User & Group Authentication

Intermediate Systems Administration Decal
September 30, 2008
Joshua Kwan

Last time…

- Filesystem hierarchy in UNIX: /dev, /usr, /bin, /sbin, etc.
- Regular files, directories, links, device files, named pipes
- The difference hard links and symbolic links
- Why file extensions don’t matter … that much

Homework 1 Remarks

- Issues with the substitution idiom
- wget's progress bar: stdout, stderr, stdin
- Google is your friend; looking up answers
  - displaying the exit code: $?
    I searched for "exit code linux" on Google.
  - running a program in the background: *command* &
    I searched for "run program background linux".

Input/Output Channels

- **Three** input/output channels in Unix
  - stdin (Standard Input): by default, the keyboard. *Use* **<** *and* **|** *to modify this behavior*
  - stdout (Standard Output): by default, your terminal screen. *Use* **>** *to modify*
  - stderr (Standard Error): by default, *also* your terminal screen. *Use* ***2>*** *to modify*
- wget used **stderr** to print its progress bar. Why?

A couple more hints...

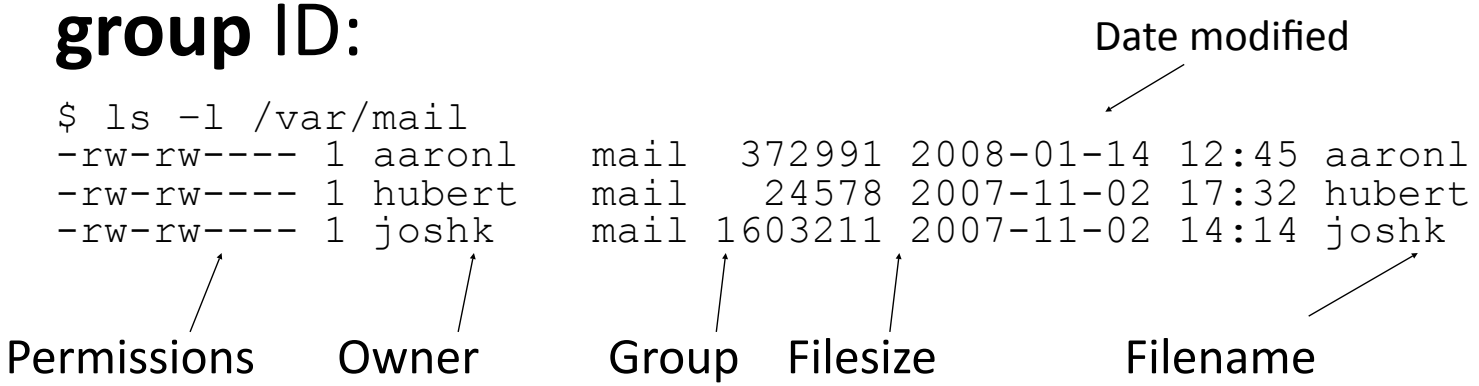
- **Changing shell**: ssh update; you can change your default shell to /bin/bash.
- **Searching in man pages**: forward slash "/", followed by the term. Term may not contain a slash unless you escape it with backslashes:
  - searching for "bah": "/bah"
  - searching for "/proc/self": "/\/proc\/self"

Today

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

Owners, Groups, Permissions

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



- Many users can be in a single 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 do this stuff!
  - **chmod** – Change the permissions on a file.
  - **chown** – Change the owner of a file.
  - **chgrp** – Change the group association of a file.
- Remember, you can set permissions individually for each set of users: the **owner**, **group**, or **everyone else**.

Owners, Groups, Permissions

- 3 types of file permissions:
  - Read: the ability to read the content 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 user who owns the file (setuid root: anyone can run this, and run as root.)
  - Setgid: Executables run as group associated with file. (setgid games: useful for saving high scores, why?)

User and Group Information

- How is all of this data stored?
- Three files…
  - /etc/passwd: Stores user name, user ID, and personal information. (World readable)
  - /etc/shadow: Contains mapping from user name to password (Only readable/writable by root)
  - /etc/group: Contains group names, group IDs, and members of the group (World readable)
- Use **getent** tool to look things up in these files

Examples

- A passwd entry

```
joshk:x:1000:1000:Joshua Kwan,208,,:/home/joshk:/bin/zsh
```

- A shadow entry

```
joshk:$1$/SWUUnPr$lx2ILBmkfsd61dTbMi.lQ.:13037:0:99999:7:::
```

- A group entry

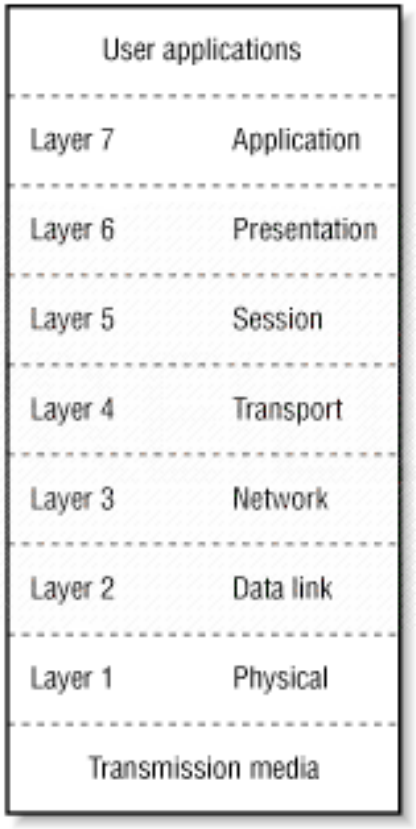
```
wheel:x:500:wjm,joshk
```

Network Authentication

- Many UNIX systems use the passwd/group/shadow 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...

Diversion (Cool Stuff)

- Remember the seven-layer OSI model
- Intent: Each layer uses layer below it to provide service to layer above it
- If you replace a low layer properly, you get all the rest for free!



IP over Avian Carrier

- RFC 1149 – look it up! (When was it written?)
- Carrier pigeons replace layer 1 – physical medium
- Some crazy Norwegians tried it out in 2001!

IP over Avian Carrier

- Results of the experiment:

```
vegard@gyversalen:~$ ping -i 900 10.0.3.1
PING 10.0.3.1 (10.0.3.1): 56 data bytes
64 bytes from 10.0.3.1: icmp_seq=0 ttl=255 time=6165731.1 ms
64 bytes from 10.0.3.1: icmp_seq=4 ttl=255 time=3211900.8 ms
64 bytes from 10.0.3.1: icmp_seq=2 ttl=255 time=5124922.8 ms
64 bytes from 10.0.3.1: icmp_seq=1 ttl=255 time=6388671.9 ms
--- 10.0.3.1 ping statistics ---
9 packets transmitted, 4 packets received, 55% packet loss
round-trip min/avg/max = 3211900.8/5222806.6/6388671.9 ms
```

Administrivia

- Try not to miss lectures without letting me know!
- All of you who are enrolled should have account forms by now. If not, bug me.
- The registration process on your class accounts should work now.

“sudo”- Fine Grained Admin Control

- **sudo**: 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)
```