03 - Access Control

2024年8月26日 星期一 13:29

03 - Access Control

Australian National University

Access Control

COMP2700 Cyber Security Foundations

Slides prepared based partly on Chapter 5 of Gollmann's "Computer Security", Wiley, 2011

1

Australian National University

Outline

- Fundamental terminology
  - Principals & subjects, access operations
- Authentication & authorisation
- Access control structures:
  - Access control matrix
  - Capabilities & access control list (ACL)
  - Discretionary & mandatory access control

DAC & MAC

2

Australian National University

Access Control: Policy vs Mechanism

- A *security policy* is a statement of what is, and what is not, allowed.
- A *security mechanism* is a method, tool, or procedure for enforcing a security policy.
- Example:
  - Policy: A student is not allowed to sit in an exam on behalf of another student.
  - Mechanism: Id check during exam.

3

Australian National University

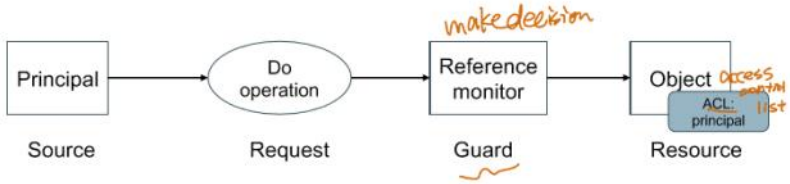
Security Policies

- Access control enforces operational security policies.
- A policy specifies who is allowed to do what.
- The active entity requesting access to a resource is called **principal**.
- The resource access is requested for is called **object**.
- **Reference monitor** is the abstract machine enforcing access control; guard mediating all access requests.

4

Australian National University

Authentication and Authorization



"If s is a statement, authentication answers the question 'Who said s?' with a principal. Thus principals make statements: this is what they are for. Likewise, if o is an object, authorization answers the question 'Who is trusted to access o?' with a principal."

B. Lampson, M. Abadi, M. Burrows, E. Wobber: Authentication in Distributed Systems: Theory and Practice, ACM Transactions on Computer Systems, 10(4), pages 265-310, 1992

5

Australian National University

Authentication and Authorization

- Authentication: reference monitor verifies the identity of the principal making the request.
- Authorisation: reference monitor decides whether access is granted or denied.
- Reference monitor has to find and evaluate the security policy relevant for the given request.

Australian National University

Users and User Identities

- Requests to reference monitor do not come directly from a **user** or a **user identity**, but from a **process**.
- In the language of access control, the process "speaks for" the user (identity).
- The active entity making a request within the system is called the **subject**.

Australian National University

Principals and Subjects

- A principal is an entity that can be granted access to objects or can make statements affecting access control decisions.
  - Example: user ID
- Subjects operate on behalf of (human users we call) principals; access is based on the principal's name bound to the subject in some unforgeable manner at authentication time.
  - Example: process (running under a user ID)

Australian National University

Access Operations and Access Rights

- On the most elementary level, a subject may
  - observe – look at the contents of an object, or
  - alter – change the contents of an object.
- Some fundamental policies can be expressed with these basic access modes.
  - For practical purposes a richer set of operations is more convenient.
- Access right (privilege/permissions): right to perform an (access) operation.

9

Australian National University

Access Rights: Bell-LaPadula model

- Bell-LaPadula model (see [Gollmann] chapter 11) has four access rights:
  - execute
  - read
  - append, also called blind write
  - write
- Mapping between access rights and access modes:

	execute	append	read	write
observe			X	X
alter		X		X

仅允许执行操作，但不允许读取或修改数据。

允许在不读取现有内容的情况下追加新数据，例如日志文件写入。

10

Australian National University

Access Rights: Bell-LaPadula model

- In a multi-user O/S, users open files to get access.
  - Files are opened for read or for write access so that the O/S can avoid conflicts like two users simultaneously writing to the same file.
- Write access usually includes read access.
  - A user editing a file should not be asked to open it twice; hence, write includes observe and alter mode.
- Few systems implement append.
  - Allowing users to alter an object without observing its content is rarely useful (exception: audit log).
- A file can be used without being opened (read).
  - Example: use of a cryptographic key; this can be expressed by an execute right that includes neither observe nor alter mode.

11

Australian National University

文件访问权说明

- **多用户操作系统**中，用户通过打开文件来获取访问权限。
  - 文件可以以读取或写入模式打开，以防止多个用户同时写入同一文件导致冲突。
- **写入权限通常包括读取权限**：
  - 用户编辑文件时无需多次打开，因此**写入权限**通常包含观察和修改模式。
- **追加权限**在系统中较少实现**：
  - 追加权限允许用户在不查看内容的情况下修改对象，通常用于**审计日志（audit log）**，以防止数据篡改。
- **文件可以在不打开的情况下使用（无需读取）**：
  - 例如使用**加密密钥**时，可以通过“执行”权限来操作，而无需观察或修改内容

ell-LaPadula 模型的特点

- **强制访问控制**：用户只能读取其授权级别下的数据，不能读取更高级别的数据（“无读高”原则）。
- **写入限制**：用户只能向其授权级别或更高的安全级别写入数据（“无写低”原则）

Australian National University

Access Rights: Unix/Linux

- Three access operations on files:
  - read: from a file
  - write: to a file
  - execute: a file
- Access operations on directories:
  - read: list contents
  - write: create or rename files in the directory
  - execute: search directory
- Deleting files/subdirectories handled by access operations in the directory.

Australian National University

Administrative rights

The rights to modify access rights, e.g.,

- Rights for creating and deleting files expressed by access control on the directory (Unix).
- Specific create and delete rights (Windows, OpenVMS).
- Specific rights like grant and revoke in database management.
- Rights to modify access control list in Windows.

对系统和资源的**访问控制权**进行修改和管理的能力

Australian National University

Access Control Structures

- The structures used for capturing security policies.
- Two requirements:
  - It should help in expressing desired access control policy.
  - We should be able to check the intended policy has been captured correctly.
- Three basic structures:
  - Access control matrix
  - Capability list
  - Access control list

Australian National University

Access Control Matrix

- Access control matrix captures each combination of subject and object and their access rights.
  - Rows → subjects
  - Columns → objects
  - Entries → access operations
- Given an access matrix M, we write $M_{s,o}$ to mean the entry in M whose row corresponds to subject s and whose column corresponds to object o.
- Each entry $M_{s,o}$ contains a set of access rights of subject s for object o, e.g, read, write, and execute for files.

Australian National University

Example: a simple system

- Consider a system with two processes (subjects) P1 and P2, two memory segments (M1 and M2) and two files (F1 and F2).
- Each process has its own private segment and owns one file.
- Neither process can control the other process.
- Permitted access operations include: read (R), write (W), execute (E), and ownership (Own)

	M1	M2	F1	F2	P1	P2
P1	R,W,E		Own,R,W			
P2		R,W,E		Own,R,E		

- 该系统包含：
  - **两个进程**（subjects）：P1 和 P2。
  - **两个内存段**（memory segments）：M1 和 M2。
  - **两个文件**（files）：F1 和 F2。
- **每个进程**有自己的**私有内存段**，并**拥有一个文件。**
- **进程之间不能互相控制**（即，一个进程无法修改另一个进程的资源）。

Australian National University

Capabilities

- Focus on the subject
  - access rights stored with the subject
  - capabilities = rows of the access control matrix
- Consider an access control matrix for principals Alice & Bob, and objects (files) 'bill.doc', 'edit.exe', 'fun.com'.

	bill.doc	edit.exe	fun.com
Alice	-	{exec}	{exec,read}
Bob	{read,write}	{exec}	{exec,read,write}

- Capabilities associated with Alice is just a row in the access matrix:

Alice	edit.exe: {exec}	fun.com: {exec,read}

Australian National University

Access control list

- Access control list (ACL) mechanism focuses on the protection of objects.
  - access rights of principals stored with the object
  - ACLs = columns of the access control matrix
    - 在**访问控制矩阵**中，ACL 对应的是**矩阵的列**
- Each object has an ACL, specifying the subjects (user IDs, user groups, etc) and the access rights of each of the subjects.

Australian National University

Example: ACL and access matrix

- Consider an access control matrix for principals Alice & Bob, and objects (files) 'bill.doc', 'edit.exe', 'fun.com'.

	bill.doc	edit.exe	fun.com
Alice	-	{exec}	{exec,read}
Bob	{read,write}	{exec}	{exec,read,write}

- An ACL for file 'fun.com' is just a column in the access matrix:

fun.com	Alice: {exec,read}	Bill: {exec,read,write}

Australian National University

Example: Unix file permission

- In Unix, each file has an ACL with three entries corresponding to:
  - The owner's access right
  - The access rights of all users in the owner's group
  - The access rights of all others.
- Example:

num. link

```
-rwxr-xr-x  1 bob  staff  1163090 27 Mar 10:24 test.txt
```

ACL — user — user's group — file name

Access rights: r (read), w (write), x (execute)

x: execute 执行

Australian National University

Example: Unix file permission

- ACL is represented as a bit string.
  - Bit 0 is used for indicating file type, not related to access control.
  - Bit 1, 2 and 3, correspond, respectively, to read, write and execute rights of the user.
  - Bit 4, 5 and 6 correspond to read/write/execute rights for the user's group.
  - Bit 7, 8 and 9 corresponds o read/write/execute rights of all others.

Australian National University

Example: Unix file permission

- When a particular bit is set, it is displayed with its corresponding rights (e.g., r, w or x).
- For example: -rwxr-xr-x means:
  - User (bob) has read, write and execute rights
  - Every member of the user's group (staff) has read and execute rights
  - Everyone else has read and execute rights.

Australian National University

Ownership

访问控制模型

Who is in charge of setting security policies?

- **Discretionary access control (DAC):** Define an owner for each resource and let the owner sets the policies.
  - Adopted in most modern operating systems
  - Focus on user identities – sometimes also called identity-based access control (IBAC).
- **Mandatory Access Control (MAC):** Impose system-wide policies on who are allowed to access what.
  - Policies refer to security labels of objects, e.g., confidential, top secret.
  - Mostly used in the defence sector.

Australian National University

Intermediate Controls 中间控制

All problems in computer science can be solved by another layer of indirection. -David Wheeler

- For large systems/organisations, intermediate layers can be introduced between subjects and objects to create more manageable policies.
- Examples:
  - Grouping of users
  - Grouping of procedures into *roles* -- role-based access control (RBAC)
  - Introduce hierarchies into access control, e.g., privilege level.

Australian National University

Summary sudo

- Basic terminologies in access control.
- Access control involves authentication 认证 and authorization 授权.
- Access control matrix serves as a reference data structure.
  - In practice different methods are used to represent the access control matrix.
- Different paradigms of access control:
  - Centered 数据 on identity (IBAC, RBAC), or systems (MAC).

Australian National University

Further Reading

- D. Denning. “Cryptography and Data Security”, Addison-Wesley, 1983. Chapter 4 (Access Control).
  - http://faculty.nps.edu/dedennin/publications/Denning-CryptographyDataSecurity.pdf
- R. Sandhu, D. Ferraiolo, and R. Kuhn: *The NIST Model for Role-Based Access Control: Towards a Unified Standard*, Proceedings of the 5th ACM Workshop on Role-Based Access Control, Berlin, Germany, July 26-27, 2000
  - http://csrc.nist.gov/rbac/sandhu-ferraiolo-kuhn-00.pdf