

Protection

File systems implement a protection system

- Who can access a file
 - How they can access it
- ➔ A protection system dictates whether a given action performed by a given subject on a given object should be allowed
- You can read and/or write your files, but others cannot
 - You can read `/etc/motd`, but you cannot write it

Representing Protection

Access Control Lists (ACL)

For each object, maintain a list of subjects and their permitted actions

Capabilities

For each subject, maintain a list of objects and their permitted actions

The diagram shows a table with subjects (rows) and objects (columns). The table is annotated with dashed lines and labels to illustrate ACL and Capabilities.

	/one	/two	/three
Alice	rw	-	rw
Bob	w	-	r
Charlie	w	r	rw

Subjects (labeled on the left side of the table)

Objects (labeled above the table)

ACL (Access Control List): Indicated by a green dashed oval around the first column (objects /one, /two, /three) and the first row (subject Alice).

Capability: Indicated by a pink dashed oval around the third row (subject Charlie) and the third column (object /three).