Announcements

- Should be done with identity mapping on P4
- Midterm regrades have been completed
- Project #3 – will be posted tonight
- Reading Chapter 11 (8th ed)

File Protection

- How to give access to some users and not others?
- Access types:
  - read, write, execute, append, delete, list
  - rename: often based on protection of directory
  - copy: usually the same as read
- Degree of control
  - access lists
    - list for each user and file the permitted operations
  - groups
    - enumerate users in a list called a group
    - provide same protection to all members of the group
    - depending on system:
      - files may be in one or many groups
      - users may be in one or many groups
  - per file passwords (tedious and a security problem)

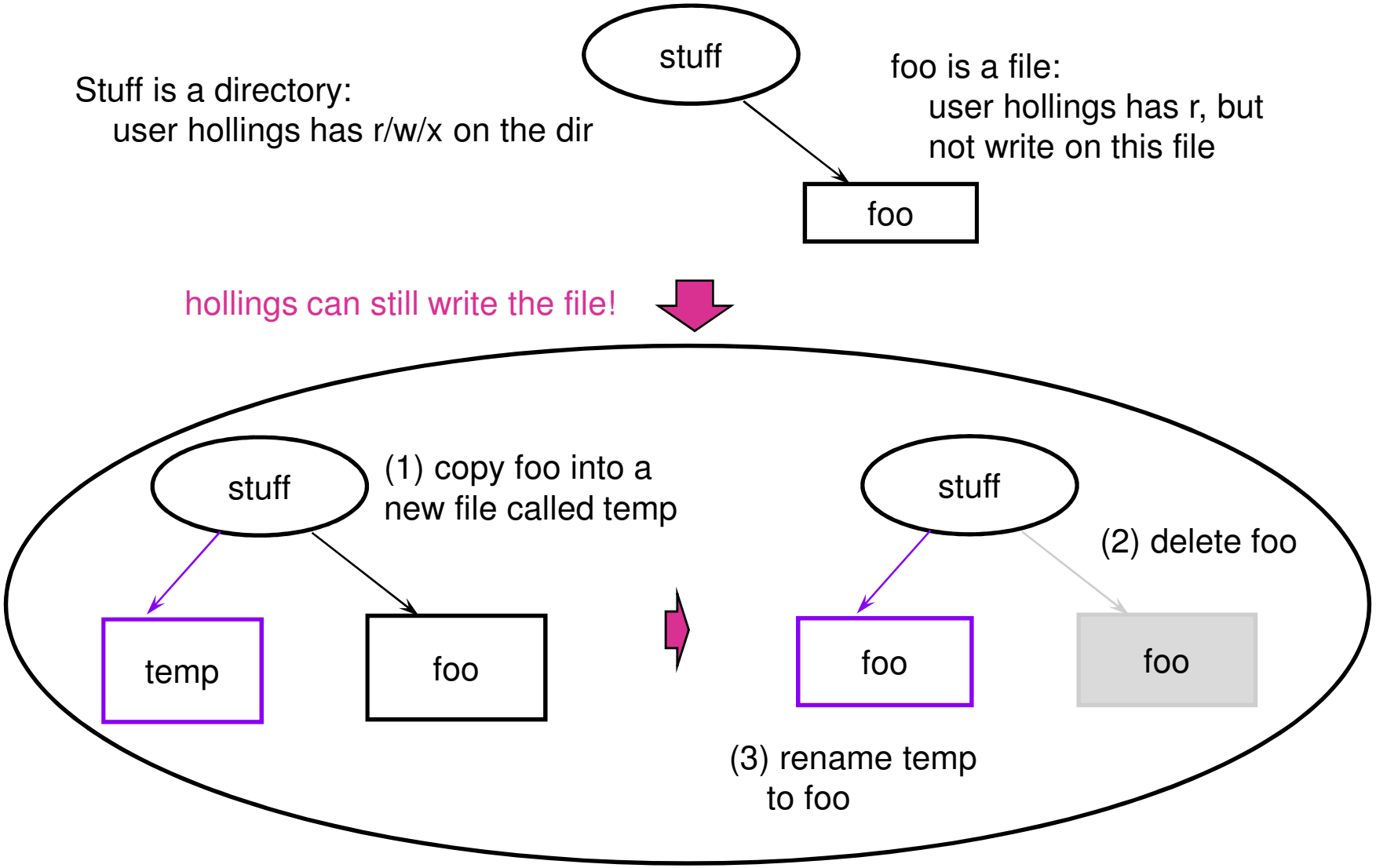
File Protection Example (UNIX)

- Each file has three classifications
  - user: the user who owns the file
  - group: a named group of other users
  - world: all others
- Each file has three access types:
  - read, write, execute
- Directory protection
  - read: list the files in the sub dir
  - write: delete or create a file
  - execute: see the attributes of the files in the subdir
  - sticky bit: contents can only be modified by root user, folder owner, or file owner

Unix File Protection (cont)

- Files have 12 bits of protection
  - 9 bits are user, group, and world for:
    - read: list the files in the sub dir
    - write: delete or create a file
    - execute: see the attributes of the files in the subdir
  - sticky bit: contents can only be modified by root user, folder owner, or file owner
  - setuid: run the program with the uid of the file's owner
    - used to provide extra privilege to some processes
      - example: passwd command
  - setgid: run the program with the group id of the file's owner

UNIX File Protection Example



File Protection Example (AFS)

- Each Directory has an ACL
  - protection information applies to all files in a directory
  - file access types are:
    - lookup, insert, delete, administer, read, write, lock (k)
  - an ACL may be for a user or a group
  - ACL may contain negative rights
    - everyone but Joe Smith may read this file
- Groups
  - are collections of users
  - each user can create up to a fixed number of groups
    - users can administer their own groups
- Cells
  - collections of computers (e.g., csic, wam)