System Administration

User and Group Management

All processes on the system run under by a *user*.

Users can be collected into *groups* which can be given common attributes

Users and groups are represented by the system using unique numeric IDs

Special User IDs:

- 0 – root
- 1 – bin
- 2 – daemon
- 99 – nobody

System Administration

User and Group Management

User accounts and group memberships are kept in two files - */etc/passwd* and */etc/group*

A typical entry in */etc/passwd* looks like

nobody:x:99:99:Nobody:/:/sbin/nologin

Username

Password

Userid

Groupid

Full Name

Home directory

Shell

System Administration

User and Group Management

More About */etc/passwd*

For historical reasons, /etc/passwd must be group readable.

This is a BIG security hole.

Shadow passwords were developed as a first attempt to make things more secure

All entries in */etc/passwd* are *shadowed* in the file */etc/shadow* where the actual passwords are kept.

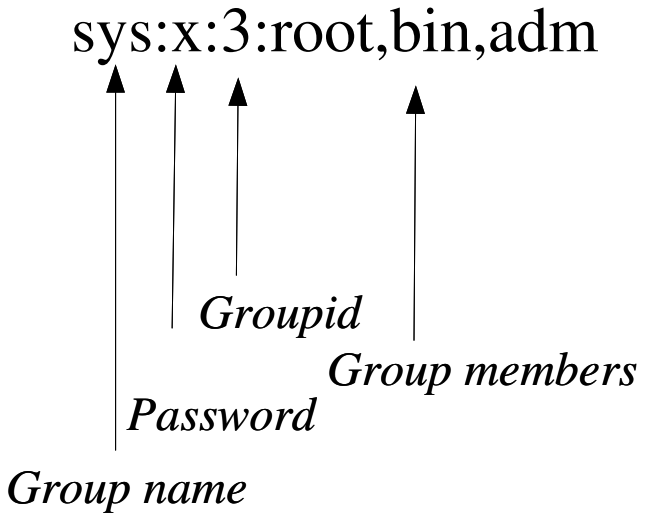
Only root can read */etc/shadow*

An *x* in the password field signifies the use of shadow passwords

System Administration

User and Group Management

A typical entry in */etc/group* looks like



System Administration

Adding and Deleting Users

Things to do before adding a new user:

- Choose a username
- Choose a default shell for the user. Allowed shells are listed in */etc/shells*
- Decide where to place the user's home directory
- Decide in which groups this user will be placed
- Pick an initial password

  14jul1789

System Administration

Adding and Deleting Users

Adding users the HARD way

- Edit the */etc/passwd* file and add
  - the username
  - userid
  - default shell
  - home directory
- Set the user's password with the **passwd** command

  passwd *username*
- Edit the */etc/group* file and add the user to the desired groups

System Administration

Adding and Deleting Users

Adding users the HARD way

- Create the user's home directory
- Copy any relevant start-up scripts and files to the user's home directory
- Use the **chown** command to change the user and group ownership of the user's home directories and all the files in it

chown -R *username.groupname <homedir>*

System Administration

Adding and Deleting Users

Adding users the EASY way

The **useradd** command

The **useradd** command and the files in */etc/skel* make life easier for the sysadmin. All of the above steps can be done in two as follows:

useradd -d *home_dir* **-g** *initial_group* ****
-G *additional groups* **-s** *shell* ****
-u *uid* <*username*>

passwd <*username*>

This will create the user's home directory, copy default files from */etc/skel*, add the user to the password and group files and set their password.

System Administration

Adding and Deleting Users

Users may be added to groups later using the **useradd** command. Or you can simply edit */etc/group*

Users may be removed from groups by editing the */etc/group* file.

Users may be removed from the system using the **userdel** command.

System Administration

Adding and Deleting Users

Or, you can use the GUI tool:

System ->
    Administration ->
        Users and Groups

/usr/bin/system-config-users

System Administration

Changing User Information

At any later time, root or the user may change some of the information associated with a user.

- **chsh** – changes the default shell
- **chfn** – changes the user's full name and other “finger” information as stored in */etc/passwd*
- **passwd** – changes the user's password

System Administration

Adding and Deleting Users

Adding users the EASY way

Exercise

Add two new users, using the method of your choice. Give one an easy password and the other a hard password

```
# /usr/sbin/useradd -s /bin/tcsh linus
# passwd linus
# /usr/sbin/useradd cody
# passwd cody
```

System Administration

Distributed User Management

For users using multiple systems (e.g. clusters), maintaining the same file on all systems is cumbersome and prone to error.

Use centralized database

Three possible (of many) methods:

- NIS – Network Information Services
- LDAP – Lightweight Directory Access Protocol
- Kerberos

System Administration

Distributed User Management

NIS

NIS uses a master server (and potential slave servers) that maintains a central password file.

Clients maintain a local password file (and other files that you want centrally maintained) which contain a “+” character to indicate the use of NIS

Changes made by the user on a client are pushed to the server and from the server to the slaves

Each client knows which machines contain the data

System Administration

Distributed User Management

LDAP

LDAP began its life as an modification of the X500 directory standard.

It has now morphed into a gargantuan database which is being (over) used to serve a variety of information

Is most often used for e-mail address look-up

As a database, it can be configured to hold passwords. LDAP clients connect to it and make requests for information

System Administration

Distributed User Management

Kerberos

Kerberos is a three-party authentication scheme developed by MIT for Project Athena (adopted by ISU as Project Vincent)

Information is passed encrypted between clients, servers and the Kerberos server

Each party obtains a *key* which allows them to access information encrypted by *their* key.

In this way, each machine can only open information for which it has a key.