Introduction to Management Information Systems

Information Assurance & Security: Access control

Network Systems

objective

Students will gain a practical understanding of access control design

by identifying and organizing access considerations

for groups, permissions, and systems

within a College/University setting

access controls

- Protects sensitive data (e.g., student records, financial information) from unauthorized access.
- Prevents security breaches by ensuring only authorized individuals can access critical systems or resources.
- managed by assigning roles and permissions based on job functions.
- access assigned through group policies and predefined roles.
- uses software like Active directory

groups

- Groups are collections of users, computers, or other groups that share common access requirements.
- They simplify access management by allowing permissions to be assigned to a group rather than individual users.

roles

- Roles define what actions or tasks a user can perform within the system.
- These roles are typically associated with specific administrative tasks or job functions. for example:
  - teacher
  - student
  - student services staff
  - student registration staff
  - student library staff

permissions

- Permissions determine the level of access a user or group has to a resource, such as files, folders, or applications.
- They can specify whether a user can **read**, **write**, **modify**, or **delete** resources.
- Permissions are applied through Access Control Lists (ACLs).

access rights

- Full access (read & write, edit, make password secure, create & delete)
- Read access (read only)
- No access

access permission

- Who has access to your grades?
- What systems are they on?
- How do your results get to you?

- How about student (course) registration, payment details, unit registration, advisor details?
- What systems are these on, are there any other systems?
- What about files and folders?

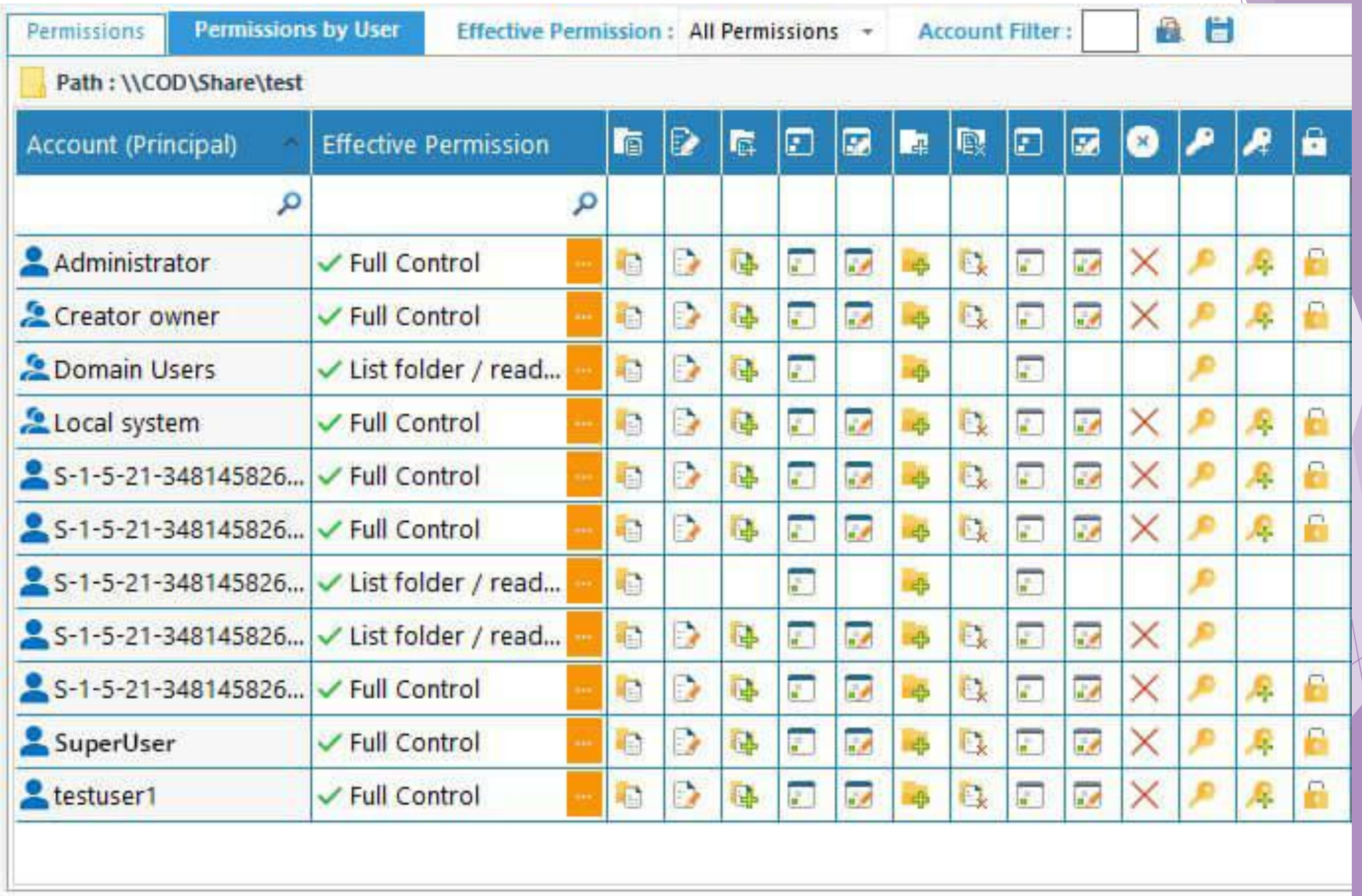
people - roles

- What about staff, what types of staff are there (teachers, administrators, support, finance, events, managers, IT, maintenance, drivers, etc.)
- What systems should they access?

- What about students?
- Can Economic students access things ICDI students can’t access?

Access Control Matrix Example

	File 1	File 2	File 3	File 4
User 1	Read	Write	Own	—
User 2	Write	Own	—	—
User 3	Own	—	—	Read
User 4	Read	Read	Read	Own


Permissions
Permissions by User
Effective Permission : All Permissions
Account Filter :
Path : \\COD\Share\test
Account (Principal)
Effective Permission
Administrator
Full Control
Creator owner
Full Control
Domain Users
List folder / read...
Local system
Full Control
S-1-5-21-348145826...
Full Control
S-1-5-21-348145826...
Full Control
S-1-5-21-348145826...
List folder / read...
S-1-5-21-348145826...
List folder / read...
S-1-5-21-348145826...
Full Control
SuperUser
Full Control
testuser1
Full Control

	A	B	C	D
	FolderName	AD Group or User	Permissions	Inherited
1	\\fs1\Shared\Accounting	ENTERPRISE\HR	Modify, Synchronize	FALSE
2	\\fs1\Shared\Accounting	NT AUTHORITY\SYSTEM	FullControl	TRUE
3	\\fs1\Shared\Accounting	ENTERPRISE\J.Carter	FullControl	TRUE
4	\\fs1\Shared\Accounting	ENTERPRISE\Domain Admins	FullControl	TRUE
5	\\fs1\Shared\Accounting	BUILTIN\Administrators	FullControl	TRUE
6 7	\\fs1\Shared\ Accounting	ENTERPRISE\ Domain Users	ReadAndExecute, Synchronize	TRUE
8	\\fs1\Shared\Accounting\Archive	ENTERPRISE\HR	Modify, Synchronize	TRUE
9	\\fs1\Shared\Accounting\Archive	NT AUTHORITY\SYSTEM	FullControl	TRUE
10	\\fs1\Shared\Accounting\Archive	ENTERPRISE\J.Carter	FullControl	TRUE
11	\\fs1\Shared\Accounting\Archive	ENTERPRISE\Domain Admins	FullControl	TRUE
12	\\fs1\Shared\Accounting\Archive	BUILTIN\Administrators	FullControl	TRUE

Access Control List

	registration	grades	salary
student			
teacher			
administrator			
HR staff			
Dean			

task 1
design an access control plan

work in groups

group work

- groups of 4 students
- ICDI is implementing a new access control system for its staff and students
- You need to decide who has access to different systems and resources

exercise #1

1. Make the most basic list of groups (roles or groups of people)
2. Make a list of systems/folders
3. Now make a table and give access permissions to the groups for each of the system or folder.

considerations

- Risks (e.g., a student accessing confidential grades).
- Internet and intranet access (e.g., campus-only resources like research databases).
- Disaster recovery (e.g., restoring data after a server crash).
- Business continuity (e.g., ensuring access during system outages).

considerations

- What are the risks?
  - malware, hacking, unauthorized access
- What are your plans to deal with the risks?
  - stronger password procedures
  - two-stage authentication
  - storage
  - backups

Thank you!

any questions?