

# 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 labeled 'Subjects' on the left and 'Objects' at the top. The subjects are Alice, Bob, and Charlie. The objects are /one, /two, and /three. The permissions are as follows:

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

The table is annotated with three dashed lines:

- A green dashed line encircles the first column (objects /one, /two, /three) and is labeled **ACL** (Access Control List).
- A magenta dashed line encircles the third row (subject Charlie) and is labeled **Capability**.
- A magenta dashed line encircles the cell for Charlie and /one.