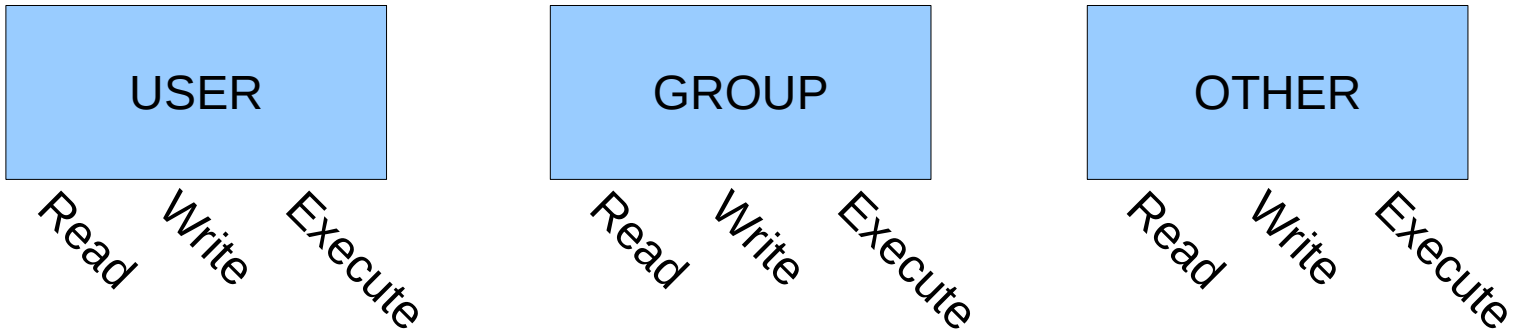
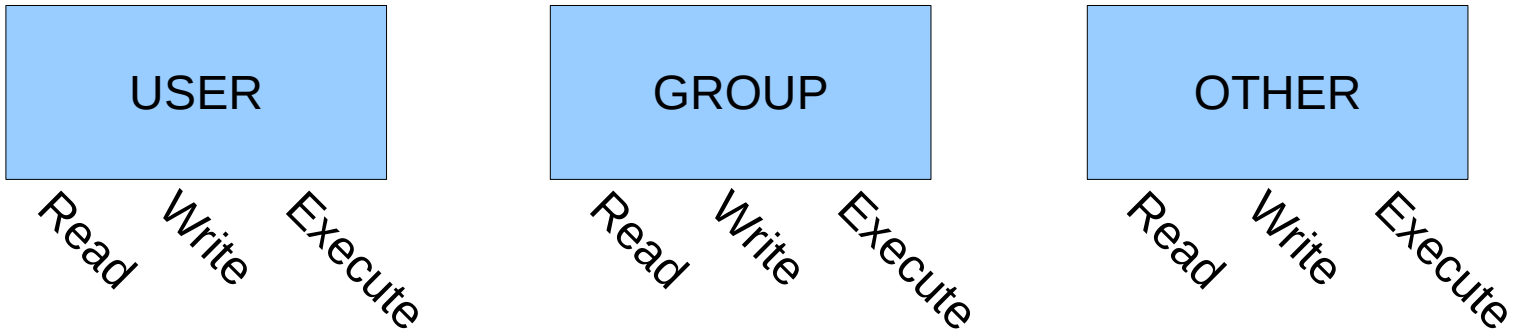
Restricted Data Protection through Access Control Lists

Sam Trahan
May 18, 2012

Old UNIX File Permissions



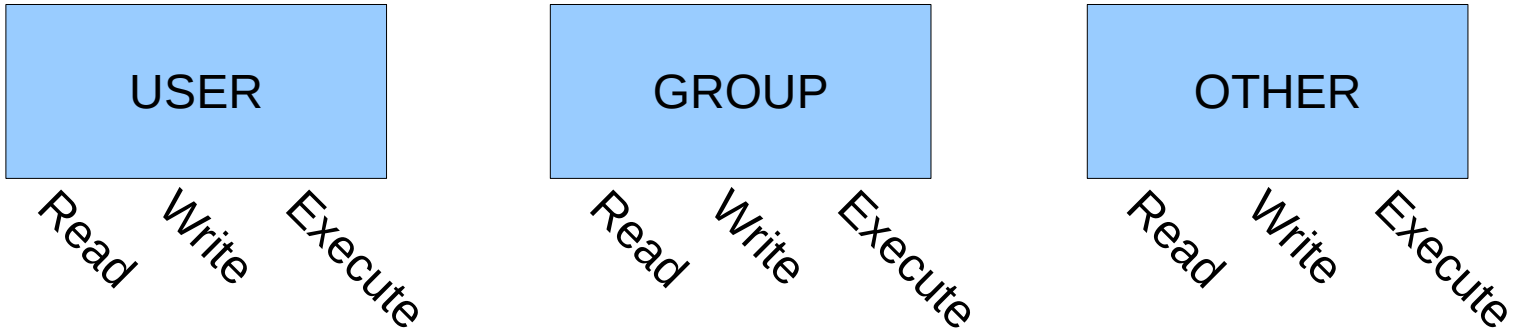
Old UNIX File Permissions



- What if we use group quotas?
- What if another group needs permission?
- What if other specific users need permissions?

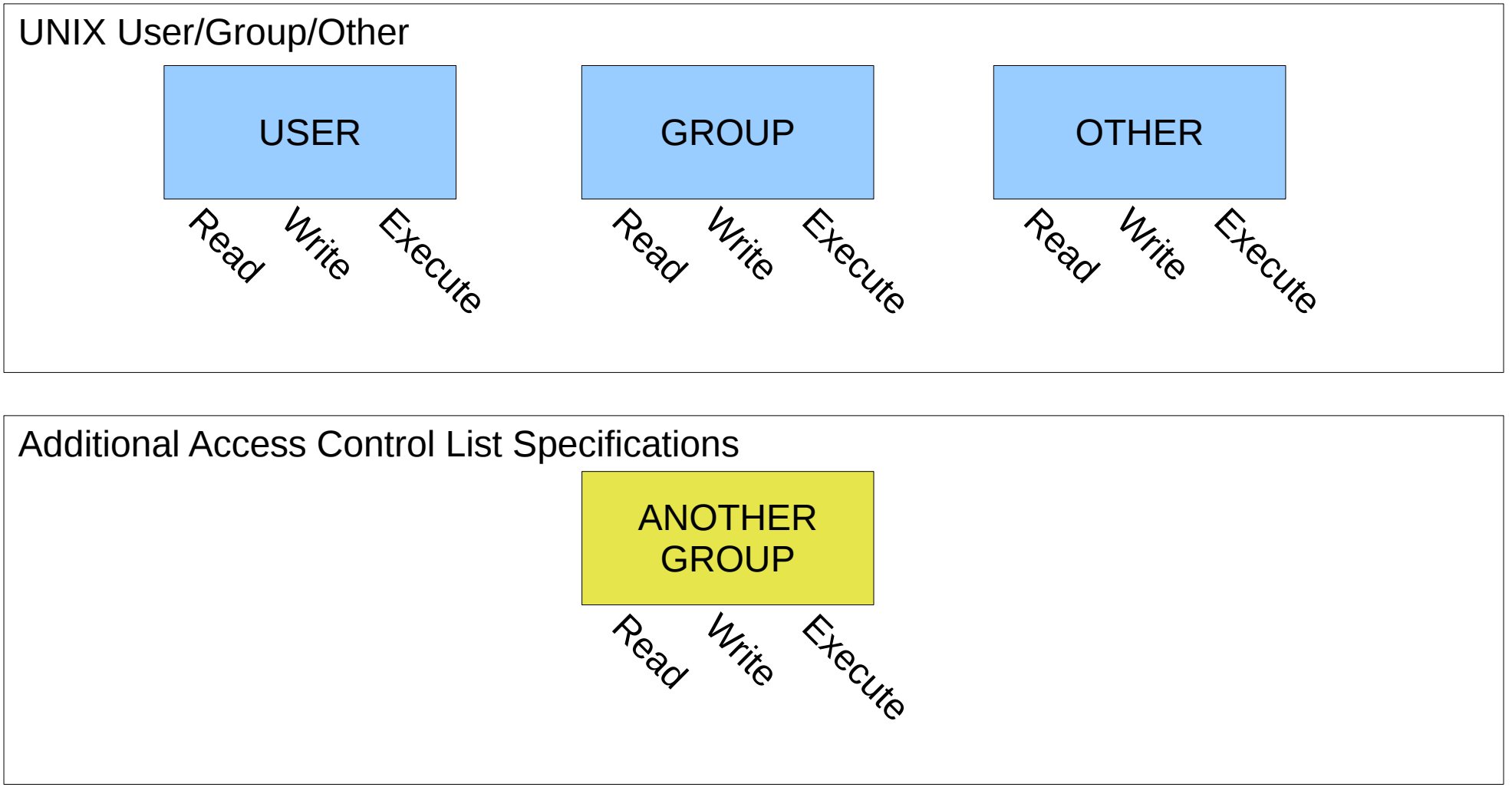
Access Control Lists

UNIX User/Group/Other

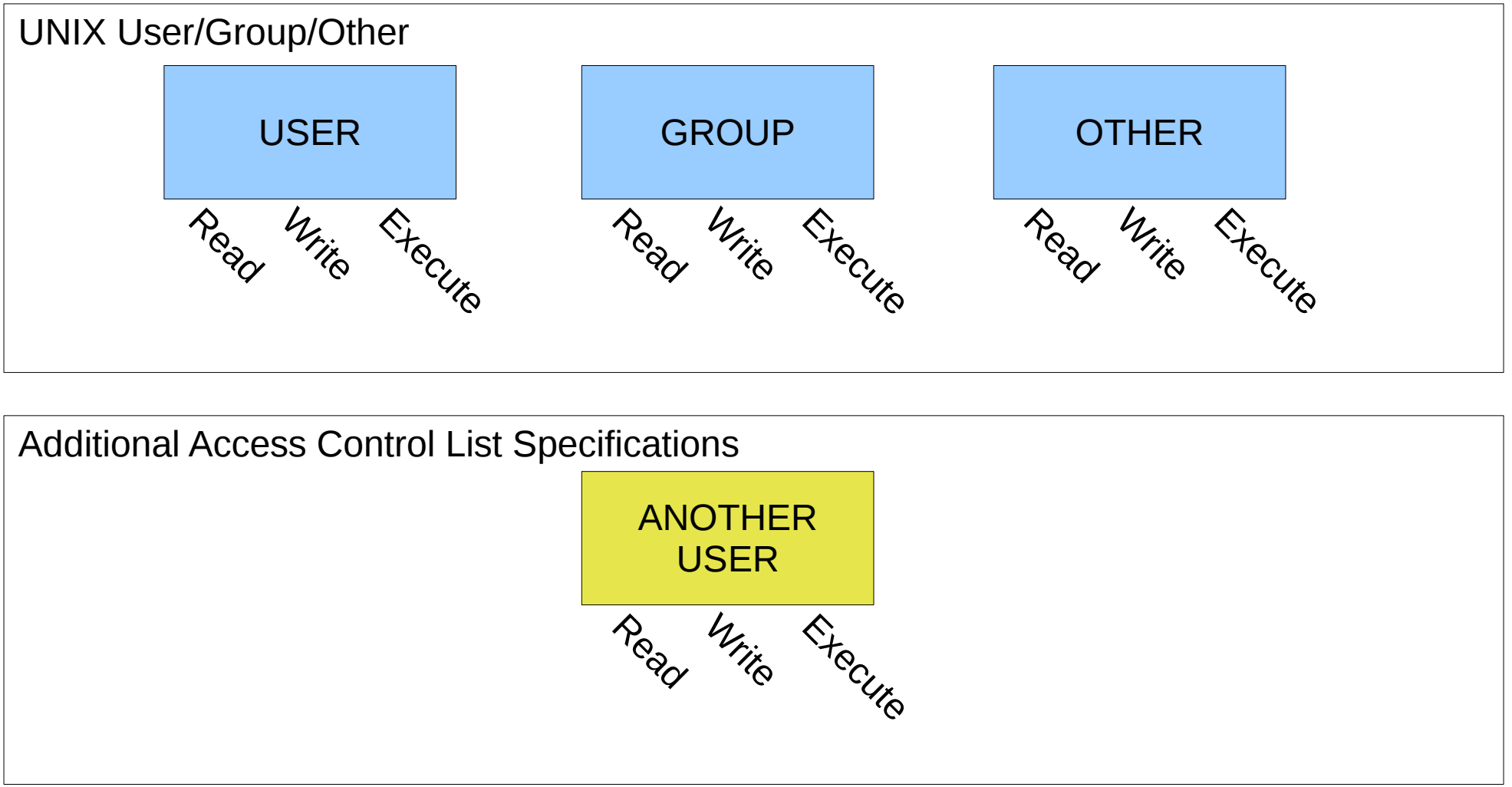


Additional Access Control List Specifications

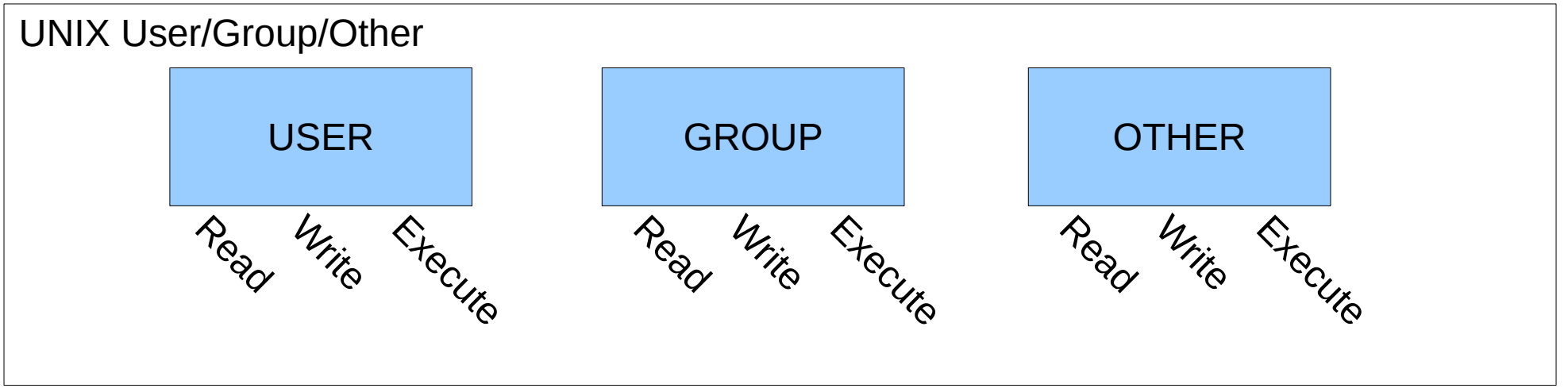
Access Control Lists

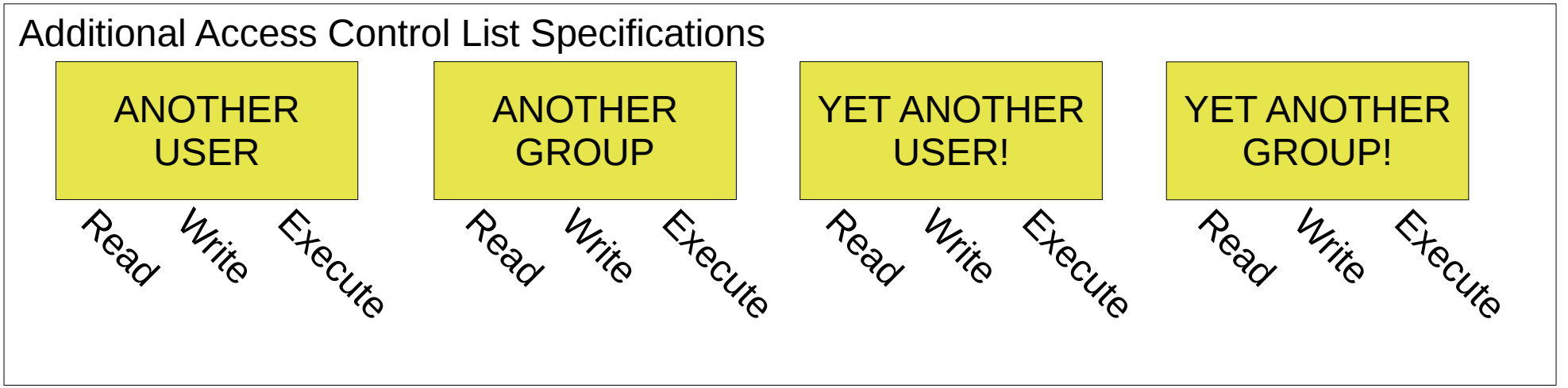


Access Control Lists



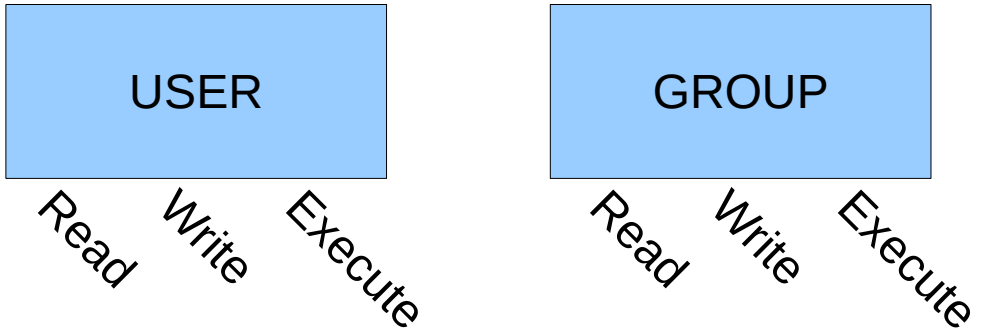
Access Control Lists





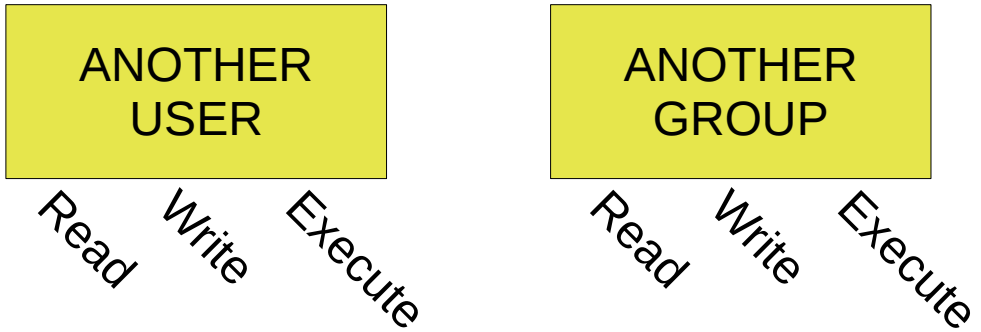
Access Control Lists

UNIX User/Group/Other



- File Ownership
  - User ownership
  - Group ownership
- QUOTA

Additional Access Control List Specifications



- Only for access control

Access Control Lists

- Permissions are additive
  - If a user matches multiple list entries, the maximum permissions allowed by any are granted.

setfacl

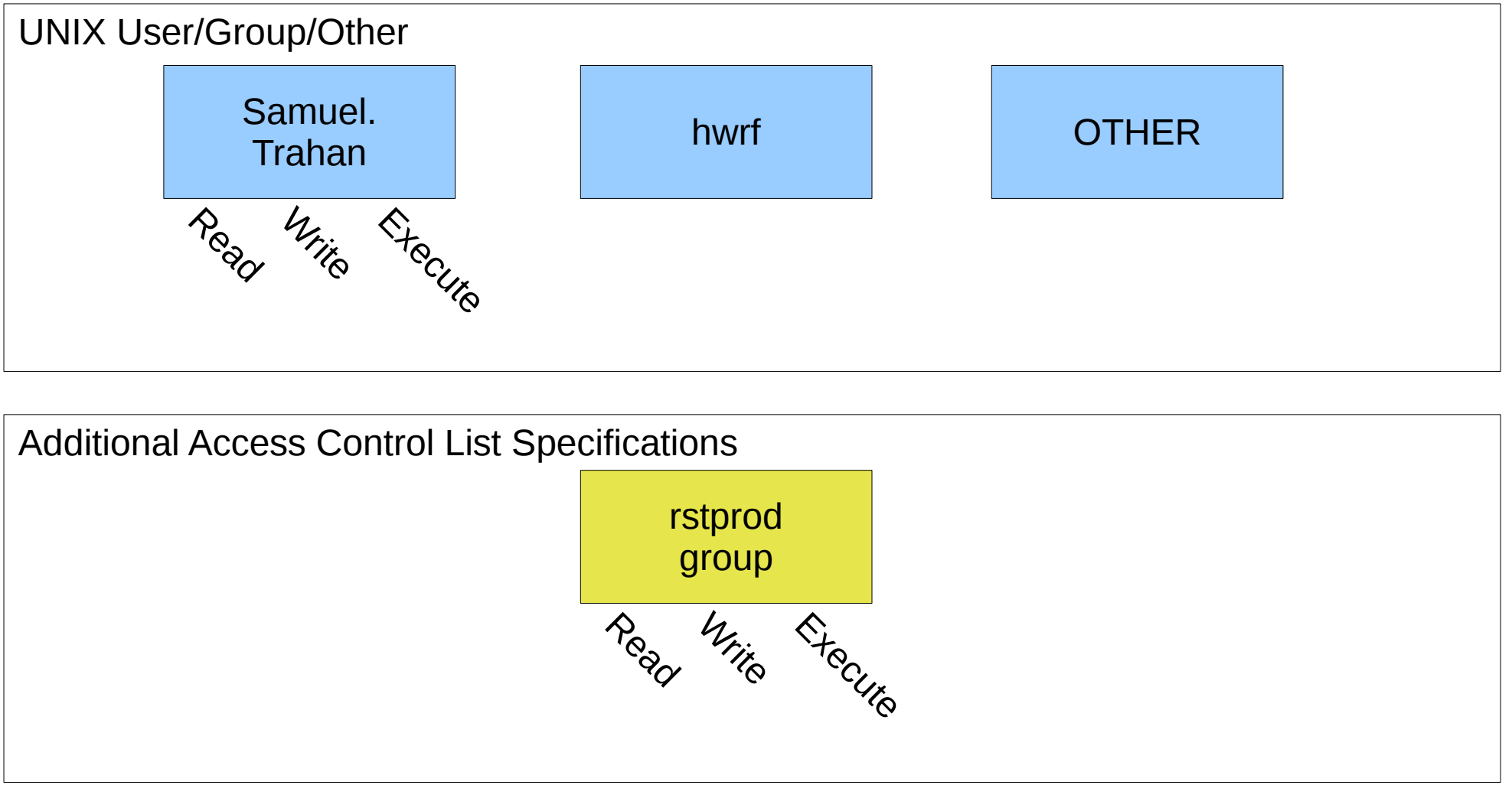
- setfacl -m g:groupname:rwx
  - Give group “groupname” read, write and execute
- setfacl -m u:username:rwx
  - Give user “username” read, write and execute
- setfacl -x g:groupname
  - Remove groupname from the access control list
- setfacl -x u:username
  - Remove username from the access control list

getfacl

- Lists all access control list entries:

```
me@zeus> getfacl afile
# file: afile
# owner: Samuel.Trahan
# group: hwrf
user::rw-
group::---
group:rstprod:r-x
mask::r-x
other::r--
```

ACL For Restricted (rstprod) Data



ACL for Restricted (rstprod) Data

- Lists all access control list entries:

```
me@zeus> getfacl afile
# file: afile
# owner: Samuel.Trahan
# group: hwrf
user::rw-
group::---
group:rstprod:r-x
mask::r-x
other::r--
```

People only in my group (hwrf) have no access.

BUT anyone in rstprod will have access

Rstprod Utilities
Craig Tierney

- tag_rstprod
  - remove group permissions, add rstprod permissions
  - does NOT change group ownership back to your group.
- untag_rstprod
  - removes extra ACL entries (anything other than user, group, other). This will remove the extra “rstprod” permissions but will not add back in your group’s permissions.
- is_rstprod
  - determines if file is correctly set to have rstprod permissions