ACLs, Caps, and attr's
it's not just RWX any more

Stuff tacked onto the side of the files….
….some of them you can use yourself

David Alan Gilbert – September 2020

ACLs

- **Add permissions for individual users/groups**

  Don’t need to be part of a group

- **Commonly used on local devices**

  e.g. CDROM, webcam

  Your user added when you login

- **Directories can have defaults**

  So they gain permissions when anything is created in the directory.

```
# file: dev/dvd
# owner: root
# group: cdrom
user::rw-
user:dg:rw-
group::rw-
mask::rw-
other::---
```

ACLs - examples

- **getfacl/setfacl**

```
$ setfacl -m ‘dg:rwx’ test
$ ls -l test
   -rw-rwxr--+ 1 root root 6 Sep  4 21:55 /tmp/test
$ getfacl test
   # file: test
   # owner: root
   # group: root
   user::rw-
   user:dg:rwx
   group::r--
   mask::rwx
   other::r--
```

Capabilities – it’s not root any more

- **Used to need ‘root’ to do some things**
  - now need the **right** capability – e.g. ‘CAP_NET_RAW’
  - Give processes just enough to do what they need
    - Don’t need to give a process root just to send a weird packet
  - Can make executables gain capabilities selectively:

```
$ getcap /bin/ping
/bin/ping = cap_net_raw+ep
```

If ping was broken somehow, you haven’t given it all of ‘root’

Extended attributes - xattr

- **key/value pairs on any file**

  - You can add your own arbitrary ones [some size limits]

  - Used by the system for capabilities, [maybe] ACLs, SELinux

- **Example:**

```
$ setfattr -n user.animal -v cat my.jpg
$ getfattr my.jpg
# file: my.jpg
user.animal=”cat”
```

- **One of 4 ‘classes’:**

  ‘user’ (follows normal file permissions)

  ‘security’, ‘system’ restricted writing - varies

  ‘trusted’ – restricted read/write

Extended attributes - uses

- **Used to store ACLs, capabilities, and SELinux:**

```
$ getfattr -m '' /dev/cdrom -d
getfattr: Removing leading '/' from absolute path names
# file: dev/cdrom
security.selinux="system_u:object_r:removable_device_t:s0"
system.posix_acl_access=0sAgAAAAEABgD/////AgAGAOgDAAAEAAYA/////
xAABgD/////IAAAAP////8=
$ getfattr -m '' -d /bin/ping
getfattr: Removing leading '/' from absolute path names
# file: bin/ping
security.capability=0sAQAAAgAgAAAAAAAAAAAAAAAAAAA=
```

- **‘trusted’ a bit rarer**

  Typically used by daemons to store something

Notes

- **Not all filesystems support these things**
  - e.g. FAT supports none (?)
- **Some filesystems handle them in different ways**
  - ACLs might be stored separately, or might be an attr.
- **Some limits on lengths**

Tar and friends

- **tar --xattrs --acls --selinux**
  - --xattrs doesn’t seem to include the selinux or acl xattr

```
$ sudo tar -cvvvf /tmp/my.tar --xattrs --selinux my.jpg --acls
-rw-rw-r--+ dg/dg             0 2020-09-05 15:58 my.jpg
  s: unconfined_u:object_r:user_home_t:s0
  a: user::rw-,user:camftp:rw-,group::rw-,mask::rw-,other::r--
  x: 3 user.animal
```

  - **doesn’t** seem to preserve capabilities
- **rsync --xattrs --acls is similar**
  - Seems to preserve capabilities

Summary

- **Extra things tacked onto files**
  - Not in the contents, but kept with it in the filesystem
- **PRO: Don’t actually change the file contents**
- **PRO: Compared to a separate file, can’t get separated**
- **CON: Some things don’t understand them**