Protecting and Sharing Files

Unix makes it easy for users to share files and directories. For instance, everyone in a group can read documents stored in one of their manager's directories without needing to make their own copies—if the manager has allowed access. There might be no need to fill peoples' email inboxes with file attachments if everyone can access those files directly through the Unix filesystem.

Here's a brief introduction to file security and sharing. Networked systems with multiple users, such as Unix, have complex security issues that take tens or hundreds of pages to explain. If you have critical security needs or you just want more information, talk to your system staff or see an up-to-date book on Unix security.

Note that the system's superuser (the system administrator and possibly other users) can do anything to any file at any time, no matter what its permissions are. So, access permissions won't keep your private information safe from *everyone*—although let's hope that you can trust your system staff!

Your system staff should also keep backup copies of users' files. These backup copies may be readable by anyone who has physical access to them. That is, anyone who can take the backup out of a cabinet (or wherever) and mount it on a computer system may be able to read the file copies. The same is true for files stored on floppy disks and any other removable media. (Once you take a file off of a Unix system, that system can't control access to it anymore.)

Directory Access Permissions

A directory's access permissions help to control access to the files and subdirectories in that directory:

- If a directory has read permission, a user can run **ls** to see what's in the directory and use wildcards to match files in it.
- A directory that has write permission allows users to add, rename, and delete files in the directory.