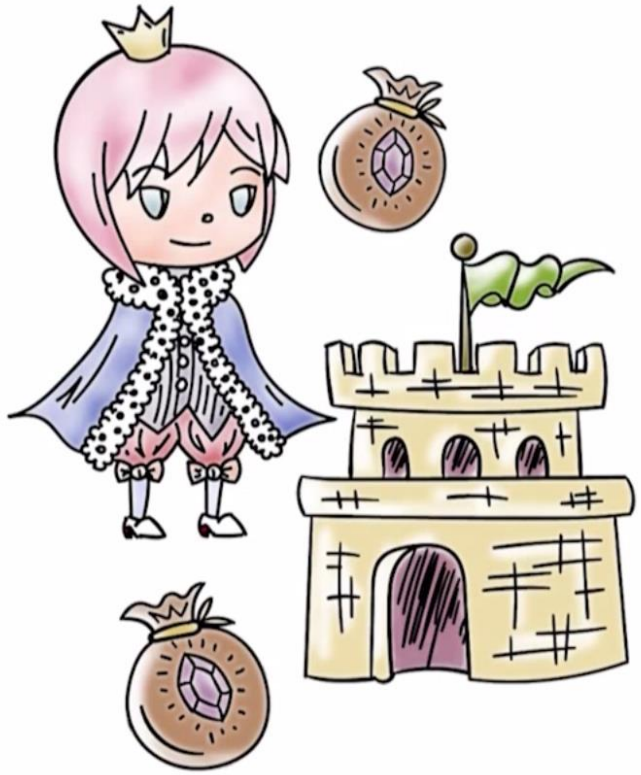
Access Control
Lesson Introduction

- Understand the **importance of access control**
- **Explore ways** in which access control can be implemented
- Understand **how access control** is implemented

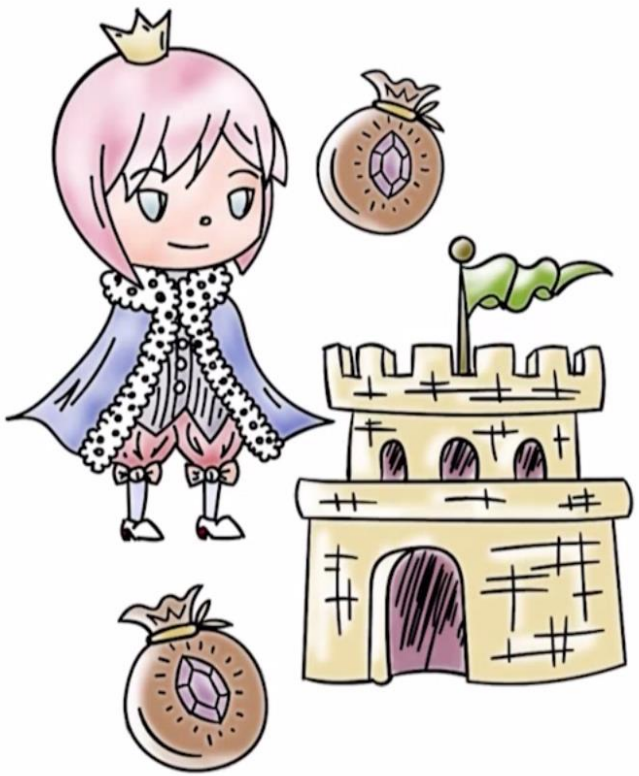
Controlling Accesses to Resources



- **TCB** (reference monitor) sees a request for a resource, how does it decide whether it should be granted?

- **Example:** Should John's process making a request to read a certain file be allowed to do so?

Controlling Accesses to Resources



- **Authentication** establishes the source of a request (e.g., John's UID)
- **Authorization** or access control answers the question if a certain source of a request (User ID) is allowed to read the file
- **Subject who owns a resource (creates it) should be able to control access to it (sometimes this is not true)**

Controlling Accesses to Resources

- **Access Control**
- Basically, it is about who is allowed to access what.
- Two parts
  - **Part I:** Decide who should have access to certain resources (access control policy)
  - **Part II:** Enforcement – only accesses defined by the access control policy are granted.
- **Complete mediation** is essential for successful enforcement

Access Control Matrix (ACM)

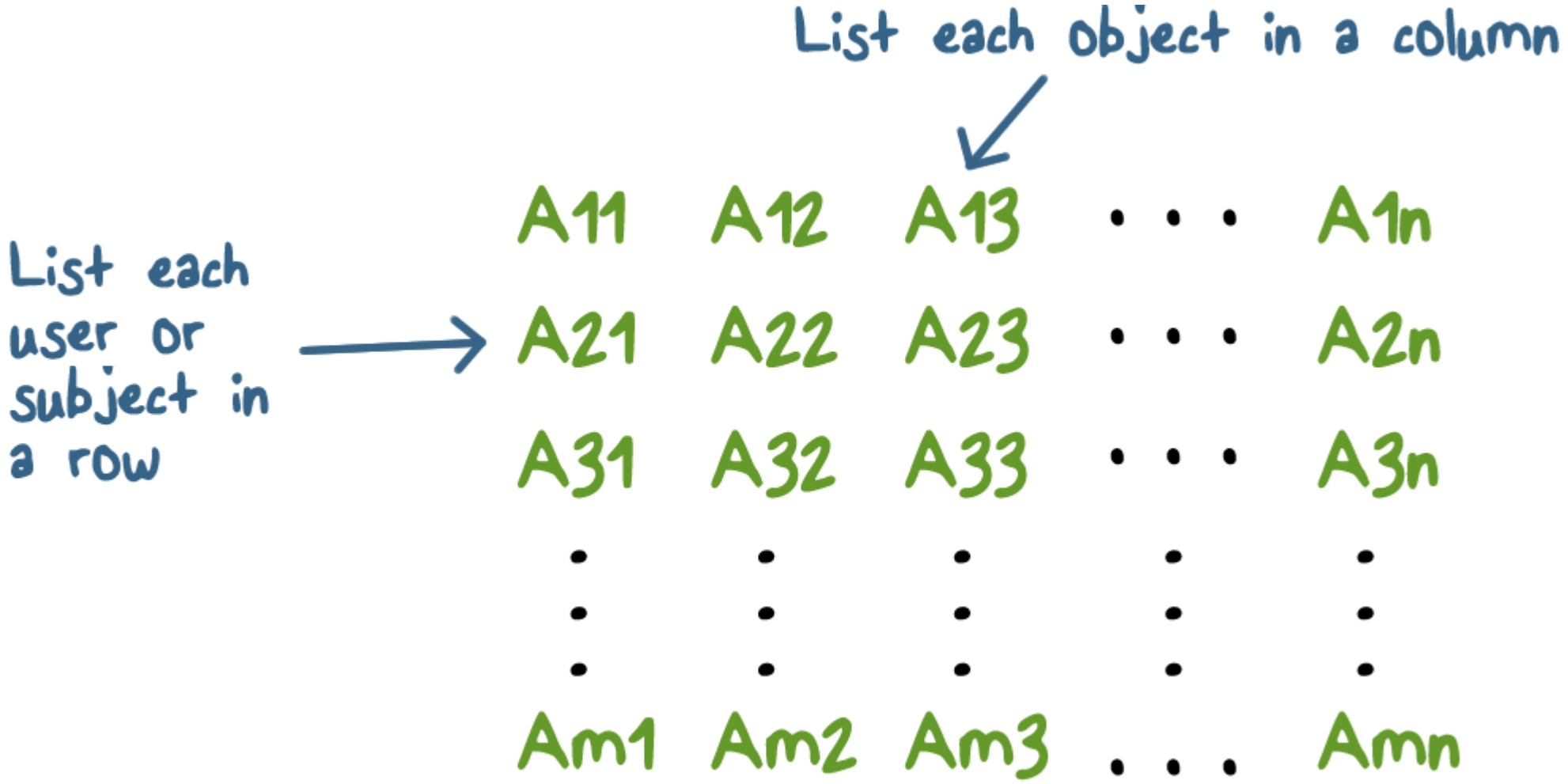
- An access control matrix (ACM)
  abstracts the state relevant to access control.
- Rows of ACM correspond to users/subjects/groups
- Columns correspond to resources that need to be protected.
- **ACM defines who can access what**
  - ACM [U,O] define what access rights user U has for object O.

Implementing Access Control

List all processes and subjects in a matrix

$$
\begin{matrix}
A_{11} & A_{12} & A_{13} & \cdots & A_{1n} \\
A_{21} & A_{22} & A_{23} & \cdots & A_{2n} \\
A_{31} & A_{32} & A_{33} & \cdots & A_{3n} \\
\vdots & \vdots & \vdots & \vdots & \vdots \\
A_{m1} & A_{m2} & A_{m3} & \cdots & A_{mn}
\end{matrix}
$$

Access Control Matrix (ACM)



Data Confidentiality Quiz

Select the best answer to complete this sentence:

A file is created by a certain user who becomes its owner. The owner can choose to provide access to this file to other users. If file data confidentiality is desired, the owner should control who has...

- ☐ Read access to the file
- ☐ Write access to the file
- ☐ Both read and write access to the file

Determining Access Quiz

Select the best answer to the question:

The access control policy in a system can either define positive access for a certain subject or can specify that the subject be denied access. Consider a case where subject Alice belongs to a group All-Students. The system specifies that members of the group All-Students be able to read file foo but Alice is denied access for it. In such a case, what should the system do?

- ☐ Alice has access because she is member of All-Students so she must be allowed to read foo
- ☐ Negative access should take precedence and Alice's request must be denied

Discretionary Access Control Quiz

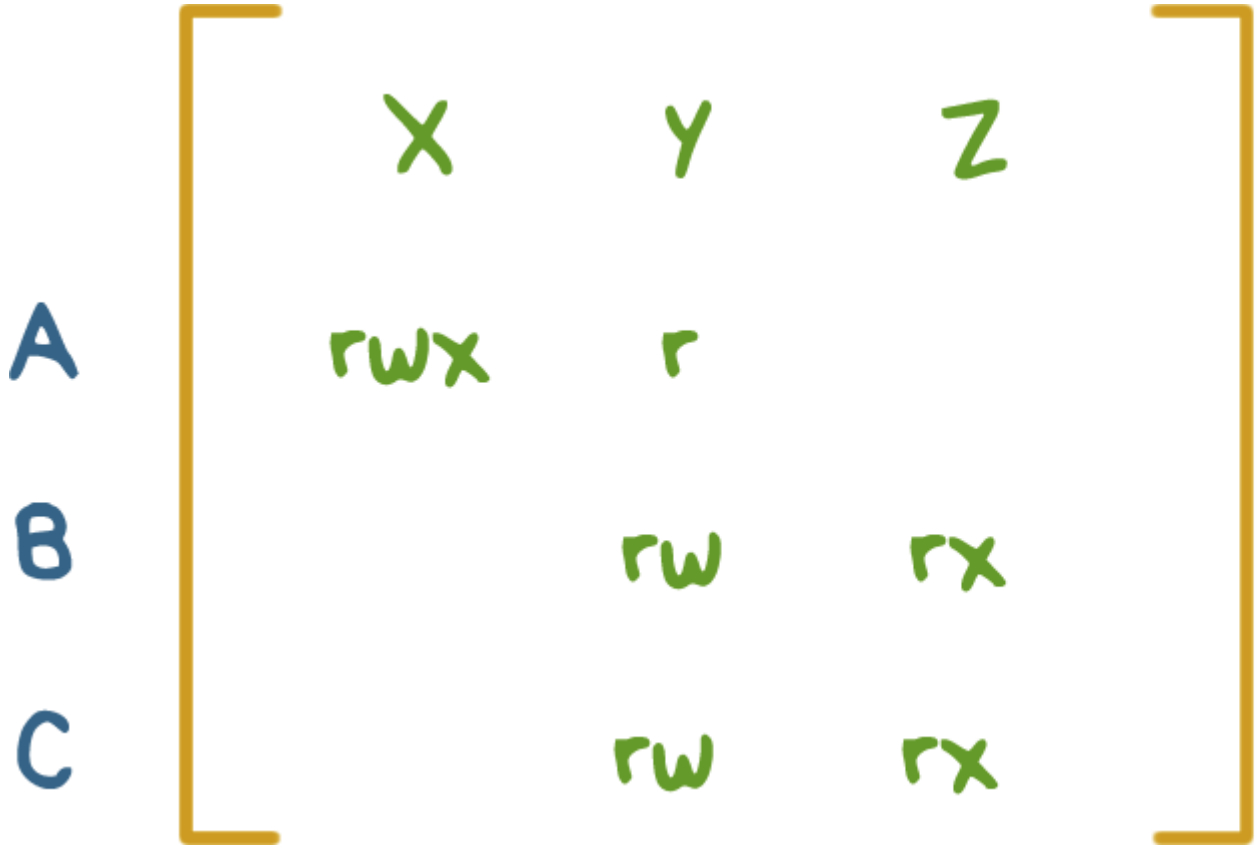
In discretionary access control, access to a resource is at the discretion of its owner. Let us assume owner Alice of file foo can choose to grant read access to foo to another user Bob but can prevent Bob from propagating this access right to others. Does this ensure that a third user, Charlie, can never read the data from foo?

- ☐ Yes, Charlie is not granted access so cannot read
- ☐ No, there may be another way for Charlie to access the data from foo

Implementing Access Control

- **Access control matrix is large**
- How do we represent it in the system?
  - Column for object Oi is [(ui1, rights1), (ui2, rights2),…]
    - Called **access control list or ACL**
    - Associated with each resource
  - For user ui, a row in the matrix is [(oi1, rights1), (oi2,rights2,….].
    - Called a capability-list or C-list.
    - Such a C-list stored for each user

Implementing Access Control



ACLs

X → [(A,rwx)]
Y → [(A,r)(B,rw)(C,rw)]
Z → [(B,rx)(C,rx)]

C-lists

A → [(X,rwx)(Y,r)]
B → [(Y,rw)(Z,rx)]
C → [(Y,rw)(Z,rx)]

ACL and C-Lists Implementation:

- **Where should an ACL be stored?**
  - In trusted part of the system
  - Consists of access control entries, or, ACEs
  - Along with other object meta-data
  - For example, file meta-data has a bunch of information where this can go as well
  - Checking requires traversal of the ACL

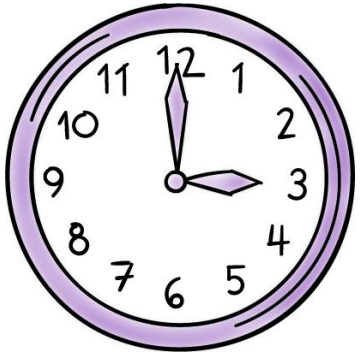
ACL and C-Lists Implementation:

C-list

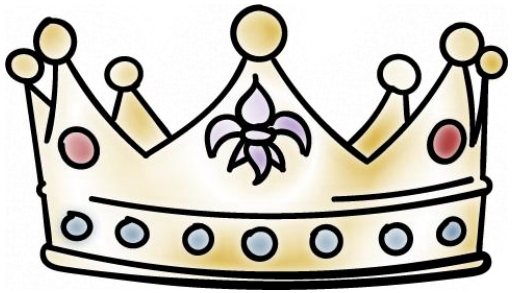
- **Where do C-lists go?**
  - A capability is an unforgeable reference/handle for a resource
  - User catalogue of capabilities defines what a certain user can access
  - Can be stored in objects/resources themselves (Hydra)
  - Sharing requires propagation of capabilities

ACL and C Lists Implementation:

ACL **vs.** **C-list**



Efficiency



Accountability

Revocation

ACE Quiz

Select the best answer:

Alice goes to a movie theater and purchases a ticket for her favorite movie. She is allowed access to the movie because she has the ticket. The ticket is more like a...

- ☐ Access control entry
- ☐ Capability

ACE Access Quiz

Select the best answer:

Some operating systems (e.g., Windows) include deny or negative access rights. In this case, an access check procedure can terminate as soon as...

- ☐ A positive or grant access ACE is found for the requestor
- ☐ A negative or deny ACE is found
- ☐ The whole ACL must be traversed always

Revocation of Rights Quiz

Select the best answer:

Revocation of access certain access rights can be carried out easily in systems that use...

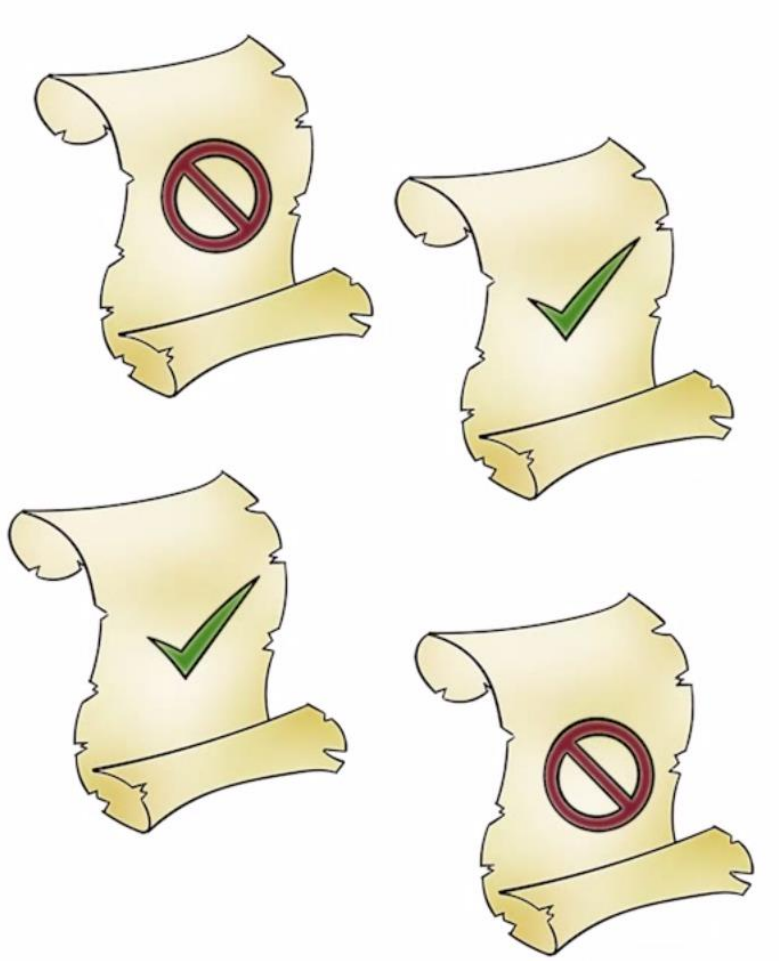
- ☐ ACLs
- ☐ C-lists

Access Control Implementation

How is Access Control Implemented in Unix-like Systems?

- In Unix, **each resource looks like a file**.
- Each file has an owner (UID) and access is possible for owner, group and everyone (world).
- **Permissions are read, write and execute.**
- Original ACL implementation had a compact fixed size representation (9 bits)
- **Now full ACL support is available in many variants** (Linux, BSD, MacOS,..)
- Few other things (sticky bit, setuid,…)

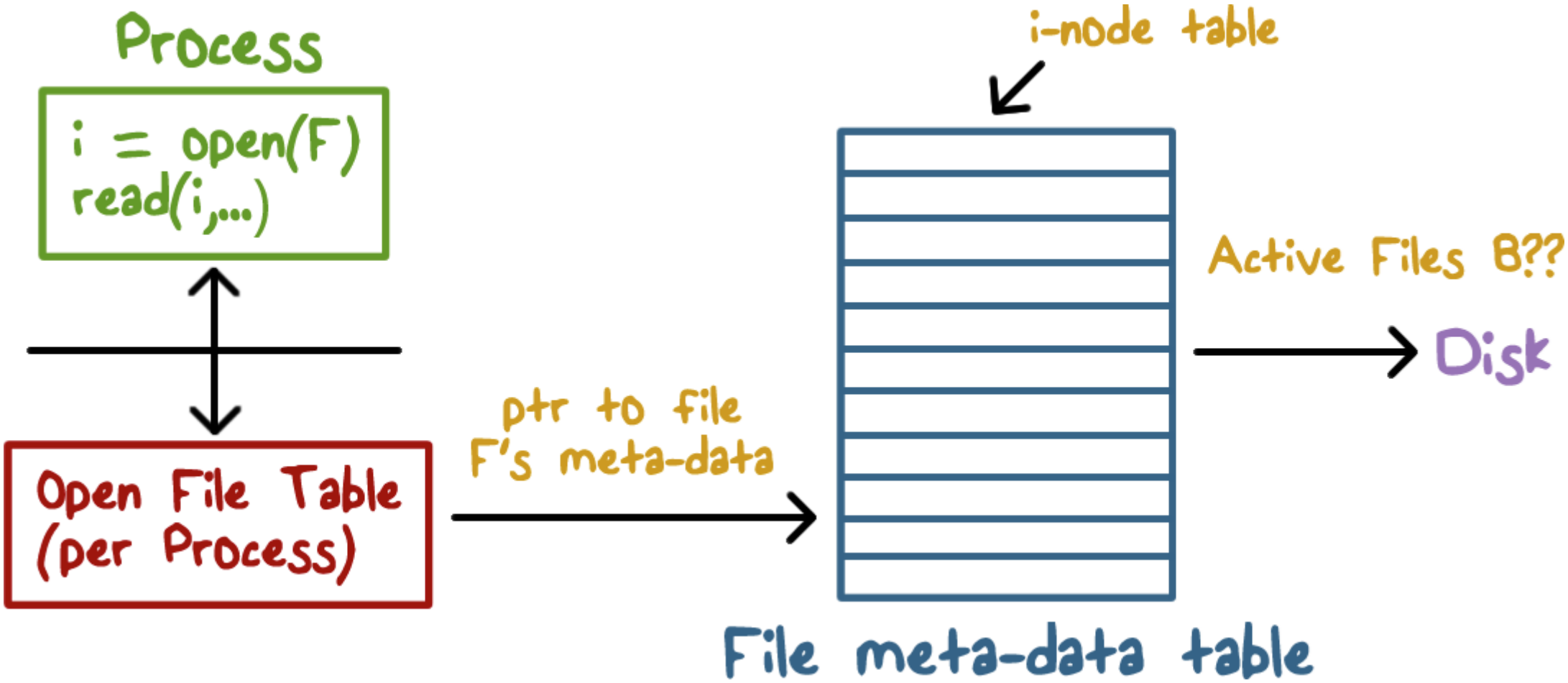
Access Control Implementation



How are files used (system calls for accessing files)?

- Create (filename) /* several ways to do it */
- fd = open (filename, mode)
- read (fd, buf, sizeof(buf))
- write (fd, buf, sizeof(buf))
- close(fd)

How does the OS Implement ACL?



Time to Check vs. Time to Use (TOCTOU) Quiz

A time-to-check-time-to-use vulnerability arises when access check is performed separately from when a file is read or written. TOCTOU vulnerability arises when...

- ☐ File permissions change after an open() call completes for the file and before it is closed.
- ☐ The file permission change only when the file is currently not opened by any program

Unix File Sharing Quiz

In Unix based systems, a file can be shared by sharing its descriptor.

☐ True

☐ False

SetUID Bit Quiz

An executable file F1 has the setuid bit set and is owned by user U1. When user U2 executes F1 (assuming U2 has execute permission for F1), the UID of the process executing F1 is...

- ☐ U1
- ☐ U2

Role-Based Access Control (RBAC)

- In enterprise setting, **access may be based on job function or role of a user**
  - Payroll manager, project member etc.
  - Access rights are associated with roles
- **Users authenticate themselves** to the system
- **Users then can activate one or more roles** for themselves

RBAC Benefits

- Policy **need not be updated when a certain person with a role leaves** the organization
- New employee **should be able to activate the desired role**
- **Revisiting least privilege**
  - User in one role has access to a subset of the files
  - Switch roles to gain access to other resources
- SELinux supports RBAC

Access Control Quiz

Alice has some sensitive data that she only wants to share with Bob and not Charlie. Alice will need to...

- [ ] Fully trust Bob to not share the data with Charlie for her to ensure that Charlie does not gain access to it.

- [ ] Does not need to trust Bob because access control will stop Charlie from accessing it

RBAC Benefits Quiz

In systems that do not support RBAC but allow user groups to be defined, benefits of RBAC can be realized with groups.

- [ ] True
- [ ] False

Access Control Policy Quiz

Fail-safe defaults implies that when an access control policy is silent about access to a certain user U ...

- ☐ Access must be denied when U makes a request
- ☐ Access can be granted because it is not explicitly denied

Access Control
Lesson Summary

- Fundamental requirement when **resources need to be protected**
- An **access control matrix** captures who can access what and the manner in which it can be done
- **ACLs and C-lists** are ways for implementing access control
- Getting **access control policy right is challenging**