reference monitor either grants or denies the access.
There are main types of access:

1. Observe: e.g. read a file
2. Alter: e.g. write a file
3. Action: execute a program

There are two ways to determine the access right to objects:

1. Discretionary access vontrol(DAC): the owner of the object decides the rights
2. Mandatory Access control(MAC): A system-wide policy decides

Mu Changrui

4 Access Control Matrix

We can use an access control matrix to specify the access right of a particular principle to a particular object. The rows are principals and columns are files. Each entries specifies access right of the principle at this row to the file at this collumn
For the entries, there are five types:

- r: read
- w: write
- x: execute
- s: execute as owner

- owner

Access control matrix is too large to be explicitly stored. We can store it in the fashion of linked list:

- Access control list(ACL)
  Access control list is of the following form

$$\begin{tikzcd}
\text{Object}_1 \arrow[r] \arrow[d] & \{\text{subject}_1, \text{right}_{11}\} \arrow[r] & \cdots \\
\text{Object}_2 \arrow[r] & \{\text{subject}_1, \text{right}_{12}\} \arrow[r] & \cdots
\end{tikzcd}$$

- Capabilities
  Capabilities is of the following form

$$\begin{tikzcd}
\text{Subject}_1 \arrow[r] \arrow[d] & \{\text{Object}_1, \text{right}_{11}\} \arrow[r] & \cdots \\
\text{Subject}_2 \arrow[r] & \{\text{Object}_1, \text{right}_{21}\} \arrow[r] & \cdots
\end{tikzcd}$$

Remark: the subscript of right is the index of right in the corresponding access control matrix Either implementation has a trade-off of time complexity with aim of better space complexity. However, the lists could still be too huge to manage. To resolve this, we use ”group” to represent groups of subjects and objects and define access right on the groups

Mu Changrui

5 Intermediate control

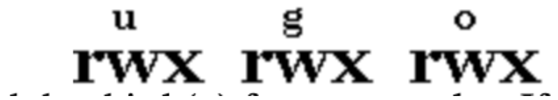
There are several types of intermediate control

5.1 Group

In Unix file permission, access control list control specify the rights for

1. owner
2. group
3. world

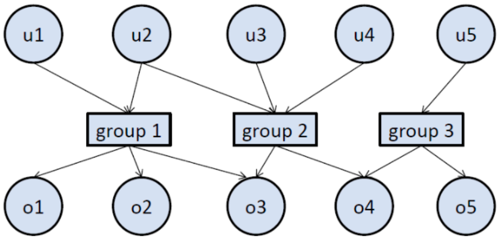
in the format of



e.g.
-rwxr-xr–
drwxr-xr—
The permissions are broken into groups of threes, and each position in the group denotes a specific permission, in the order of read(r), write(w), execute(x)

- The first three characters(2-4) represent the permission for the file's owner.
- The second group of characters(5-7) consists of the permission for the group to which the file belongs.
- The last group of three characters(8-10) represents the permission for everyone else

Subjects in the same group have the same rights



In Unix, groups can only be created by root

6 Privileges

Privilege can be used to describe access right

7 Role

The grouping can determined by the "role" of the subject. A role associates with a collection of procedures. In order to carry out these procedures, access rights to certain objects are required The access right to objects by subjects is determined by **least privilege principle**, which states the access right that are not required to complete the assigned role will not be granted

Mu Changrui

8 Protection Ring

In protection rings, each object and subject is assigned a number. Whether a subject can access an object can be determined by their respective assigned number. Objects with smaller number are more important
We call processes with the lower ring number as have higher privilege since a subject cannot access an object with smaller ring number numbers. It can only do so if itds privilege is escalated.
Unix has only 2 rings, superuser and user
In the following models, objects are subjects are divided into linear levels, e.e. level 0, level 1, etc. Higher level corresponds to higher security

1. Bell-LaPadula Model, which ensures confidentiality of higher level objects by enforcing
    - No read-up: A subject has only read access to objects whose security level is below the subjects;s current clearance level
    - No write-down: A subject has write access to objects whose security level is higher than its current clearance level
2. Biba Model< which ensures integrity of higher level objects by enforcing
    - No write-up: A subject has only write access to objects whose security level is below the subjects' current clearance level
    - No read-down: a subject has only read access to object whose security level is higher than its current clearance level

Mu Changrui