

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).

ACLs and Capabilities

Approaches differ only in how the table is represented

➡ Capabilities are easier to transfer

They are like keys, can handoff, does not depend on subject

➡ But ACLs are easier to manage in practice

- Object-centric, easy to grant, revoke
- To revoke capabilities, have to keep track of all subjects that have the capability – a challenging problem

ACLs have a problem when objects are heavily shared

● The ACLs become very large

● Use groups (e.g. Unix)