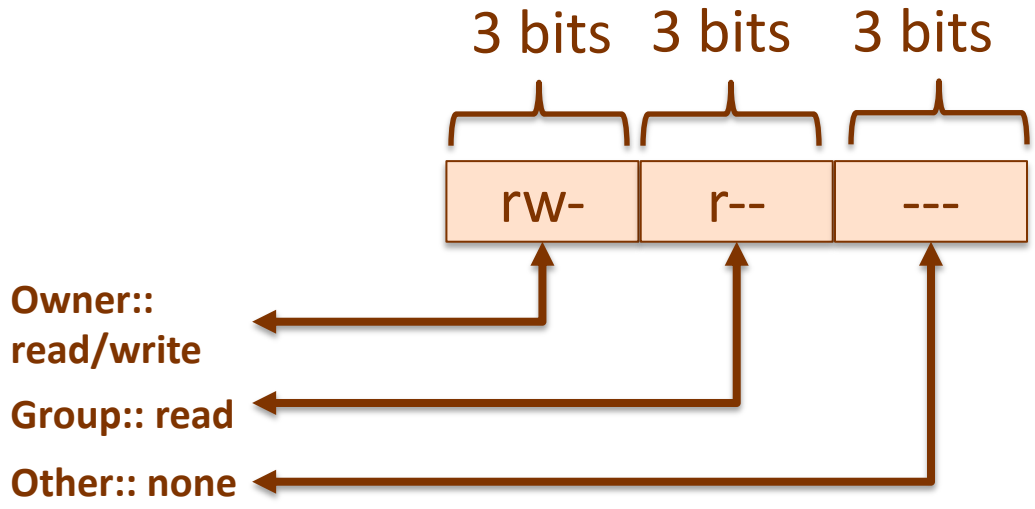
Discretionary Access Control in Practice

UNIX File Access Control

Oregon State University
College of Engineering

- Unique user identification number (user ID)
- Member of a primary group identified by a group ID
- Three permission octets associated with each file and directory
  - Specify read, write, and execute permission for the owner of the file, members of the group and all other users
- The owner ID, group ID, and protection bits are part of the file's inode



Traditional Unix File Protection

UNIX File Access Control

Oregon State University
College of Engineering

- 3 additional bits
  - "Set user ID"(SetUID)
  - "Set group ID"(SetGID)
  - "Sticky Bit"

- "Set user ID"(SetUID), "Set group ID"(SetGID)
  - System temporarily uses rights of the file owner/group in addition to the real user's rights when making access control decisions
  - Enables privileged programs to access files/resources not generally accessible

- Sticky bit
  - When applied to a directory it specifies that only the owner of any file in the directory can rename, move, or delete that file

UNIX File Access Control

- Superuser
  - Is exempt from usual access control restrictions
  - Has system-wide access

ACLs in UNIX

Oregon State University
College of Engineering

Modern UNIX systems support ACLs

- FreeBSD, OpenBSD, Linux, Solaris

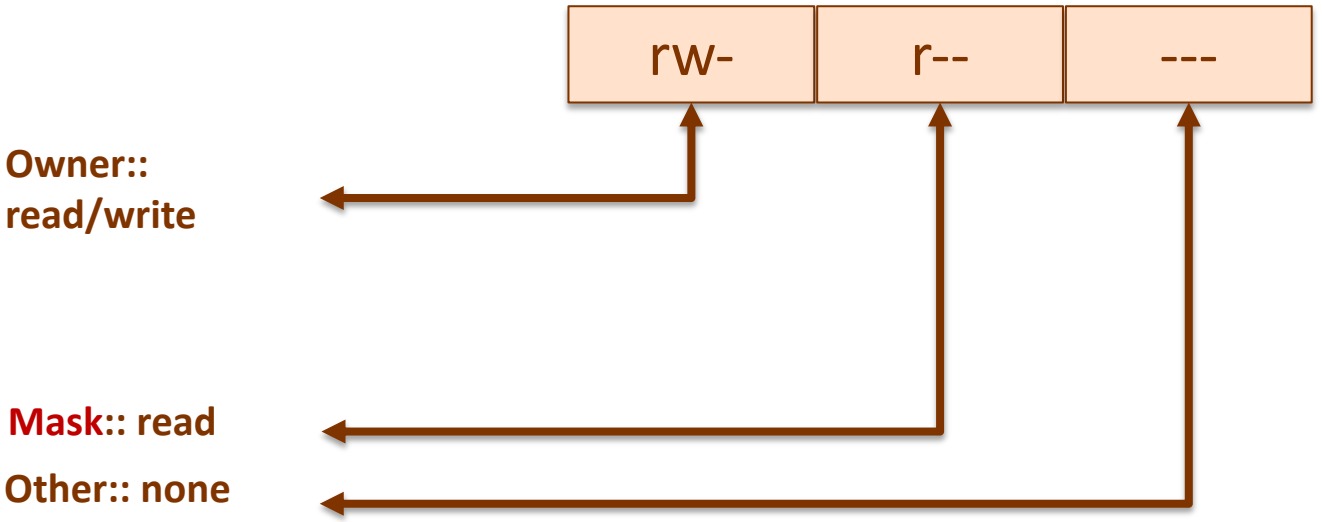
FreeBSD

- Setfacl command assigns a list of UNIX user IDs and groups
- Any number of users and groups can be associated with a file
- Read, write, execute protection bits
- A file does not need to have an ACL
- Includes an additional protection bit that indicates whether the file has an extended ACL

When a process requests access to a file system object two steps are performed:

- Step 1 selects the most appropriate ACL
- Step 2 checks if the matching entry contains sufficient permissions

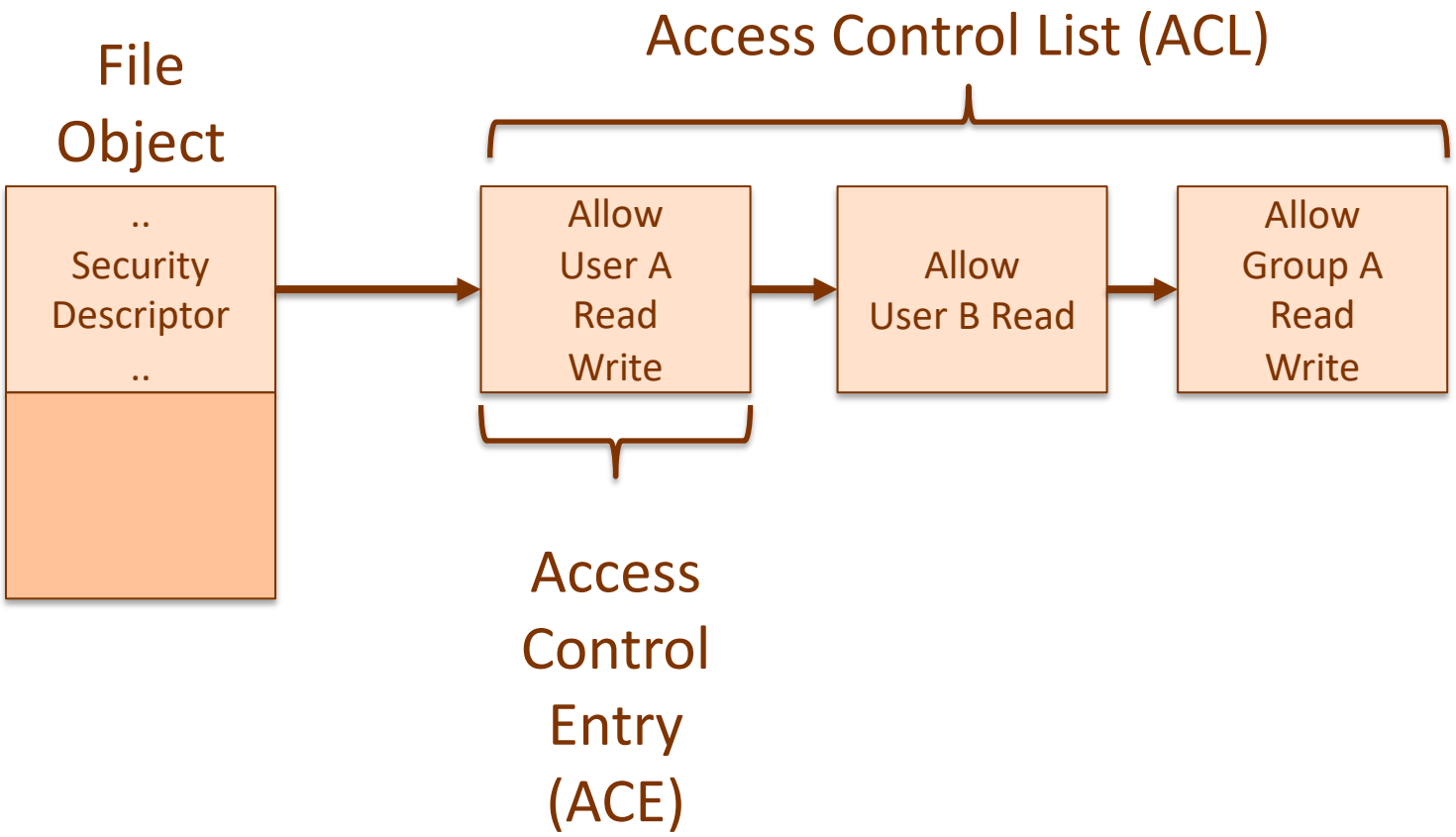
Extended Unix ACL

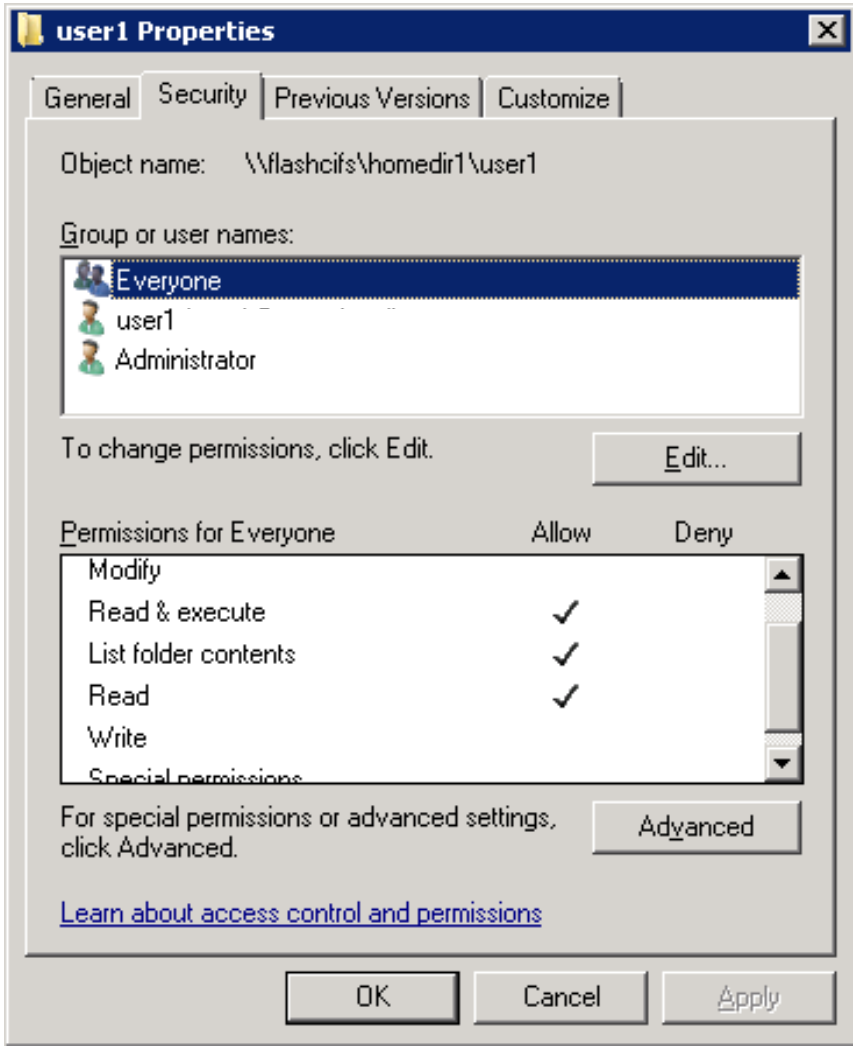


Extended Unix ACL

Windows ACL (1 of 2)

Oregon State University
College of Engineering





Windows ACL (2 of 2)

Oregon State University
College of Engineering

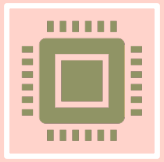
- Actually two ACL's per file
  - System ACL (SACL) – controls auditing and now integrity controls
  - Discretionary ACL (DACL) – controls object access

- Windows ACLs apply to all named objects
  - Files
  - Pipes
  - Events

Summary

Oregon State University
College of Engineering

Both Unix and Windows primarily use DAC, specifically ACLs



Mandatory Access Controls have slowly found their way into mainstream OSes for integrity protection

e.g., SACL in Windows