

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)

Acknowledgments

Some of the course materials and projects are from

- Ryan Huang - teaching CS 318 at *John Hopkins University*
- David Mazière - teaching CS 140 at *Stanford*
- Sina Meraji - teaching CS 369 at *University of Toronto*