User and Group Authentication

Intermediate System Administration
Spring 2010
Michael Gasidlo

Last time

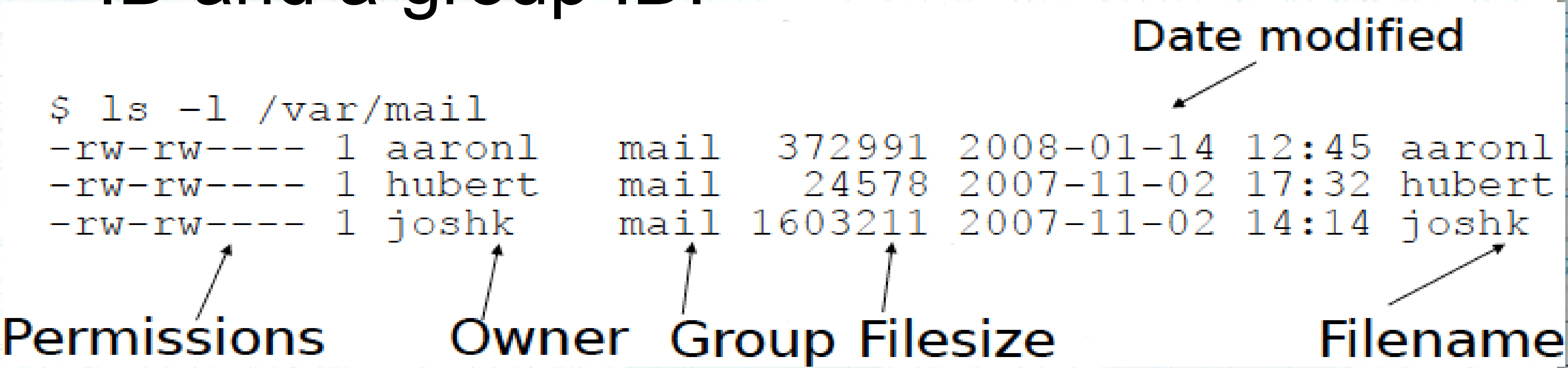
- Building software from scratch
- We apologize again for the somewhat rushed nature of the lecture

This Time

- Learn about file, user, group permissions
- When you log into a Unix machine, how is your password checked?
- Special types of permissions: sticky bit, setgid, setuid
- sudo – Administrative permission controls with ACLs

Owners, Groups, Permissions

- In Unix, every file associated with a user ID and a group ID:



```
$ ls -l /var/mail
-rw-rw---- 1 aaronl   mail   372991 2008-01-14 12:45 aaronl
-rw-rw---- 1 hubert   mail    24578 2007-11-02 17:32 hubert
-rw-rw---- 1 joshk    mail  1603211 2007-11-02 14:14 joshk
```

- Many users can be in one group; one user can be in many groups
- Here, aaronl can read/write his mail file, and members of group mail also can

Owners, Groups, Permissions

- Utilities that help you change this stuff:
  - chmod- change permissions
  - chown- change the ownership
  - chgrp- change the group ownership
- Remember, you can set permissions individually for each set of users: the owner, group, or everyone else

Owner, Groups, Permissions

- 3 types of file permissions:
  - Read: the ability to read the contents of the file
  - Write: the ability to modify the file
  - Execute: the file can be run as a program
- New permissions:
  - Sticky bit: All files created in dir will have GID of dir
  - Setuid: Executables run as the owner
  - Setgid: Executables run as the group

User and Group Information

- How is all of this data stored?
- Three files:
  - /etc/passwd: stores username, user ID, and personal information
  - /etc/shadow: stores mapping from username to passwor hash (only readable or writable by root)
  - /etc/group: stores group names, ID's, and group membership
- Use getent to lookup information in these files

Examples

- A passwd entry
- A shadow entry
- A group entry

Network Authentication

- Many Unix systems use the passwd/shadow/group method of authentication
- NIS: Network Information Service
- LDAP: Lightweight Directory Access Protocol
- Using a system called PAM (Pluggable Authentication Modules), you can use anything for authentication
  - Fingerprints, SecurID token, iButton. . .

Network Authentication

- The new standard: LDAP/Kerberos
  - LDAP: passwd/group replacement
  - LDAP can also store password hashes
  - Kerberos: authentication over insecure networks
  - LDAP/Kerberos form the backbone of most modern network authentication mechanisms
  - CalNet is an LDAP/Kerberos database

sudo

- A tool for letting normal users run certain things as root
- Like an ACL for privileged commands
- Managed with the visudo command

`# User privilege specification`

`root ALL= ALL(ALL)` (root may use all commands – duh)

`%wheel ALL= ALL(ALL)` (all in group wheel also may do everything)

`wm ALL=/usr/sbin/apache2ctl` (wm may only use apache2ctl)