Adding New Users

MSc. Ivan A. Escobar Broitman

http://ivanescobar.com

iescobar@itesm.mx

The /etc/passwd File

The /etc/passwd File is a list of users recognized by the system.

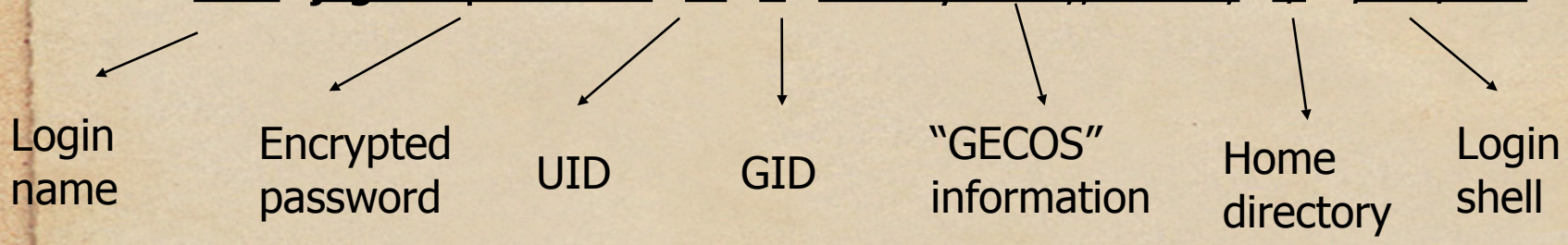
- Login name
- Encrypted password
- UID number
- Default GID number
- "GECOS" information: full name, extention, home phone
- Home directory
- Login shell

/etc/passwd file (MAC)

- nobody:*:-2:-2:Unprivileged User:/:/usr/bin/false
- root:*:0:0:System Administrator:/var/root:/bin/sh
- daemon:*:1:1:System Services:/var/root:/usr/bin/false
- uucp:*:4:4:Unix to Unix Copy Protocol:/var/spool/uucp:/usr/sbin/uucico
- lp:*:26:26:Printing Services:/var/spool/cups:/usr/bin/false
- postfix:*:27:27:Postfix User:/var/spool/postfix:/usr/bin/false
- www:*:70:70:World Wide Web Server:/Library/WebServer:/usr/bin/false

Example:

root: jsg8Y.1p6uWMo: 0 : 0: The system,,x6096, : / : /bin/csh



* Each line in the file represents one user and contains seven fields separated by colons

* Root : x : 0 : 0 : root : /root : /bin/bash

shadow

Login name

- Must be unique.
- Usually no more than 8 characters long depending on the OS.
- NIS or NIS+, login names are limited to 8 characters regardless of the OS.

Login name cont.

Thumb up rules:

- Stick to alphanumerics and to limit login names to 8 characters.
- Case sensitive.
- Since most mail systems expect login names to be lower case, we suggest avoiding uppercase characters in login names unless the user is not expect to receive any mail.
- Easy to remember. F_names, l_names, initials, or some combination of these all make reasonable naming schemes.

More than one machine

Login names should be unique:

1. A user should have the same login name on every machine.
2. A particular login name should always refer to the same person.

* Duplicate names can lead to email confusion. Users will often send mail to the wrong address.

Edit /etc/passwd

Q: How to edit /etc/passwd to create a new account ?

- '*' in the encrypted passwd field prevents unauthorized use of the account until you have set a real password.

Edit /etc/passwd cont.

- Big no no

Never leave passwd field empty – that introduces a jumbo-sized security hole because no passwd is required to access the account.

Encryption algorithm

Standard DES passwords:

- Unencrypted passwords is limited to 8 characters.
- Only first 8 chars are significant for long password.

Hint:

- HP-UX : trusted mode- allow and use passwords of and length.
- Red Hat linux & Free BSD :
  - support MD5-based Passwd
  - password can be of any length

Password Security

Don't

leave encrypted password in plain view.

Shadow Password mechanism

- Placing them in a separated file that is not world readable

Hint: on Solaris, shadow passwd is required! Must modify the shadow passwd file when adding or removing user to keep it consistent with /etc/passwd (p82)

UID number

- 32 bit integers from 0 – 2,147,483,647
- Suggest: 0 – 32,767
- Root has UID 0
- Assign UIDs to real users starting at 100

UID number cont.

- Big no:

never create multiple accounts with UID 0

if people need to have alternate way to login as root, using a program likes sudo(p41).

- Avoid recycling UID

- prevent confusion if files are later restored from backups in which user are identified by UID rather than a login name.

- keep unique across your entire organization

a UID -> same login name -> same person

UID number cont.

Multiple administrators/ organizations

- Central DB contains record for each user and enforces uniqueness (uniquid).
- Assign each group with an organization a range of UIDs and let each group mange its own set

Side effect:

Keep the UID space separate, but does not address the parallel issues of unique login names.

Default GID number

- 16 or 32 bit integer
- Signed or unsigned
- GID 0 is reserved for “root” or “wheel”
- GID 1 is usually for “daemon”
- Allow a user to be in up to 16 groups at a time, so GID is never used to determine access.

GECOS field

- No well-defined syntax
- Commonly used to record personal information about each user.

Command:

- who
- finger a_user
- chfn a_user

(full name, office, office phone, home phone)

Home directory

- Users are placed in their home directories when they log in.
- Some sys allow the login to proceed and put the user in the root directory. Others do not.
- If home directory are mounted over NFS, they may be unavailable in the event of server or network problems.

Login Shell

- A command interpreter
- Bourne shell(/bin/sh), C shell(/bin/csh)

ksh, bash, tcsh

- Sh is the default on most systems and is used if /etc/passwd doesn't specify a login shell.
- Select/add a shell : /etc/shells

The FreeBSD /etc/master.passwd

- The "real" password file
- **Master.passwd** file function as a shadow password file in that it is readable only by root.
- 3 additional fields

- login class
- passwd change time
- expiration time

The FreeBSD /etc/login.conf

- Sets account – related parameters for user and groups of users.
- When user logs in, the login class field of **/etc/master.passwd** determines which entry in **/etc/login.conf** to apply. If no login class has been specified by the user's master.passwd entry, the default class is used.

The Solaris and Red Hat

/etc/shadow File

1. readable only by the superuser and serves to keep encrypted passwords safe from prying eyes.
2. Provides account information that is not available from /etc/passwd.
3. The shadow file is not a superset of the passwd file, and the passwd file is not generated from it. Must maintain both files by hand.

/etc/shadow

millert:inNO.VAsc1Wn.:11031::180:14::18627

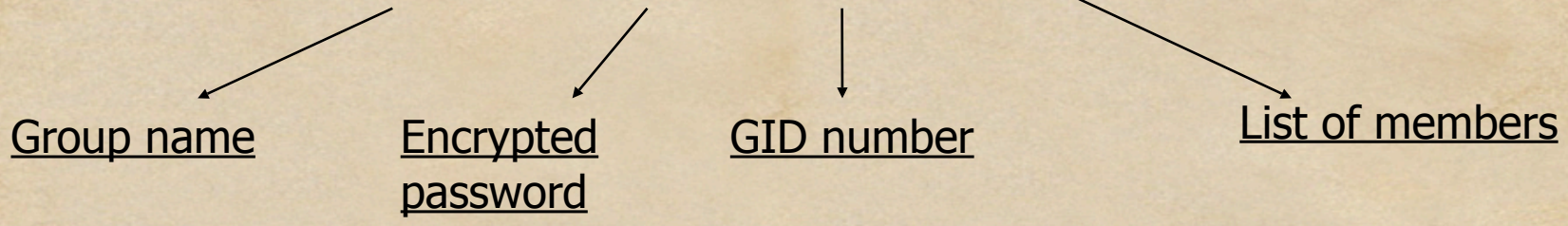
1. Login name
2. Encrypted password
3. Date of last password change
4. Min. number of days between password changes (better unset)
5. Max.number of days between password changes
6. Number of days in advance to warn users about password expiration
7. Number of inactive days before account expiration(solaris)
8. Account expiration date
9. flags

The /etc/group

Contains the names of UNIX groups and a list of each group's members.

example:

Student : * : 200 : dotty,mike,scott



Add users

Required:

1. Edit the passwd and shadow files to define the user's account.
2. Set an initial password.
3. Create the user's home directory

Add users cont.

- **For the user:**

1. Copy default startup files to the user's home directory.
2. Set the user's mail home and establish mail aliases.

Adding users cont.

- **For you:**

1. Add the user to the /etc/group file.
2. Configure disk quotas.
3. Verify that the account is set up correctly.

Adding users cont.

- Edit the passwd and shadow files

1. vipw (allow only one person to edit)
2. vi /etc/passwd

- Edit /etc/group file

Adding users cont.

- Setting an initial password

  # passwd user

Suggestion:

replacing the system's passwd command with an updated version that checks prospective passwords for guessability before accepting them (such as npasswd).

Adding users cont.

- Creating the user's home directory

```
# mkdir /home/staff/tyler
# chown tyler /home/staff/tyler
# chgrp staff /home/staff/tyler
# chmod 700 /home/staff/tyler
```

Adding users cont.

- Copying the default startup files

Begin with '.' , causes **ls** to elide these file from directory listings unless '-a' option is used.

End with 'rc', short for "run command".

Adding user cont.

- Command sequence for installing startup files

```
# cp  /usr/local/lib/skel/.[a-zA-Z]* ~/tyler
# chmod 644 ~tyler /.[a-zA-Z]*
# chown tyler ~tyler /.[a-zA-Z]*
# chgrp staff ~tyler /.[a-zA-Z]*
```

- Edit the /etc/group file

example:

Wheel:*:0:root,evi,garth,scott,trent,tyler

Setting disk quotas

- Set quota limits for each new account with the **edquota** command.

```
# edquota -p proto-user new-user
```

Adding users cont.

- Verify the new login

Login as the new user

% pwd /*verify the home directory*/

% ls –la /* check owner/group of startup files*/

* Remind new user to change their passwords immediately

Removing users

Involves removing all references to the login name that were added by you or your adduser program.

- Set the user's disk quota to 0, if quota are in use.
- Remove the user from any local user databases or phone lists.
- Remove the user from the **aliases** file or add a forwarding address.

Adding users cont.

- Remove the user's **crontab** file and any pending **at** jobs.
- Kill any of the user's processes that are still running.
- Remove the user from the **passwd** and **group** files.
- Remove the user's home directory.
- Remove the user's mail spool.

Adding users cont.

Quot: # quot /home

- Number of disk blocks consumed by each user
- Which UIDs are not list in /etc/passwd

To find exact paths

find –x /home –nouser -print

Management Utilities

- Useradd -> add user
- Usermod -> change the passwd entries of existing users
- Userdel -> remove a user from the system
- Groupadd, groupmod, groupdel -> operate on the /etc/group file

Account management utilities

- **#useradd** cindy

Cindy:*:105:20::/home/hilbert:/bin/sh

- **#useradd** –c "Cindy King" –d /home/math/cindy –g faculty –G famous –m –s /bin/tcsh cindy

Cindy:*:105:30:Cindy King:/home/math/cindy:/bin/tcsh

Add group, create directory, entry in /etc/shadow

Acount management utilities

- Determine default

  #useradd –D

- Set default

  /etc/default/useradd

- Set expiration date

  #usermod –e “June 6,2002” cindy

- Delete account

(remove in passwd shadow group, except home directory)

#userdel cindy