

Controlling System Access

Most Linux systems still use standard UNIX access control system:

1. Access control decisions depend on user's UNIX group membership.
2. Objects (files, ps) have owners and can control them.
3. You create object => you own it.
4. Root has unlimited privilege.
 - a. System calls are restricted to root, some use more complicated scheme.
 - b. FS access is most elaborate.

Filesystem and kernel have a relationship

1. Communication with devices is done with files that represent them in /dev directory.
2. Device files belong to FS, so subject to file access control semantics.

Filesystem Access control

1. Each file has an owner and a group.
2. Owner sets permissions on their files.
3. Groups defined in **/etc/group** file.
4. User IDs (UIDs) re mapped to users in **/etc/passwd**.
5. Group IDs (GIDs) are mapped to groups in **/etc/group**.

Who is the root?

1. Superuser, "root".
2. UID is 0

Can you change the account name or add other accounts with user id of 0?
Yes, but.... Bad idea. Why?
3. Can you login into root account? Yes, but..... Another bad idea... Why?
 - a. Root logins are not logged to indicate what was performed.
 - b. Many people can have root logins, so who did iwhat and when?
 - c. Should disable everywhere, but the physical system console.

su: substitute user

1. **su** (no arguments) prompts for root password and starts a root shell
 - a. does not record commands executed, but logs who became root and when.
 - b. point of entry is /home directory of the root.
 - c. displays the entire CLP (command line prompt)
2. **su -** (hyphen) prompts for root password and starts root shell
 - a. point of entry is /root directory (this is what hyphen stands for).
 - b. displays the entire CLP.

3. **su username** – can login as *username* with their password
4. always use full path **/bin/su** or **/usr/bin/su** to avoid using rogue commands.
5. What is group **%wheel**?

special user group used on some Unix systems (BSD) allowed to su or sudo.
Ubuntu creates a group called sudo with similar purpose to %wheel group.

sudo : limited su

1. Keeps logs of commands, users, hosts, directories, and times.
2. Asks for the password of user running sudo.
3. sudo checks **/etc/sudoers** file to see who is authorized to do what and asks for user's own password.
4. Gives you 15 minutes before you have to re-authenticate.
5. Edit it with **visudo**!
6. Maintained by Todd Miller
 - a. improper syntax in **/etc/sudoers** can leave you with a system where it is impossible to obtain elevated privileges. Do this:

sudo visudo

- b. **visudo** opens a text editor like normal, but validates the syntax of the file upon saving. This prevents configuration errors from blocking **sudo** operations, which may be your only way of obtaining root privileges.
- c. **visudo** opens the **/etc/sudoers** file with default editor, even though it says vi. Ubuntu, however, has configured it to use the nano instead. You can change the default by typing the command below and selecting another editor from the menu.

sudo update-alternatives --config editor

File example from the textbook (well, almost):

```
# Set defaults
Defaults    env_reset
Defaults    mail_badpass
Defaults    secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin"
```

```
#Define aliases for machines in CS & Physics departments
Host_Alias CS = tigger, anchor, piper, moet, sigi
Host_Alias PHYSICS = eprince, pprince, Icarus

#Define collections of commands
Cmnd_Alias DUMP = /sbin/dump, /sbin/restore
Cmnd_Alia  WATCHDOG = /usr/local/bin/watchdog
Cmnd_Alias SHELLS = /bin/sh, /bin/dash, /bin/bash

#Permissions
mark, ed    PHYSICS = ALL
herb        CS = /usr/sbin/tcpdump : PHYSICS = (operator) DUMP
lynda       ALL = (ALL) ALL, !SHELLS
%wheel      ALL, !PHYSICS = NOPASSWD : WATCHDOG
```

Sudo always obeys the last matching line.

Advantages of sudo:

1. Everything is logged!
2. Users can do specific chores without unlimited root privileges.
3. No need to give out root password to anyone.
4. sudo is faster – used on command line, no need to su or login as root.
5. Revoke privileges without changing root password.
6. Have a list of all users with privileges.
7. One file controls access to entire network.
8. Runs on all UNIX/Linux systems

Disadvantages:

1. Breached account of a sudoer = breach of the root account.
2. Can be subverted by **sudo sh** and **sudo su**

What is the difference between commands?

sudo su -- will place you into a /home directory and display the full prompt:
"user@host:/path\$".

sudo sh -- will place you into /home and display # for the prompt only

sudo su - -- (with a hyphen) places you to /root with full prompt.

Talking about /etc/passwd

1. List of users recognized by system.
2. World readable, used to store encrypted users' passwords.
3. Ubuntu stores encrypted files in /etc/shadow, which is NOT world readable.
4. System checks the file to determine user's UID and home directory at login time.
5. 7 fields:
 - a. Login name
 - b. Encrypted password placeholder UID
 - c. GID
 - d. Optional info
 - e. Home dir
 - f. Login shell

/etc/shadow

1. Encrypted passwd field used DES, MD-5 in the past.
2. Now uses salted SHA-512, 86 chars, start with \$6\$.