SESSION 4 – USER ACCOUNT MANAGEMENT

Course Writer: Dr. Ed. Danso Ansong, Dept of Computer Sc.
Contact Information: edansong@ug.edu.gh

UNIVERSITY OF GHANA
College of Education
School of Continuing and Distance Education

- This session introduces students to one of the core tasks of systems administration which is user account management.

The key topics to be covered in the session are as follows:

- User account management
- Group account management
- User and group account permissions
- root and sudo privileges management
- Fundamental System administration tasks

- Refer to the following reading material which is available on Sakai

RECOMMENDED TEXT

- Unix And Linux System Administration Handbook, 5th Edition, Linux Administration Handbook, Second Edition [Pages 243-268]
- Linux Administration Handbook, Second Edition [Pages 111-129].

Chapter Objectives

At the end of the session, the student will be able to:

- Explore user and group account management.
- Perform sysadmin tasks using basic administrative tools
- Demonstrative safe removal of user account and files
- Explain the use of user account security and protection

Users

- Many System Administrators rate tasks they have to perform on a "headache" scale. (How nasty will the headache be when I have to do ***task***?)
  - Installing and OS is usually a light headache.
  - Installing applications is usually a light headache.
  - Patches are usually a light headache.
  - Account maintenance is generally a medium sized/nasty headache...

Users

- So far, we have discussed:
  - Booting/Halting a system
  - Installing an OS
  - Customizing/Patching the OS
  - Installing applications
  - License managers
  - Filesystems
  - Processes
- By now we should have a working system. All we need is users...

Users

- Users - background information
  - There are several things to consider before attempting to create/install user accounts on a system.
    - Creating login names
      - How is a login constructed?
        - **Users last name?**
        - **Users first name?**
        - **Combination of names?**
        - **Random string?**
        - **Alphanumeric string?**
        - **It is best if the site has a policy about login names. Otherwise users will request login names that may not be acceptable (to management, society, ...).**


SUDDENLY, FIRST INITIAL AND LAST NAME DIDN'T SEEM LIKE SUCH A GREAT COMBINATION FOR A USER ID AFTERALL
NAME, PLEASE
DAVID. DAVID UDELOVE.

Users

- Users - background information
  - Assigning a homedir
    - On large systems there may be many “user” directories. The system administrator needs to think about how users are distributed across these file systems.
      - » Space requirements
      - » Project/Work Unit Association
      - » Other considerations (special needs)

Users

- Users - background information
  - Creating UID's
    - Each user must have a unique user-id. Most Unix systems use integers in the range of 0 - 65536.
      - » Are there special (reserved) userids?
      - » What happens at a large company/university where there are more than 65536 employees?
      - » Are UID's reused? For example, if an employee leaves the company, is their userid assigned to the next person hired in?

Users

- Users - background information
  - Assigning a shell
    - Shells are a very personal choice. But the administrator has to assign some shell program to each user.
      - sh - standard with almost every UNIX
      - csh - standard with almost every UNIX
      - bash - Standard with Linux
      - tcsh - Popular, but not generally shipped with system.
      - ksh - used by many install programs

Users

- Users - background information
  - In addition to the items above, the administrator may elect (or be forced) to set constraints like:
    - What workstations can the user access
    - What hours can the user access the workstation
    - Account expiration date
    - How often user must change their password
    - What are acceptable passwords

Users

- Users - background information
  - Format of password file (Unix)
    - The Unix password file conforms to a very strict format:
      - **USER:PASSWD:UID:GID:GECOS:HOMEDIR:SHELL**
      - If the password file format is incorrect, one of the following situations may occur:
        - » Nobody listed after the error can login.
        - » Nobody can login
        - » The password file is automatically truncated by the system to remove the error.

Users

- Password file fields
  - User - the login name assigned to the user.
  - Password - may be one of the following:
    - NP - No password assigned
    - [xX] - Look in some alternate location
    - encrypted password
  - UID - the UID assigned to this user
  - GID - the login group this user belongs to
    - Users may be in other groups (see /etc/group)

Users

- Password file fields
  - GECOS - This field is a list of comma separated informational items related to this user. Standard format is:
    - Full name
    - Office
    - Phone
    - Comments

Users

- Password file fields
  - Homedir - the home directory assigned to this user
  - shell - the shell program assigned to this user
    - Make sure it is listed in /etc/shells!
- Sorting the password file
  - Some sites want names alphabetically.
    - Problem: What happens if an error occurs somewhere before the letter “r” in the password file?
  - Some sites want ascending UID’s.
    - Not real convenient when searching for a username.
  - Some sites have several password files, and use some tool to create password files for individual systems.

Users

- The principle method by which an operating system determines the authenticity of a user is by a password.
  - Good passwords are essential to the security of all operating systems.
  - Choosing passwords, educating users in the use of passwords, and choosing and employing one or more tools to enhance password security are tasks a sysadmin will face when creating user accounts.

Users

- Both Windows and UNIX systems employ reusable passwords as their default.
  - Reusable passwords have several problems.
  - First, they are vulnerable, either through manual or automated brute force attacks, to discovery if unchanged for long periods of time..
  - Reusable passwords are vulnerable to their own quality; poorly chosen passwords are more easily guessed.
  - If the user accesses the system using an insecure connection such as *telnet* or *ftp*, the user's password is transmitted over the connection in clear text, which is easily intercepted if an attacker is listening.

Users

- The first approach to improve password securiy is to educate the users of your systems to the dangers of reusable passwords.
  - Education on choosing good passwords and encouragement to change them periodically is universally applicable to all operating systems.
  - Good password construction techniques include assembling passwords from words separated by punctuation characters or numbers, or assembling a password using the first letter of each word in a phrase of the user's choosing.
  - Semester breaks, seasonal changes, and holiday breaks can help provide cues to encourage periodic password changes.

Users

- Password aging (or password expiration) is another method to improve password security.
  - The aging process allows the system manager to enforce the practice of changing account passwords on a regular basis.
  - The downside to password aging is the psychological factor. Some users dislike changing passwords.
  - Being asked to change with no warning may contribute to a user choosing a simpler, easily guessed password, or simply entering a new password and then changing back to the old password immediately afterward.
  - Password aging is most effective when the account user understands the reasons for periodically changing a password and the elements of a good password, and is given a chance to choose a good password.

Users

- Other features present in some UNIX variants are incorrect password attempt counters and account inactivity timers.
  - These can be employed to reduce the chances of success by an attacker guessing a user's password or of an old unused account being exploited to gain access to a system.
  - A password attempt counter records failed attempts to provide the system with a password. When a user attempts to log in, the number of failed password attempts is checked against a set limit.
  - The user account is disabled if the limit is exceeded. Likewise, an inactivity timer records the last time an account was used.

Users

- In the case of the inactivity timer, when a user attempts to log in, the length of inactivity for the account is compared to a set limit and the account is disabled if it has been inactive for longer than the limit.
- Both of these tools have the downside of preventing access by valid users and of adding additional work for the system administrator as he spends time resetting password attempt counters or inactivity timers triggered by the forgetful or infrequent user.

Users

- The long-term solution to the problems of reusable passwords is passwords that are used just once and not used again.
  - These one-time passwords make use of a shared secret typically held on a secure authentication server and a token held by the user, typically a small calculator or a program on a personal digital assistant (PDA), such as a Palm Pilot.
  - Instead of requesting a password when accessing a system, under one-time passwords the system responds to a log-in request with a challenge in the form of a string of numbers and letters.

Users

- This string is entered into the token that produces another string, the response.
- The response is entered instead of the password to gain access. Both the challenge and the response are a mixture of the shared secret and a continually changing value, usually the current date and time, ensuring that the same combination of challenge and response are never used more than once.

Users

- This sophisticated and secure scheme is not without its own problems. None of the Windows or UNIX variants seem to come with one-time passwords built in.
- They must be added to the system as a separate product. All users making use of the system will be required to carry a token with them, with the resulting problems of loss and damage to the token and the frustration to the user when they are unable to gain access.

Users

- Alternative password token systems are also available.
  - Physical devices such as a smart card or dongle that carry authentication information or provide challenge/response authentication.
  - The devices are read via special readers (smart cards) or are attached to a system via a connection such as a USB port (dongle).
  - Such devices are generally used in highly secure systems for which the cost of the additional hardware for every user can be justified.
  - Another technique is the use of biometric information such as the visual pattern of a fingerprint or the blood vessels in the retina.

Users

- This information is read from the person's finger or eye via a special-purpose reader.
  - Although believed to be very secure, biometrics suffer from problems such as how account revocation is performed, as the information being used for authentication is a permanent feature of the user.
  - As with smart cards and dongles, biometric authentication is only seen in situations for which the cost of the additional hardware can be justified.

Users

- Under NT Workstation, there is a great point/click interface called the User Manager.
  - User Manager lets the administrator add one account at a time on individual computers.
  - User Manager lets the administrator force password changes, disable the user, give the user privileges, move the user to a new directory, ...
  - How would an administrator (easily) add 20 accounts with User Manager?
- Under NT Server (or any system participating in an NT domain) the application is called User Manager for Domains.
  - Same as user manager, but it works with a domain wide account database (registry).

Users

- UNIX suffers from the same account management design problems.
  - The standard tools for adding users are not set up to deal with “mass” account changes.
    - The “old” method for adding/changing user information is to edit the /etc/password file.
      - **vipw** is provided on some versions of UNIX so the person doing the editing can’t do stupid things.
      - Solaris did away with vipw, so you have to use some other text editor if you plan to change the password file manually.
    - Solaris provides **admintool** which can be used like the NT User Manager to add/change/delete one user at a time.

Users

- Solaris provides an extended version of **admintool** which can be used like the NT User Manager for Domains to add/change/delete accounts on all systems (one user at a time).

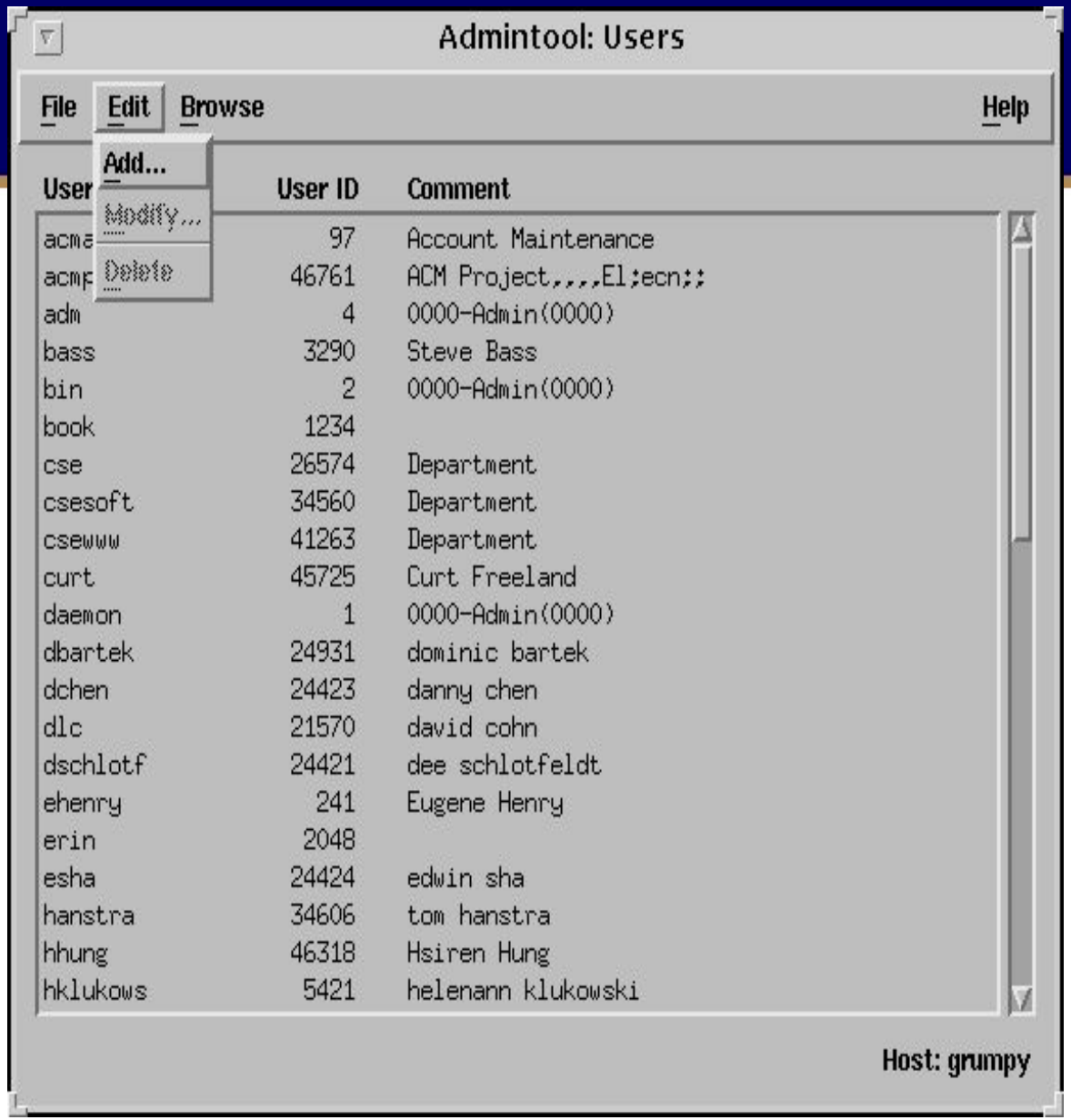
– Problem: How would the administrator install several hundred (or thousand) accounts on several hundred (or thousand) computers with these systems?
  - A few possible answers:
    – very carefully
    – very crabbily
    – they wouldn't
    – they would find a better way

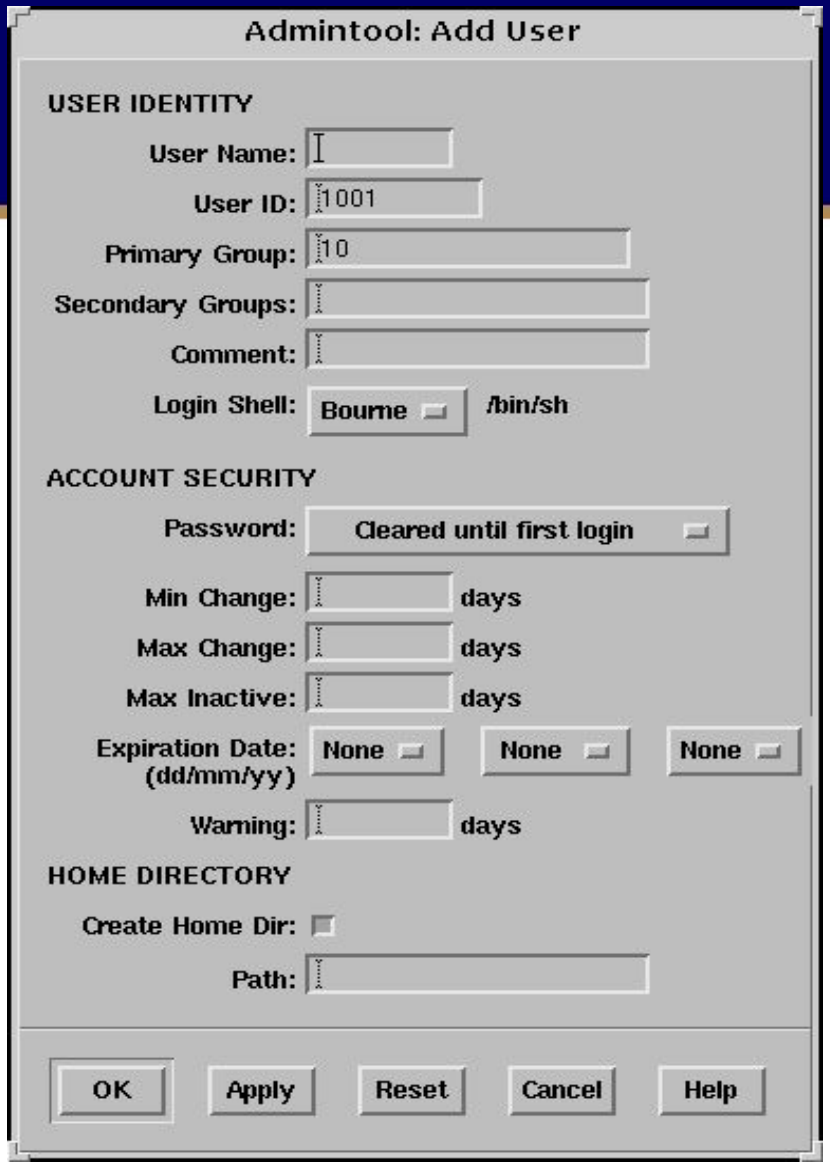
Users

– To start up admintool, login as root, start OpenWindows, and type

 # admintool


Admintool: Users
File
Edit
Browse
Help
Users
Groups
Hosts
Printers
Serial Ports
Software
User Name
D
Comment
acmaint 7 Account Maintenance
acmproj 1 ACM Project,,,,El;ecn;;
adm 4 0000-Admin(0000)
bass 0 Steve Bass
bin 2 0000-Admin(0000)
book 4
cse 26574 Department
csesoft 34560 Department
csewww 41263 Department
curt 45725 Curt Freeland
daemon 1 0000-Admin(0000)
dbartek 24931 dominic bartek
dchen 24423 danny chen
dlc 21570 david cohn
dschlotf 24421 dee schlotfeldt
ehenry 241 Eugene Henry
erin 2048
esha 24424 edwin sha
hanstra 34606 tom hanstra
hhung 46318 Hsiren Hung
hklukows 5421 helenann klukowski
Host: grumpy


Admintool: Users
File
Edit
Browse
Help
Add...
Modify...
Delete
User
User ID
Comment
acma 97 Account Maintenance
acmp 46761 ACM Project,,,,El;ecn;;
adm 4 0000-Admin(0000)
bass 3290 Steve Bass
bin 2 0000-Admin(0000)
book 1234
cse 26574 Department
csesoft 34560 Department
csewww 41263 Department
curt 45725 Curt Freeland
daemon 1 0000-Admin(0000)
dbartek 24931 dominic bartek
dchen 24423 danny chen
dlc 21570 david cohn
dschlotf 24421 dee schlotfeldt
ehenry 241 Eugene Henry
erin 2048
esha 24424 edwin sha
hanstra 34606 tom hanstra
hhung 46318 Hsiren Hung
hklukows 5421 helenann klukowski
Host: grumpy


Admintool: Add User
USER IDENTITY
User Name:
User ID:
1001
Primary Group:
10
Secondary Groups:
Comment:
Login Shell:
Bourne
/bin/sh
ACCOUNT SECURITY
Password:
Cleared until first login
Min Change:
days
Max Change:
days
Max Inactive:
days
Expiration Date:
(dd/mm/yy)
None
None
None
Warning:
days
HOME DIRECTORY
Create Home Dir:
Path:
OK
Apply
Reset
Cancel
Help

Users

- Account Maintenance Packages
  - Several organizations have created account maintenance packages. These packages attempt to solve one or more problems with the standard account installation tools. In lab we will examine a few of these tools:
    - Sun Microsystems - YP (Yellow Pages) also known as Network Information Service (NIS).
    - M.I.T. - Athena Service Management System
    - Oregon State - Asmodeus
    - Purdue University - ACMaint

Summary

- This chapter explored the user account.
- Sysadmins must pay attention to many tasks as part of account creation.
  - Site policies regarding user account names, rights, acceptable use, …
  - Password security
  - Disk management
  - Automation of account creation process.

- Unix And Linux System Administration Handbook, 5th Edition By Evi Nemeth, Garth Snyder, Trent R. Hein, Ben Whaley, Dan Mackin. Released September 2017. Publisher(s): Addison-Wesley Professional. ISBN: 9780134278308
- Practice Of System And Network Administration, The: Devops And Other Best Practices For Enterprise IT, Volume 1, By Thomas A. Limoncelli, Strata R. Chalup, Christina J. Hogan. Released November 2016. Publisher(s): Addison-Wesley Professional. ISBN: 9780133415087
- Essential System Administration, Third Edition by Æleen Frisch, Published by O'Reilly Media, Inc. (20(0-596-00343-9