Object Security

COMP755 Advanced Operating Systems

Object Permissions

- Operating systems must determine if a user has permission to perform an action upon an object.
- The objects that we are usually concerned with are files and printers.

Access Control

- The definition of access rights can be defined for a user or an object.
- **Capabilities** specify what a user can do.
- **Access Control Lists (ACL)** are created for each object and specify who can perform what action.

Access Matrix

	FileX	FileY	Prt1	/dir
userA	read	read / execute	print	list
userB	read / write	read / execute	print / manage	list / write

- Row are capabilities
- Columns are access control lists

Complex Security Access

- Imagine you have a file of sensitive information. You want users to be able to run your program to add data to the file but you don't want users to be able to read the file.
- Imagine you are a manager going on leave. You want to give your assistant certain privileges while you are gone. You don't want them to be able to do anything and you want to rescind privileges on your return.

Unix File Security

- Unix files use Access Control Lists.
- Each file has 9 bits defining the access rights

  user group world

  RWX RWX RWX
- Rights can be expressed as a three digit octal number

Unix File Permissions

- 400 read by the user
- 200 write by the user
- 600 read and write by the user
- 604 read/write by user, read by world
- 701 user anything, world can execute
- 751 user anything, group read/execute world can execute

Changing File Permissions

- chmod - Changes permission codes

```
chmod 604  myfile
```

Set the permissions for myfile so I can read and write it while everyone else can only read it.

Windows Permissions

- Windows NT, 2000 and XP provide security for objects.
- The NTFS file system allows access rights to be set for files and directories.

Windows Domains

- A Microsoft Windows system can belong to a workgroup or domain.
- Domains have a domain controller, a server that authorizes user login.
- When you enter your userid and password on a domain, the domain controller verifies you password.
- Users on a domain can access resources in the domain.

Windows File Permissions

- A user can allow or deny the following actions on a file:
  - read
  - read & execute
  - write
  - modify
  - full control
  - special

Windows Printer Permissions

- A user can allow or deny the following actions with a printer:
  - **print** – send a file to the printer
  - **manage documents** – reorder or cancel the documents to be printed.
  - **manage printer** – change printer parameters or disable the printer.

Users and Groups

- Permissions can be given to individual users or groups
- You can define a group on a local computer and put users in the group.
- Users in a domain can belong to global groups.
- Local groups can include global groups.
- An individual user can belong to many local and global groups.

Access Conflicts

- Consider user Fred who belongs to the ***student*** group and the ***tutor*** group.
- The student group has read access to fileA
- The tutor group has read and write access to fileA
- Can Fred write to fileA?

Access Resolution

- The effective permission is the highest level permission given to the individual or any group
  - deny
  - allow full control
  - allow write
  - read

Windows Access Example

- Group *student* has read access to FileA
- Group *tutor* has read and write access to FileA
- User Mary belongs to the student and tutor groups.
- FileA specifies deny write to Mary.
- What can Mary do with FileA?