Access Control Basics

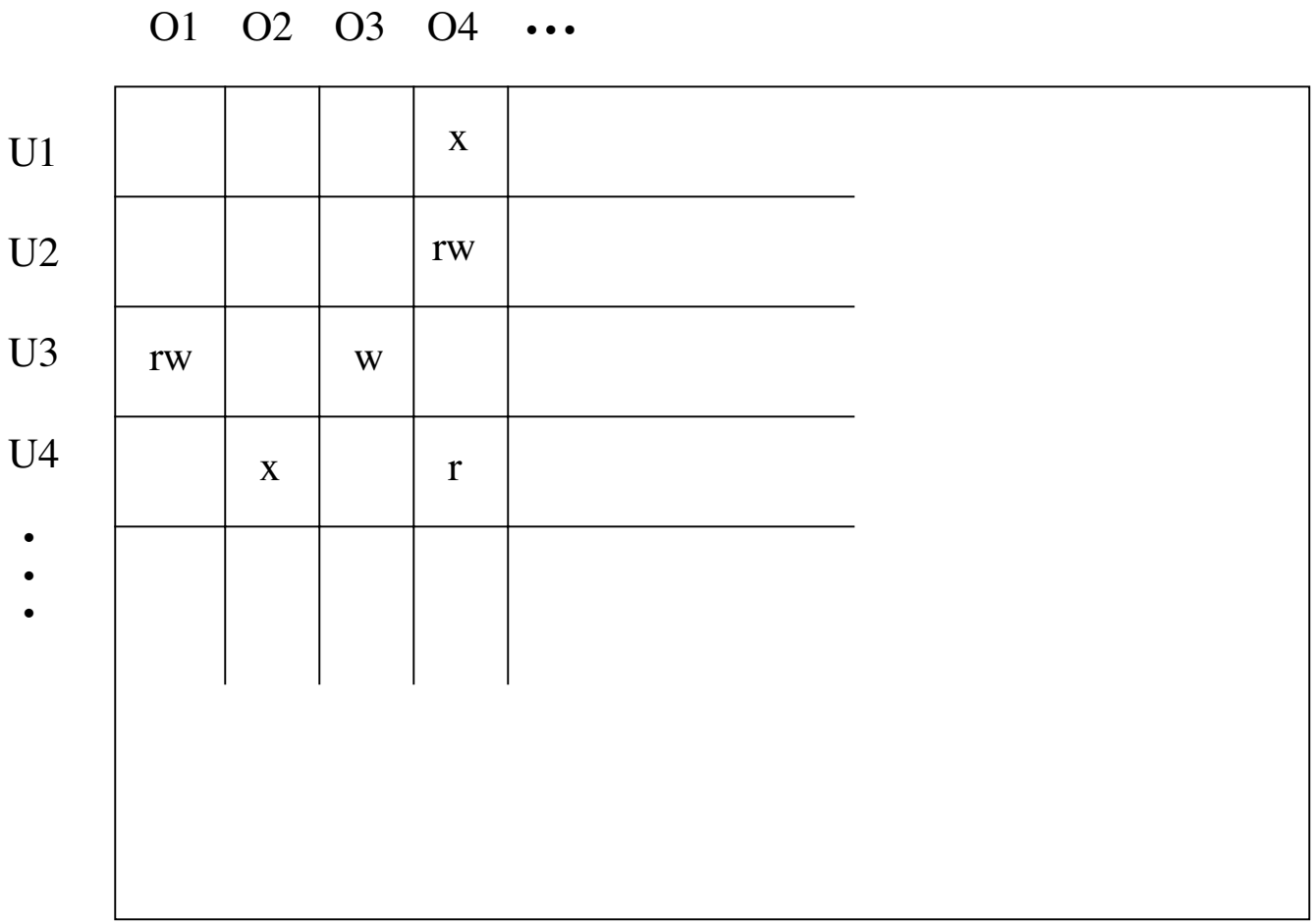
P. J. Denning

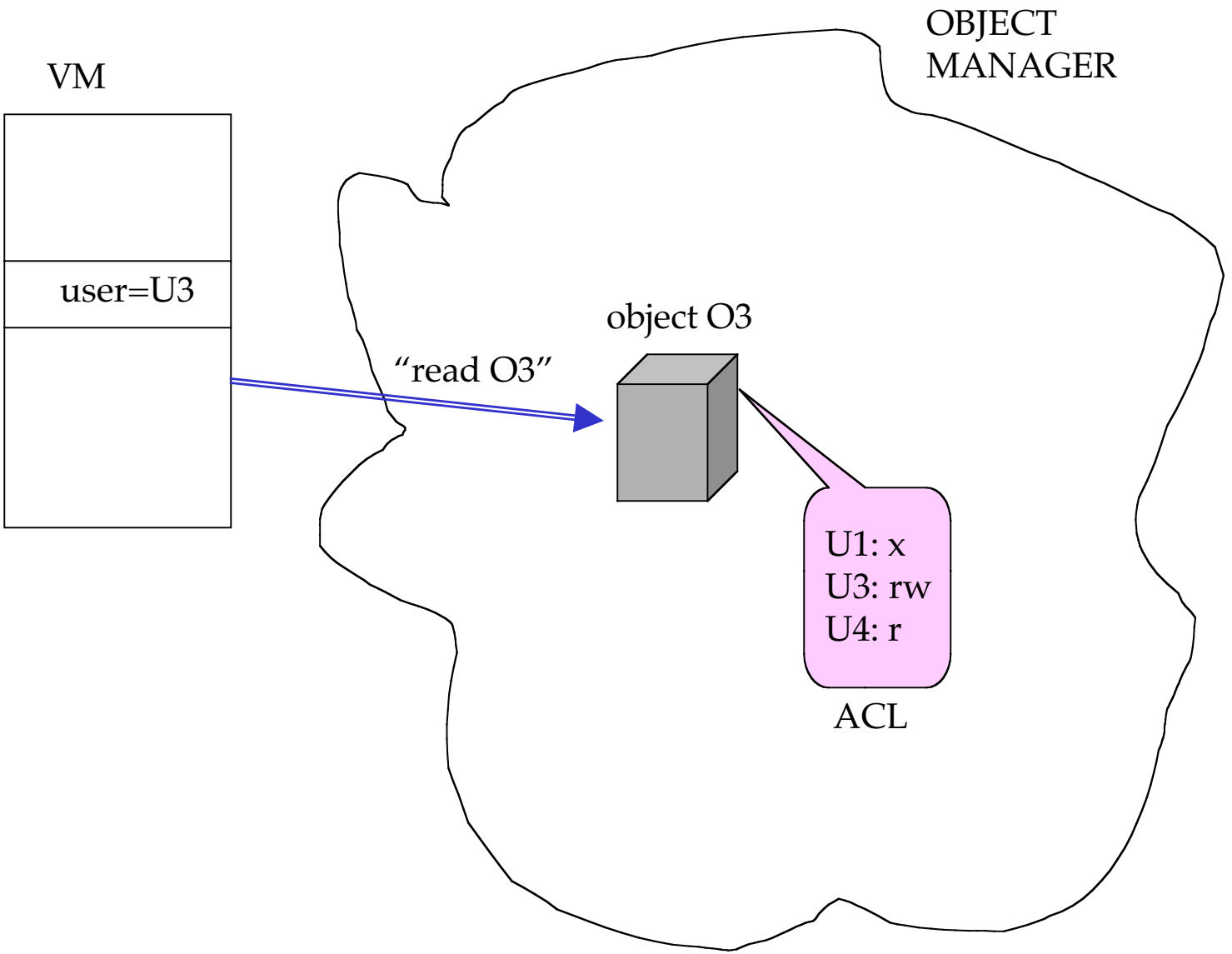
For CS471/CS571

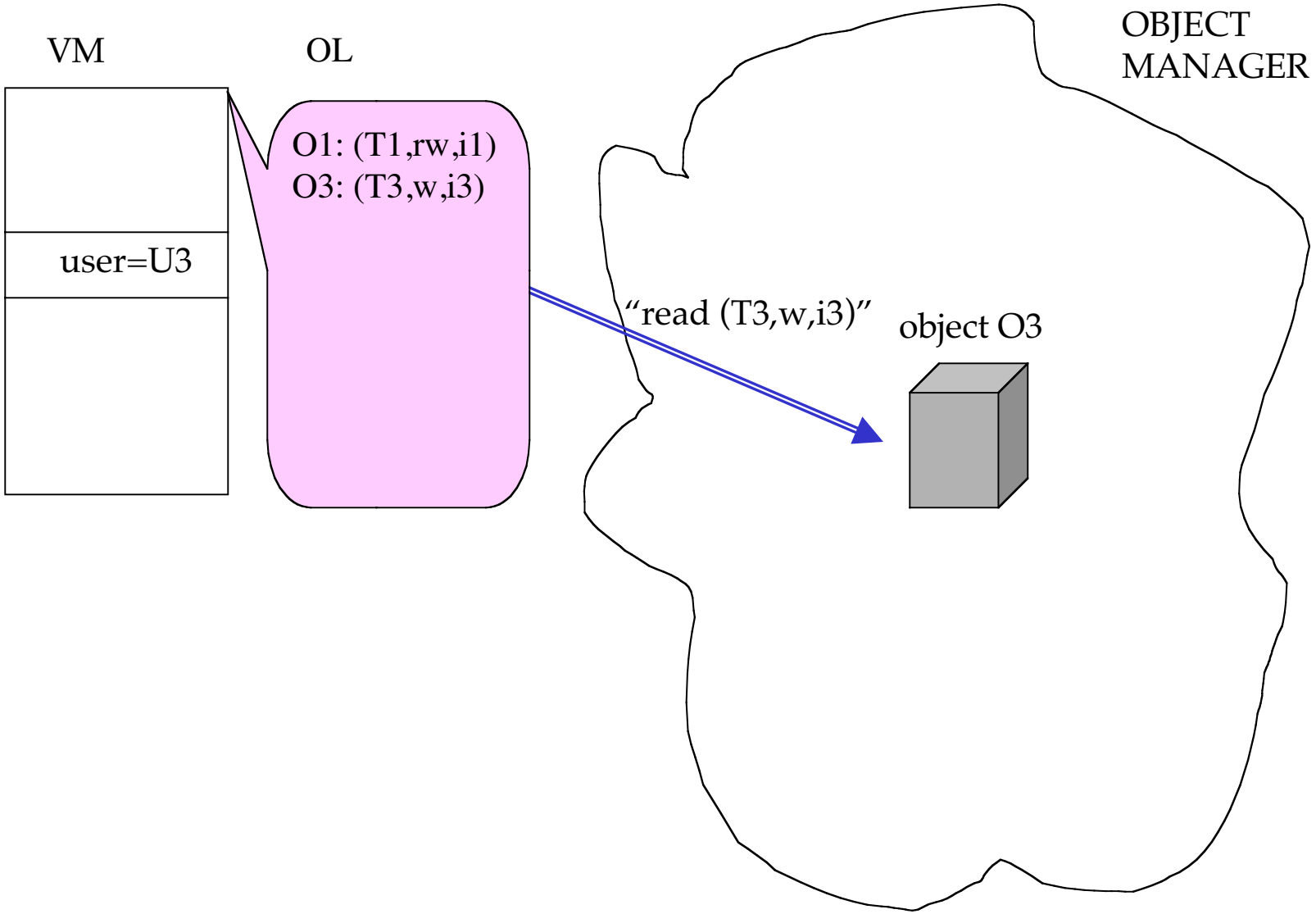
Access Control

- SEARCH seems insecure: anyone with a directory's pathname can search it.
- What controls do owners of directories and other objects have over who can see and access their objects?

- Every object has an owner.
- Owners can set access rights for their objects.
- Add user field to VM control block.
  - inherited from creator
  - can be overridden by superuser
- Access matrix
  - users -- rows
  - objects -- columns
  - entries -- rights granted (depend on object type)







- ACL = access control list
  - linked to object
  - lists authorized users and rights
- OL = object list
  - linked to user
  - lists authorized objects and their handles
  - handles contain rights in their access codes
- Real systems use both -- e.g.,
  - access control lists in directories
  - page tables in virtual memory

- OL is more volatile -- exists as long as VM exists
- ACL is more permanent -- exists as long as object exists
- Can load OL dynamically from ACL when VM started (e.g., page table)
- In this case, OL is a cache of object handles needed by VM

- OL solves another problem.
- Objects move from file system to computational store as normal part of caching in VM workspaces -- e.g., opening a file, swapping in a page.
- The handles generated in an OL enable object manager to quickly and dynamically check authorization of access

Unix Model

- Unix divides users into categories:
  - owner
  - group
  - world
- Provides 3-bit rights designator (RWE) for each category
- Collapses ACL to 9-bit string

- Search operations succeed only if all directories of the pathname grant X right for searcher
- Read (write) operations succeed only if search succeeds and target object grants R (W) access

- Extend SEARCH by defining new variable "path" as part of virtual machine.
- Path = a list of directories, ending with the current directory (.)
  - NOTE: All directories contain standard entries "." for current directory and ".." for parent directory.
- SEARCH looks for target object in each of the directories on the "path".