Filesystems

File Permissions

We now look at file protection

Filesystems
File Permissions

We now look at file protection

It is not good if every user of a computer can read or update any file on the system

We now look at file protection

It is not good if every user of a computer can read or update any file on the system

Quite apart from issues of privacy, there are many files that are essential to the good running of the OS itself (configuration files, system library files, etc.)

Filesystems
File Permissions

We now look at file protection

It is not good if every user of a computer can read or update any file on the system

Quite apart from issues of privacy, there are many files that are essential to the good running of the OS itself (configuration files, system library files, etc.)

So we need to limit access somehow

Filesystems
File Permissions

There are generally three ways to access a file

Filesystems
File Permissions

There are generally three ways to access a file

- to read from it

Filesystems

There are generally three ways to access a file

- to read from it
- to write to it

Filesystems
File Permissions

There are generally three ways to access a file

- to read from it
- to write to it
- to run it as a program

Filesystems
File Permissions

There are generally three ways to access a file

- to read from it
- to write to it
- to run it as a program

Other ways include *append only*, where you can add to the end of a file but otherwise can't update it: useful for logging (you can't accidentally — or by choice – alter the earlier part of the log)

Similarly, for a directory

Filesystems
File Permissions

Similarly, for a directory

- list the directory's contents (read)

Similarly, for a directory

- list the directory's contents (read)
- create/delete/rename a file (write)

Filesystems

Similarly, for a directory

- list the directory's contents (read)
- create/delete/rename a file (write)
- search a directory

Filesystems
File Permissions

Files have owners, generally they inherit the userid of the process that created it

Filesystems
File Permissions

Files have owners, generally they inherit the userid of the process that created it

There are also *groups*, collections of users

Filesystems
File Permissions

Files have owners, generally they inherit the userid of the process that created it

There are also *groups*, collections of users

For example, "First year computing" and "Computing Staff"

Files have owners, generally they inherit the userid of the process that created it

There are also *groups*, collections of users

For example, "First year computing" and "Computing Staff"

Groups allow us to allow or deny access to large numbers of people

Filesystems
File Permissions

Files have owners, generally they inherit the userid of the process that created it

There are also *groups*, collections of users

For example, "First year computing" and "Computing Staff"

Groups allow us to allow or deny access to large numbers of people

Each user can be in several groups

Unfortunately groups are quite inflexible and are set by the systems operators: normal users cannot create groups

Filesystems
File Permissions

Unfortunately groups are quite inflexible and are set by the systems operators: normal users cannot create groups

We have to rely on the operators creating the right groups

Filesystems
File Permissions

Unfortunately groups are quite inflexible and are set by the systems operators: normal users cannot create groups

We have to rely on the operators creating the right groups

Each file has a single group ownership to go alongside the user ownership

Filesystems

Unix permissions mostly work OK but are very inflexible regarding groups

Filesystems
File Permissions

Unix permissions mostly work OK but are very inflexible regarding groups

You can't specify that just users Alice and Bob should have read/write access but others read only, unless the operators have created a group containing just Alice and Bob

□

Filesystems
File Permissions

Unix permissions mostly work OK but are very inflexible regarding groups

You can't specify that just users Alice and Bob should have read/write access but others read only, unless the operators have created a group containing just Alice and Bob

A more general mechanism is *access control lists* (ACLs) that allows a low more flexible way of allowing and disallowing access

□

Filesystems
File Permissions

Unix permissions mostly work OK but are very inflexible regarding groups

You can't specify that just users Alice and Bob should have read/write access but others read only, unless the operators have created a group containing just Alice and Bob

A more general mechanism is *access control lists* (ACLs) that allows a low more flexible way of allowing and disallowing access

Exercise. Read about ACLs

□