* File Sharing *

⇒ fileSharing is very desirable for users who want to collaborate and to reduce the effort required to achieve computing goal.

⇒ Therefore, user-oriented operating systems must accommodate the need to share files inspite of inherent difficulties.

1. Multiple Users :-

* when an operating system accommodates multiple users, the issues of file sharing, file naming, and file protection become preeminent.

* Given a directory structure that allows files to be shared by users, the system must mediate the file sharing

→ The system can either allow a user to access the files of others users by default or require that a user specifically grant access to files.

* To implement sharing and protection, the system must maintain more file and directory attributes than are needed

on a single-user system

⇒ most systems have evolved to use the concepts of file owner (user) and group attribu

⇒ owner: The owner is the user who can change attributes and grant access and who has the most control over the file.

group attribute:

The group attribute defines a subset of users who can share access to the file.

* For example, the owner of a file on a UNIX system can issue all operations on a file, while members of the file's group can execute one subset of those operations, and all other users can executed another subset of operations. Exactly which operations can be executed by group members and other users is definable by the file's owner.

⇒ The owner and group ID's of a given file are stored with the other file attributes. When a user requests an operation on a file, the user ID can be compared with the owner attribute to determine if the requesting user is the owner of the file.

Remote File Systems :-

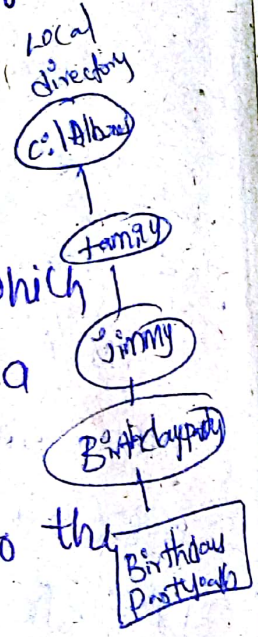
Remote file sharing is a type of distributed file system technology that enables file and/or data access to multiple remote users over the internet.

⇒ Ex: LAN, WAN,

⇒ Evolution of networks file technology.

1) Manually transferring files b/w machines via programs like FTP.

2) Distributed file system (DFS) in which remote directories are visible from a local machine.



3) World wide web is a reversion to the first.

A browser is needed to gain access to the remote files, and separate operations are used to transfer files.

DFS: it is a client server based application that allows clients to access and process data on server.

Client - Server model :

→ The machine containing the files is the server, and the machine seeking access to the files is the client

→ A server can serve multiple clients, and a client can use multiple servers

server specific available files in directory path.

Distributed Information Systems :

→ To make client server systems easier to manage, distributed information system provide unified access to the information need to remote computing.

→ The domain name system (DNS) provides host name to network address.

→ Before DNS became widespread files containing the same information were sent via e-mail of ftp b/w all networked hosts

→ other distributed information systems provide user name / password space for distributed facility.

NIS (Network Information Service)

It centralizes storage of user names, host names, printer info.

⇒ Unfortunately, it uses unsecure authentication methods, including sending user passwords unencrypted and identifying hosts by IP address.

⇒ CIFS (Common Internet file system) network information is used in conjuction with user authentication to create a network login that the server uses to decide whether to allow or deny access to requested file system.

⇒ The industry is moving toward use of the light weight directory access protocol (LDAP) as a secure distributed naming mechan.

⇒ LDAP directory could be used by an organization to store all user and resource information for all the organizations computers.

* Consistency semantics

(1) UNIX 2) Session 3) Immutable.

Protection

⇒ we have to keep safe the files from physical damage and improper access.

1. Reliability:
protecting files from physical damage.

* File systems can be damaged by
  1) Hardware problems
  2) Power surges or failures
     Head crashes
  3) Bugs in file system software.

to prevent from it,
2. Sec
⇒ provided by duplicate copies of files.
⇒ Take backups at regular intervals (daily | weekly | monthly).

2. Security:
* protecting files from unauthorized access
* more important in a multi user system.
* provided by 'controlling access to files'.

↓

to control access of files the protection mechanism should ~~provide controlled type of~~ limit access.