Access Control

COMP620

"History is rife with examples of governments taking actions to 'protect' their citizens from harm by controlling access to information and inhibiting freedom of expression and other freedoms outlined in The Universal Declaration of Human Rights. We must make sure, collectively, that the Internet avoids a similar fate."

Vint Cerf

Final Exam

The final exam in COMP620 will be on Saturday, December 1, from 10:00am – 12:00pm in Graham 210

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 access
- **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	no access	print / manage	list / write

- Rows 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 everything and you want to rescind privileges on your return

Unix File Access Control

- Unix file systems provide access to
  - owner – The person creating the file
  - group – Users can only belong to one group
  - world – Everyone
- For each group you can allow
  - Read
  - Write
  - Execute

chmod

- The chmod command can be used to change the permissions
- Think of RWX as three bits making an octal *(decimal)* digit representing **R**ead, **W**rite, e**X**ecute
- The permissions can be expressed as three digits for user, group, world

```
chmod  704  myfile
```

- sets read, write and execute for the user and read for the world

Microsoft Access Control

- Microsoft Windows provides a means of controlling access to files, printers and other objects
- Different users on a Windows computer can have different access rights to files

Microsoft Active Directory

- Access control system for Microsoft Domains
- Consists of services on the clients and a server with a database called the Domain Controller
- When a user logs onto any computer in the domain, the login information is sent to the server for authentication
- Once authenticated, the user may access other domain resources without having to authenticate again

What access does everyone have?

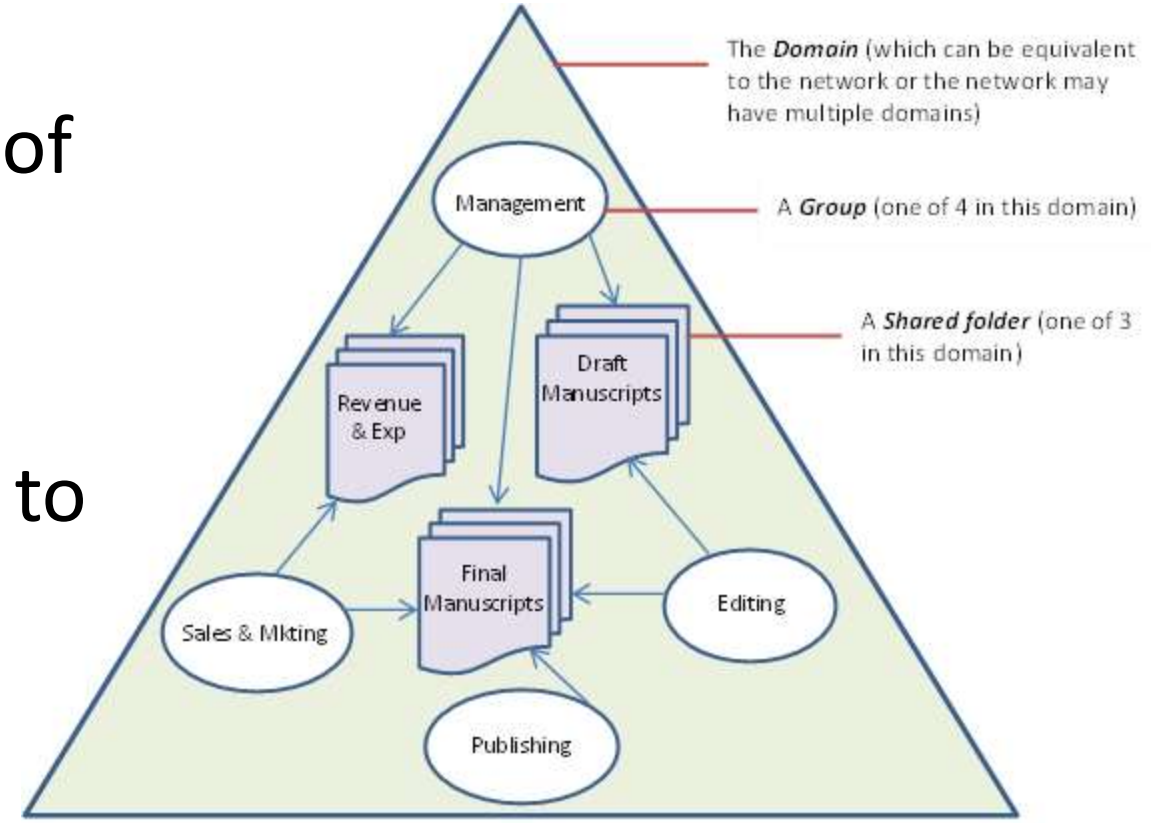
- Assume you have done

```
chmod 444 secrets.txt
```

A. Read
B. Write
C. Execute
D. Read & Write
E. None

Active Directory Groups

- Users can be organized into trees of Organizational Units
- Users can be assigned to groups
- Groups can be given access rights to objects



PC Login

With Microsoft Windows, there are several options for authenticating

- A user can have a local userid and password for that machine
- You can use a Microsoft userid and password
- You can login using your organization’s email password
- Windows Hello allows you to authenticate with fingerprint or facial recognition
- Windows Picture Password allows you to click or swipe over a picture
- Windows supports multifactor login

Multiple Users on a PC

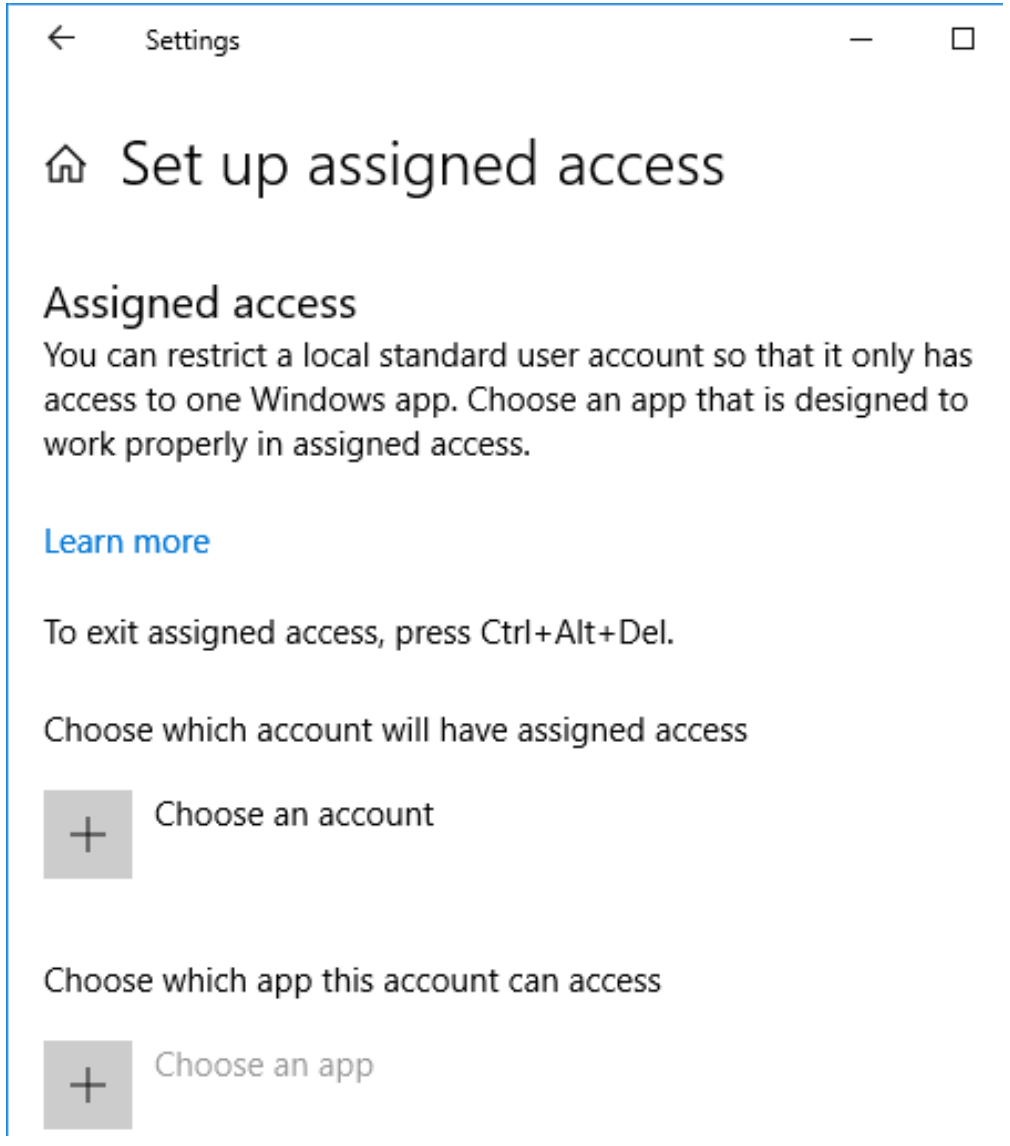
- Most Windows PCs are used by one person at a time
- Multiple users might use the same computer at different times
- Background activities (e.g. backup services, anti-virus or web server) can run as different users
- The Microsoft Windows Server OS uses the same access security system

Principle of Least Privilege

- In almost every aspect of computer security, a basic rule is to **give a user or program only enough access necessary to accomplish the task**
- You may not need full administrator privileges for most activities
- If you are not an administrator, then a malware attack is limited in the damage it can inflict

Assigned Access

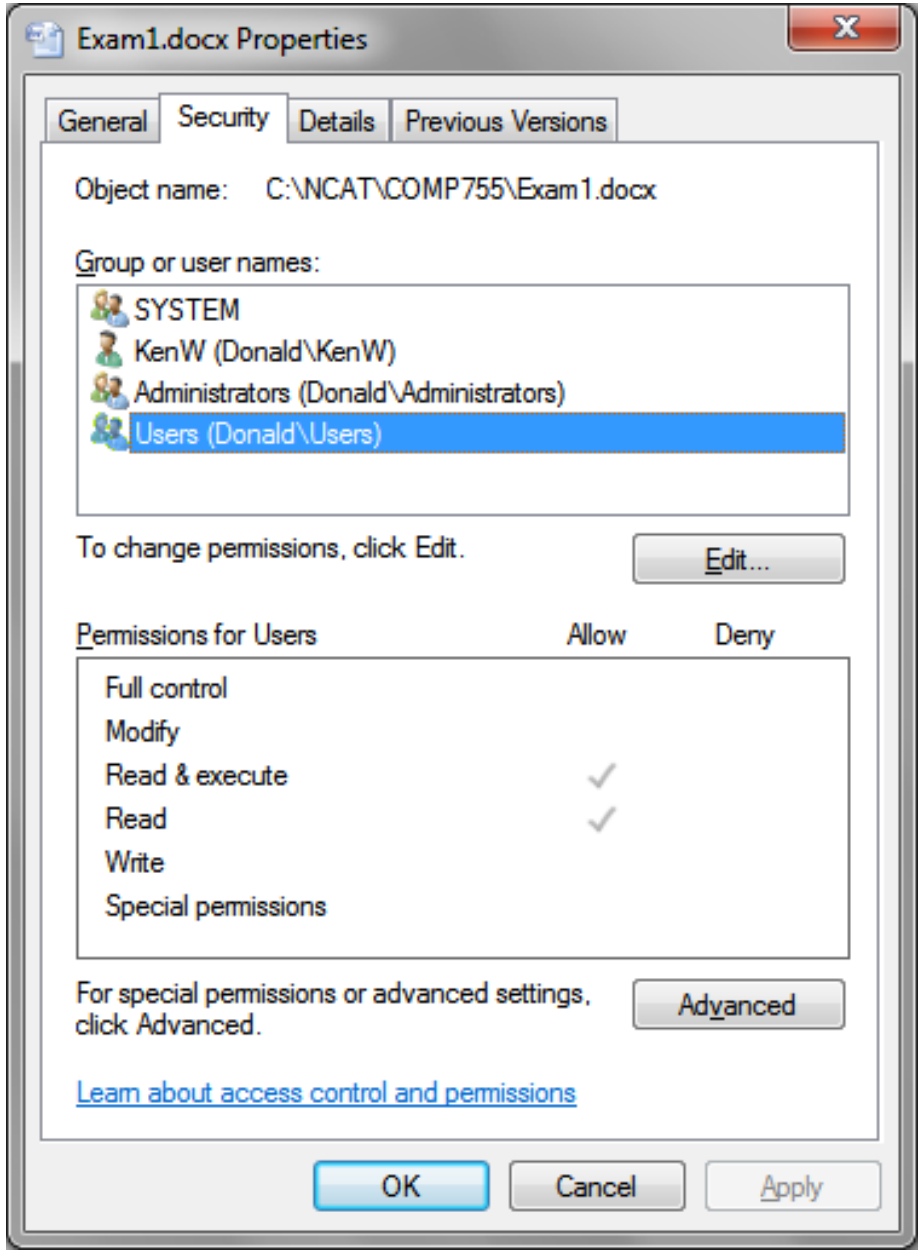
- Microsoft Assigned Access allows you to create a userid that can only execute on app
- Intended to make your device act like a kiosk



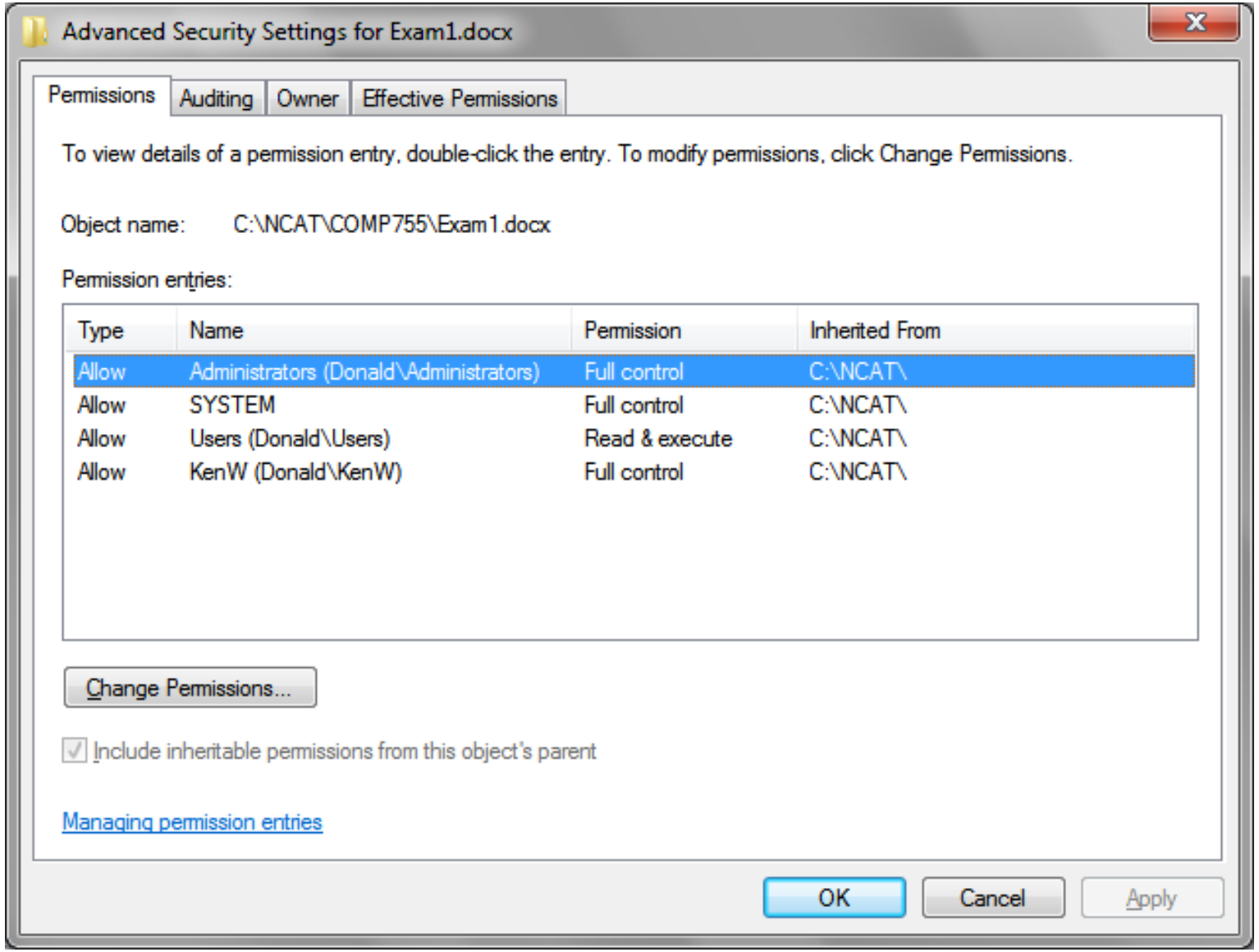
Security for Novices

- Microsoft operating systems have included the idea of shared directories
- Files in shared directories are accessible to all users
- The very same result can be obtained by properly setting the permissions for file

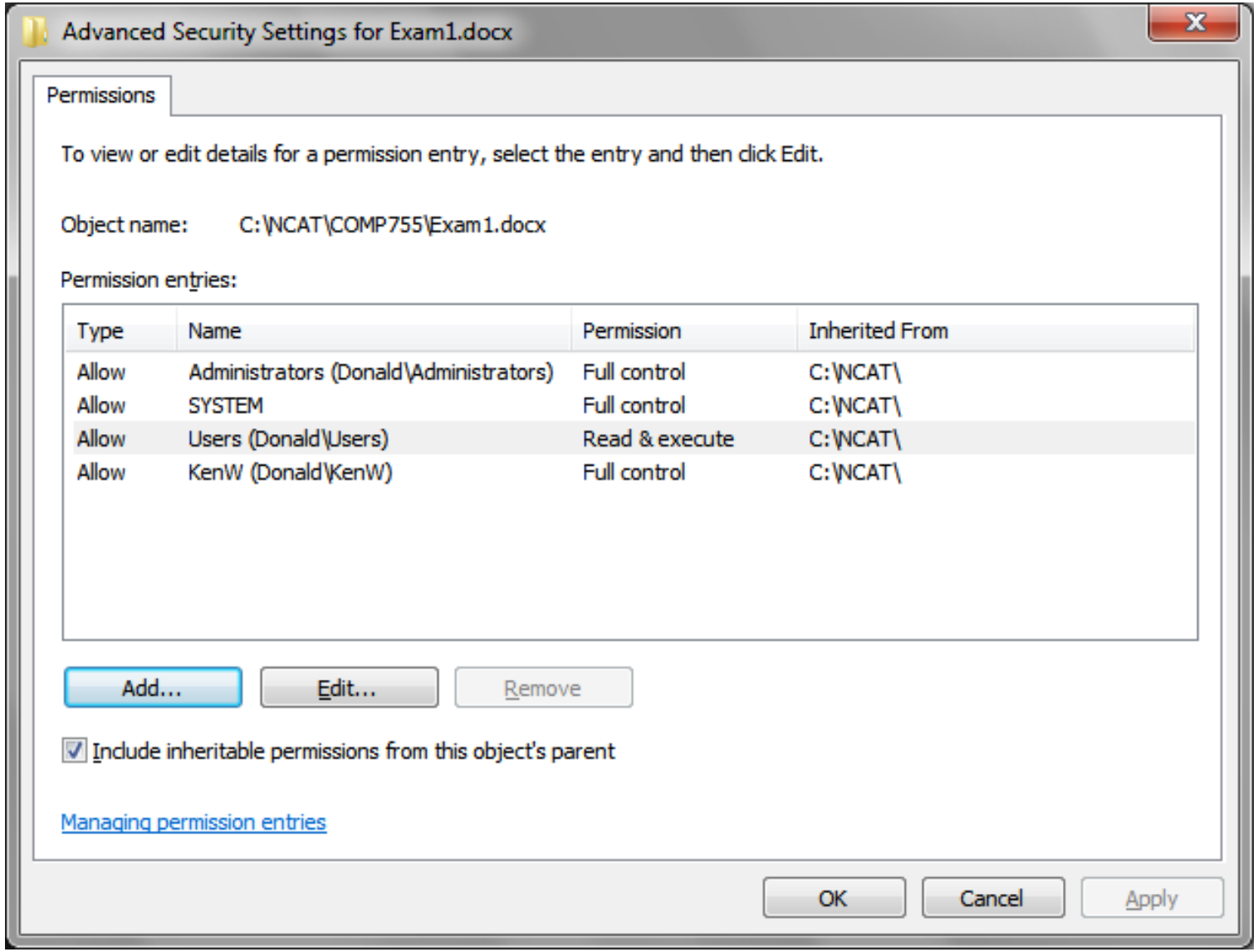
File Properties



Advanced Permissions



Change Permissions



Inheriting Permissions

- By default files and directories inherit the permissions of their parent directory
- If you create a new file, it automatically has the permissions of that directory
- To change the permissions of an object, it must not inherit permissions
- When you unclick “Include inheritable permissions”, you can copy or remove the parent permissions

Object Owner

	FileX	FileY	Prt1	/dir
Owner	Fred	Mary	Admin	Joe
userA	read	read / execute	print	list
userB	read / write	no access	print / manage	list / write

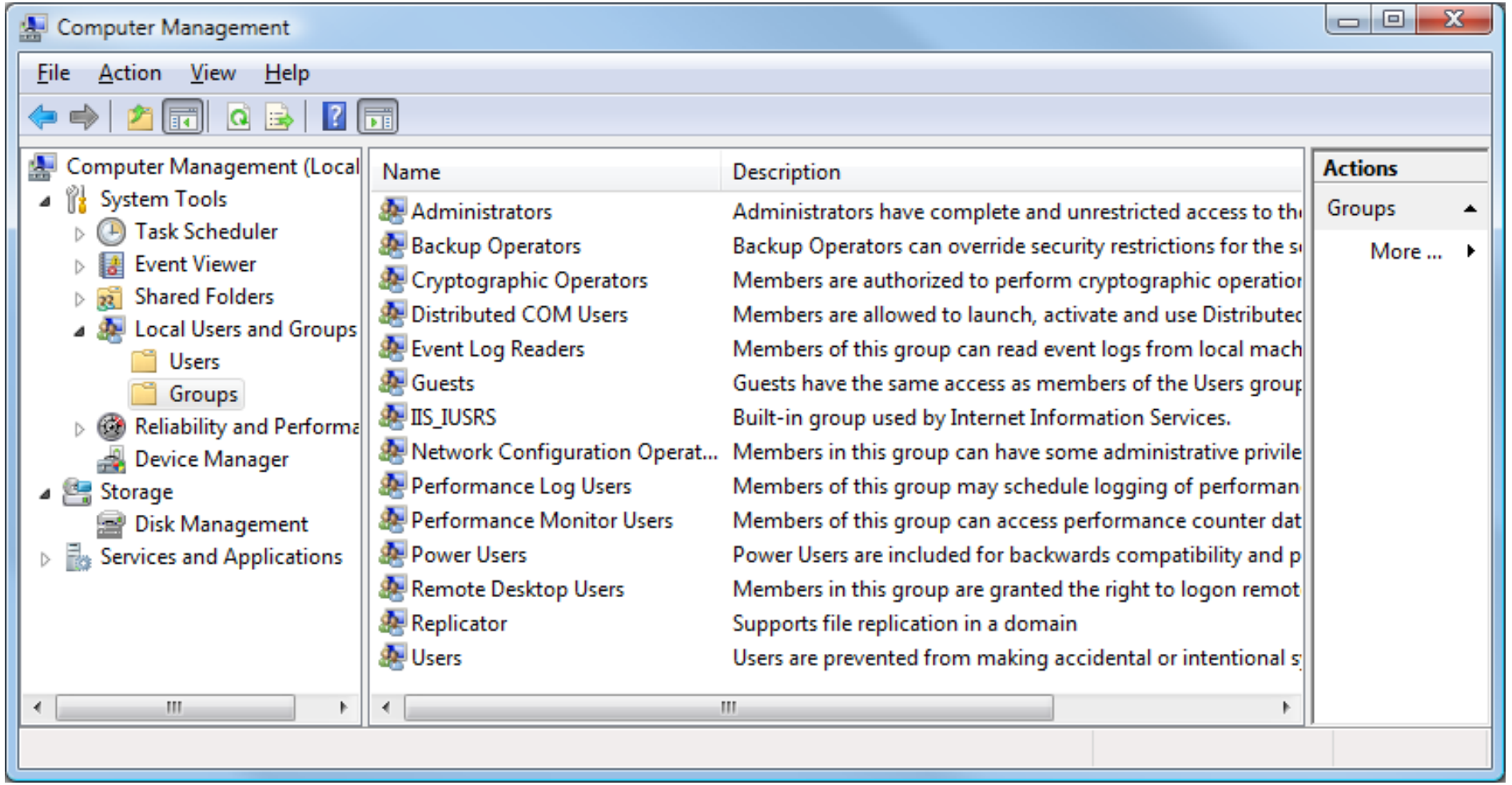
- The object's owner has the authority to change the access rights for the object
- The owner can set control the column

Groups

- Microsoft Windows allows an administrator to create groups of users
- Groups define a set of users that should have the same permission
- This allows you to easily grant permissions to a large number of users without having to individually specify each user

Groups

- Administrators can define Groups in the Computer Management tool



Domains

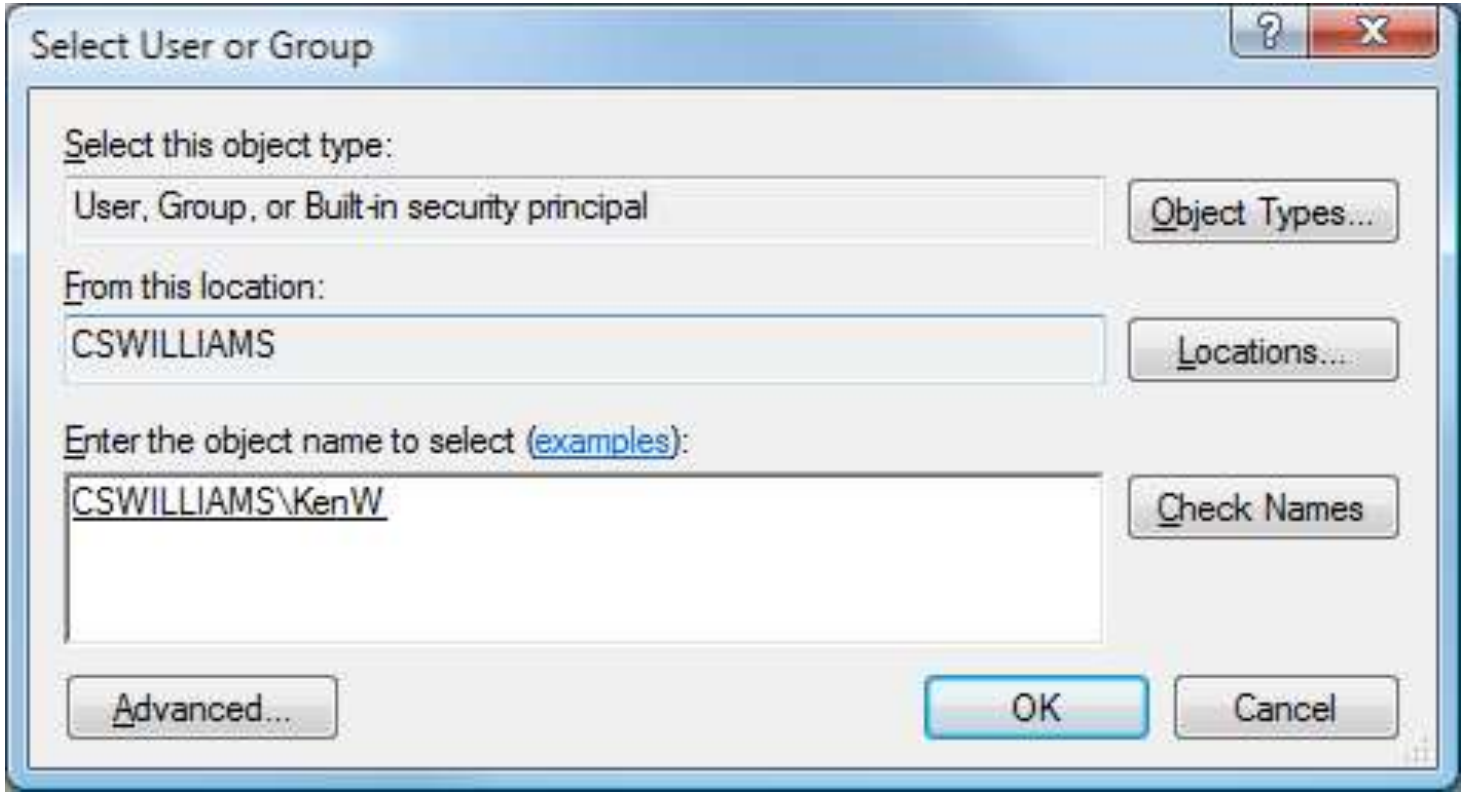
- Microsoft Windows supports the concept of a network domain with centralized login
- A computer can be a member of a domain or it can be an independent workstation
- Once a computer is logged into a domain, it has access to all resources of the domain (assuming security permission)

Domain and Local Groups

- Administrators can define groups at the domain level or at the local computer level
- Domain groups can contain domain users or other domain groups
- Local groups can contain domain users, domain groups, local groups or local users

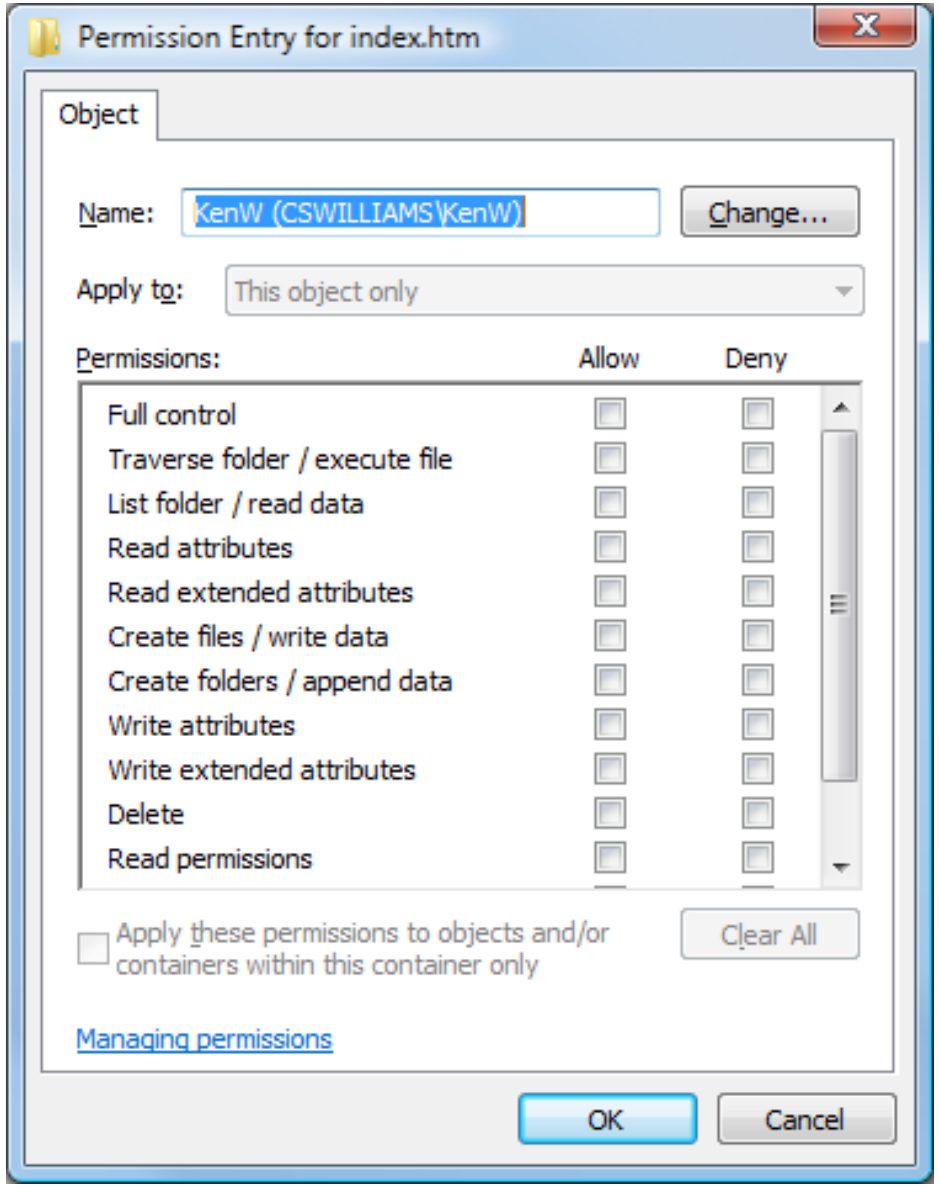
Adding a User or Group

- When you click add in the file permissions dialog, you get a new dialog box that asks you for the new user or group



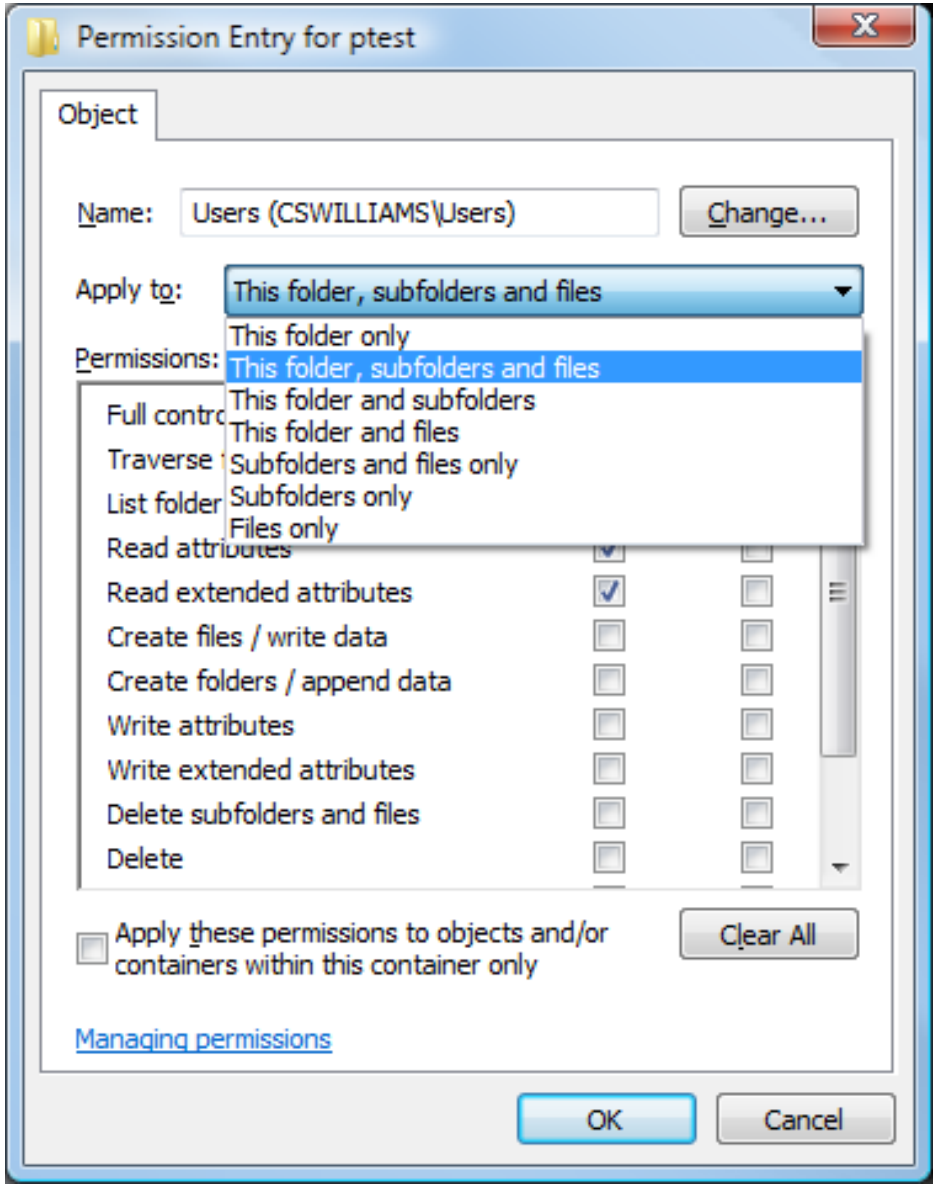
Setting Permissions

- After adding a new user or group, you must select the permissions for that user or group



Directory Permissions

- You can set permissions for just the folder or for the objects in the folder



Resolving Permissions

- A user may belong to multiple groups
- Each group might have different permissions for an object
- When the OS checks permissions, it has to check the permissions of the user and all groups where the user is a member

Permission Order

- Windows gives a user the highest ranking permission based on their permission and the permissions of all groups in the order:
  - Deny *highest ranking*
  - Full control
  - Write
  - Read & execute
  - Read *lowest ranking*

No Permission Specified

- If a user does not have any permission specified for an object, then they cannot access the object
- Having no permission specified is slightly different from being denied access
- If your userid does not specify a permission, but a group does, then you have the group's rights
- If your userid is denied access, then no group can override this

What permission does Fred have for ideas.docx?

Fred is a member of the ADVERTISING group which has WRITE permission for the file ideas.docx He is also a member of the HR group which has Read & execute permission for the file.

A. None
B. Full control
C. Write
D. Read & execute
E. Read

What permission does Joe have for click.txt?

Joe is a member of the PR group which has READ permission for the file click.txt He is also a member of the HR group which does not specify permission for the file.

A. None
B. Full control
C. Write
D. Read & execute
E. Read

What permissions does user “Susan” have for files in the XYZ directory?

The ENGINEERING group has Write permission for directory XYZ. The MARKETING group has Read and Execute permissions to the directory and the ACCOUNTING group has Deny permission. User “Susan” is a member of the ENGINEERING, MARKETING and ACCOUNTING groups.

A. None
B. Full control
C. Write
D. Read & execute
E. Read

Hardware Capabilities

- Some processors enforce strong typing of all data. Examples are the IBM AS/400 and the Intel i430
- If a data value was flagged as an address, you could not modify it with an integer

```
union {
    int number;
    int *address;
}
```

Final Exam

The final exam in COMP620 will be on Saturday, December 1, from 10:00am – 12:00pm in Graham 210