# CMSE353 Fall 2021

Prepared by Alexander Chefranov 04.10.2018

Modified by Tansel Sarıhan 01.10.2019

# Access Control in Linux

Contents

[CMSE353 Fall 2021 1](#_Toc85618531)

[Access Control in Linux 1](#_Toc85618532)

[Contents 1](#_Toc85618533)

[1. Task 3](#_Toc85618534)

[2. Linux Operating System 3](#_Toc85618535)

[2.1 Bash Terminal 3](#_Toc85618536)

[2.2 List of Some Important and Useful Commands 4](#_Toc85618537)

[3. Introduction to access control 5](#_Toc85618538)

[4. Unix file permissions and inodes 5](#_Toc85618539)

[Example 1 6](#_Toc85618540)

[Example 2 6](#_Toc85618541)

[Example 3 7](#_Toc85618542)

[Example 4 7](#_Toc85618543)

[Example 5 7](#_Toc85618544)

[5. Octal representation of permissions 7](#_Toc85618545)

[Example 6 8](#_Toc85618546)

[6. Changing file permissions on Linux system, adding users, groups, changing file owner and group 8](#_Toc85618547)

[Example 7 9](#_Toc85618548)

[Example 8 9](#_Toc85618549)

[Example 9 10](#_Toc85618550)

[Example 10 11](#_Toc85618551)

[Example 11 11](#_Toc85618552)

[Example 12 12](#_Toc85618553)

[Example 14 12](#_Toc85618554)

[Example 15 12](#_Toc85618555)

[Example 16 13](#_Toc85618556)

[Example 17 13](#_Toc85618557)

[Example 18 13](#_Toc85618558)

[Example 19 13](#_Toc85618559)

[Example 20 14](#_Toc85618560)

[Example 21 14](#_Toc85618561)

[Example 22 14](#_Toc85618562)

[Example 23 15](#_Toc85618563)

[Example 24 15](#_Toc85618564)

[Example 25 15](#_Toc85618565)

[Challenge 1. 15](#_Toc85618566)

[7. Command umask 15](#_Toc85618567)

[Example 26 16](#_Toc85618568)

[Challenge 2. 16](#_Toc85618569)

[8. Set UID (SUID) 16](#_Toc85618570)

[Example 27 16](#_Toc85618571)

[Example 28 17](#_Toc85618572)

[Example 29 17](#_Toc85618573)

[Example 30 18](#_Toc85618574)

[9. Writing a SUID program in C 18](#_Toc85618575)

[Example 31 18](#_Toc85618576)

[Example 32 19](#_Toc85618577)

[Example 33 20](#_Toc85618578)

[Example 34 20](#_Toc85618579)

[Example 35 21](#_Toc85618580)

[Challenge 3 21](#_Toc85618581)

[Challenge 4 21](#_Toc85618582)

[Challenge 5 21](#_Toc85618583)

[Challenge 6 21](#_Toc85618584)

[10. Linux Extended ACLs 22](#_Toc85618585)

[Example 36 22](#_Toc85618586)

[11. Conclusion 22](#_Toc85618587)

[References 23](#_Toc85618588)

Our lab material is based on [1]. Section 1 describes the task. Sections 2, 3 briefly introduce the most important Linux commands and access control concepts. You will work with Fedora Linux-based operating system in the laboratories. Sections 4-10 contain examples (prepared in Kali Linux (with alex@lenovo in the screenshots) and Fedora (with linuxlab@asus in the screenshots) operating systems) and challenges. Section 11 concludes the material.

## Task

Read material below in line with running your own examples repeating Examples 1-36 (screenshots) shown in the lab material (use your own user name instead of alex or linuxlab e.g. “chmod 701 /home/your\_username/”). There are Challenges 1-6 expected to be solved by you. The lab shall be done in groups. Each group prepares a report (pdf file) on the work done containing screenshots of your variants of the Examples 1-36, Challenges 1-6 solutions, and explanations. Also, a **Winrar archive shall be provided** with all the lab related materials (report, sources, executable, etc.). Upload your Winrar file to a location specified by the Lab Assistant.  **Due date for reporting is**

* **Gr 1: November 15, 2021, 14.30, CMPE134 & Teams;**
* **Gr 2: November 11, 2021, 16.30, CMPE238 & Teams.**

**You will run your examples and solutions and explain them answering the questions of the Lab Assistant.**

## Linux Operating System

You will use some Linux operating system installed according to recommendations provided by former Lab Coordinator Abdolrahman Farshgar. For example, Fedora is a Linux distribution developed by the community-supported Fedora Project. It is an open-source and free. Fedora operating system is user friendly because it is developed in collaboration with the user. Screenshots of the experiments given below are from Fedora (with linuxlab@asus) and Kali Linux (alex@lenovo).

### 2.1 Bash Terminal

We will use the bash terminal frequently for our experiments. Therefore, let's get to know what we will see when we open the bash terminal.

 

When we open the terminal, we see an image as above. “linuxlab” is our user name, "asus" after the "@" sign is the name of the machine we use, and "~" means the user's home directory.



Same way, “root” is an username(which has all privileges on the system), “asus” is machine name and “#” means we are logged in as administrator(root).

### 2.2 List of Some Important and Useful Commands

* Fedora uses dnf package manager. If you want to install any open source program or tool, you need to use dnf. For instance, you need to install a text editor to edit your texts or program codes. A text editor “KWrite” can be installed by using “dnf install kwrite” command on terminal.



* Sudo command - The sudo command makes it easier to manage your Fedora system. Certain commands in Fedora expect to be run only by a privileged user or administrator. The sudo command lets you run a command as if you're the administrator, known as root. For instance, “sudo chmod 666 somefile”.



* Su command – switch user. For example, “su student” command can be used for switching between current user and student user.



* Ls command – lists directory contents of files and directories. For example, when run “ls /home/linuxlab” command, contents of /home/linuxlab directory will be shown on terminal window.



* Cd command – changes the current directory. For example, “cd Desktop” command changes the current directory to /Desktop directory. (in the same way, “cd ..” command can also be used to return to the previous directory.)



* Mkdir – This command creates a new directory. Example usage for creating a new directory with name “myLabWorks”: “mkdir myLabWorks”.



* Rm command – this command can be used for deleting some file or directories. For example, we can delete the “test.txt” file with "rm test.txt".



## Introduction to access control

Access control enforces authorization by determining and enforcing which actions are allowed. Some terminology: a subject is an active entity taking actions, such as a user or program, and an object is the (often passive) resource that can be accessed, such as a file or network resource. Access control mediates subjects' access to objects by enforcing a security policy, limiting which actions are and are not allowed. The policy expresses what is allowed, either formally or informally as a set of rules. An access control mechanism is the code or thing that enforces a policy. An access control model is a way of representing and reasoning about a policy or types of policy.

## Unix file permissions and inodes

The traditional Unix security model is based on the discretionary access control (DAC) model, which enables users to configure who can access the resources that they “own”. Each user can control which other users can access the files that they create. This enables users to grant permissions, without involving a system admin. This is the type of security that has traditionally been built into most consumer OSs such as Windows and Unix. Unix file permissions uses an abbreviated (simplified) form of access control list (ACL). A (full) ACL involves attaching a list of every subject and what they can do to each file (this is how Windows manages file access). For example, a file may have this ACL: “Joe can read, Frank can write, Alice can read, and Eve can read”. Unix simplifies permissions by only defining rules for these three kinds of subjects:

● The user that owns the file (u)

● The file's group (g)

● Other users (o)

ls command is used to display the permissions of the files, -l flag provides detailed output, e.g., ls –l /bin/ls displays permissions of the ls command

### Example 1



File path

Owner can read, write, execute

Group can read and execute

Others can read and execute

The file has this many names (hard links)

File owner is root

File group is root

Files size (bytes)

Last modified

The meaning for a regular file (as is the case for /bin/ls, the first symbol is – (dash)):

● **r**: Read the contents of the file

● **w**: Change the contents of the file

● **x**: Execute the file as a process (The first few bytes describe what type of executable it is, a program or a script)

For a directory (the first symbol is d):

● **r**: See what files are in the directory

● **w**: Add, rename, or delete names from the directory

● **x**: 'stat' the file (view the file owners and sizes), cd into the directory, and access

files within

● **t** (instead of x), AKA the “sticky bit”: write is not enough to delete a file from the directory, in this case you also need to own the file.

The permissions for each file are stored in the file’s inode. An inode is a data structure in Unix filesystems that defines a file. An inode includes an inode number, and defines the location of the file on disk, along with attributes including the Unix file permissions, and access times for the file. View the inode number for this file:

ls -i /bin/ls

### Example 2



File type may be also l for links on the files (with the help of the links one and the same data can be accessed using different file names linked to one and the same inode for hard links).

Create a hard link to the ls program:

mkdir /bin/tmp (create a new directory for hard link)

ln /bin/ls /bin/tmp/ls

Now view the details for your new filename, /bin/tmp/ls:

ls -l /bin/tmp/ls

### Example 3



Thus, we see that the both files share the same inode. Thus, change of one of these files will affect also the other one.

Deleting one of the names simply decrements the link counter. Only when that

reaches 0 is the inode actually removed:

rm /bin/tmp/ls

### Example 4



Permission denied! Interestingly, in this case as a normal user we can create the

link to /bin/ls, but cannot then delete that link since the sticky bit is set for the /tmp/

directory.

ls -ld /tmp/

Note the “t” in the permissions, and refer to the meaning described above.

You can delete the link as root:

sudo rm /bin/tmp/ls

### Example 5



We see no content in /bin/tmp/ after /bin/tmp/ls removal.

## Octal representation of permissions

The stat command can be used to display further information from the inode:

stat /bin/ls

### Example 6



Unix file permissions

File’s owner

File’s group

Look through this information. Note that the output includes the access rights, along

with the last time the file was accessed, modified, and when the inode was last

changed.

The output from stat includes the format that the information is stored as, along with a more “human readable” output. As we know, user accounts are referred to by UIDs by the system, in this case the UID is 0, as the file is owned by the root user. Similarly, groups are identified by GID, in this case also 0. The actual permissions are stored as four octets (digits 0-7), in this case “0755”. This translates to the (now familiar) human-friendly output, “-rwxr-xr-x”. For now we will ignore the first octet, this is normally 0, we will come back to the special meaning of this later. Each of the other three octets simply represents the binary for rwx, each represented as a 0 or a 1. The first of the three represents the **u**ser, then the **g**roup, then the **o**ther permission. An easy and quick way to do the conversion is to simply remember:

● r = 4

● w = 2

● x = 1

And add them together to produce each of the three octets. So for example, rwx = binary 111 = (4 + 2 + 1) = 7.

Likewise, r-x = binary 101 = (4 + 1) = 5.

Therefore, “-rwxr-xr-x” = 755.

## Changing file permissions on Linux system, adding users, groups, changing file owner and group

Now, we shall need an opportunity to switch between two users. The list of users can be displayed by

cat /etc/passwd

showing contents of the /etc/passwd file.

### Example 7



We see that /etc/passwd can be read every user. Let us now create a new user, student with password student. We need for that task to use super user rights with the help of sudo. Rights of the users allowed doing sudo (from sudo group) are enlisted in /etc/sudoers file

cat /etc/sudoers

### Example 8



We see that sudo group users have the same permissions as root. Groups and their members can viewed by

cat /etc/group

### Example 9



We see that user alex belongs to sudo group as well as to adm (can monitor system tasks), cdrom (can access CDROM), and dip (can use tools such as ppp, dip etc. to dial-up connection) groups. A new user is created by

sudo adduser student

### Example 10



Check that the new user student is in the list of user:

### Example 11



Create a file named “mysecret” in your home directory:

cat > ~/mysecret

### Example 12



Enter a number of lines of content. Press Ctrl-D when finished entering a “secret” (that others may see). Your first aim is to ensure your “mysecret” file is not visible to other users on the same system. First view the permissions of your newly created file:

ls –l ~/mysecret

Example 13



Oh no! It’s not so secret…

The chmod command can be used to set permissions on a file. chmod can set permissions based on absolute octal values, or relative changes. So for example, you could use chmod to set permissions on a file based on octet: 770 would give the owner and group rwx, and others no permissions Example:

chmod 770 /home/tmp/somefile

### Example 14



Thus, the permissions are changed from 644 (rw-) to 770 (rwxrwx---) for /home/tmp/somefile when using sudo command. Or you can make relative changes: u-x would remove the owner (user) the ability to execute the file. Example:

chmod u-x /home/tmp/somefile

### Example 15



Likewise, o+w would add other’s ability to write to the file

Example:

chmod o+w /home/tmp/somefile

### Example 16



Use chmod to give read-write permissions to yourself to your mysecrets file and everyone else no permissions to the file:

chmod 660 ~/mysecrets

### Example 17



Try accessing the file on behalf of the user student:

cat /home/alex/mysecrets

### Example 18



Create a file “~/myshare”, and grant everyone read-write access. Test whether you have correctly set permissions. Also give other necessary permissions to other users for finding file “~/myshare”.

### Example 19



Create “mygroupshare”, grant only read access to everyone in your group. Test whether you have correctly set permissions.

### Example 20



Add user student to group alex by

sudo usermod –a –G alex student

### Example 21









Create a new group mygroup using

sudo groupadd mygroup

### Example 22



Change group of mygroupshare from alex to mygroup using

Sudo chown :mygroup ~/mygroupshare

To change owner and group of a file use

chown new\_owner:newgroup file

### Example 23



Change back mygroupshare group to alex and give alex group only read access to mygroupshare:

sudo chown :alex ~/mygroupshare

sudo chmod g-w ~/mygroupshare

### Example 24





Create a new group called “staff”, and create a file that you and a fellow classmate

(other user) can collaborate on (both edit). Test whether you have correctly set permissions. Both users should be able to edit the file, yet other users should not have write access.

### Example 25



### Challenge 1.

mkdir test

touch test/test1 test/test2 test/test3

Use a single chmod command to recursively set the permissions for all files contained in the new “test” directory.

Hint: “man chmod”

## Command umask

Remember that our newly created file started with permissions that meant that everyone could read the file. This can be avoided by setting the **u**ser file-creation mode **mask** (umask) . Every process has a umask: an octal that determines the permissions of newly created files. It works by removing permissions from the default “666” for files and “777” for new executables (based on a logical NOT). That is, a umask of “000” would result in new files with permissions “666”. A umask of “022” (which is the default value) gives “644”, that is “rw- -r- -r-”. The umask system call can be used to set the umask for the current process.

Check the current umask value:

umask

### Example 26



### Challenge 2.

Using the umask builtin command, set your umask so that new files are only rw

accessible by you (but not to your group or others):

umask XXX

where XXX is the new umask to use.

Test your new umask value by creating a new file and checking its permissions:

touch newfilename

ls -l newfilename

Do the permissions read “rw-------”? If not, change the umask and try again.

## Set UID (SUID)

Sometimes a user needs to be able to do things that require permissions that they should not always have. For example, the passwd command is used to change your password. It needs read and write access to /etc/shadow. Clearly not every user should have that kind of access! Also, the ping command needs raw network access... Again not something that every user can do. The Unix solution is set UID (SUID). Using SUID, processes can be given permission to run as another user. For example, when you run passwd, the program actually runs as root (on most Unix systems). In fact, every process actually has multiple identities, including:

● The real UID (RUID): the user who is running the command

● The effective UID (EUID): the way the process is treated

Take a look at how the effective UID is specified:

ls -l /usr/bin/passwd

### Example 27



The “s” in the file permissions means that the file UID will be used as the effective UID. Run

stat /usr/bin/passwd

Then switch to another user (bob) and run passwd

### Example 28



Digit 4 in the octet permissions 4755 means that the file will be executed with UID=root. Thus, the SUID bit is stored in the first (user) permission octet in the inode.

Viewing the processes running from another bash tab with

ps –af

### Example 29



we see that passwd runs with UID=root in spite of launched by bob.

Find all programs with SUID in /home/ by

sudo find /home –perm -4000 –type f –print

and check the findings using stat:

### Example 30



The program accessmysecrets is described below.

## Writing a SUID program in C

You are going to create a SUID program, to grant access to the contents of your

“mysecret” file to anyone who runs the program, without sharing direct access to the file.

Make sure “~/mysecrets” is only accessible by the owner: ls -la should show “rw-------”

for that file.

### Example 31



Create a C program by making a new file “accessmysecret.c”:

vi accessmysecret.c

Remember, vi is modal. Press “i” to enter insert mode, then enter this code:

#include <stdio.h>

#include <stdlib.h>

#include <sys/types.h>

#include <unistd.h>

#include <errno.h>

int main()

{

printf(" UID GID \n"

"Real %d Real %d \n"

"Effective %d Effective %d \n",

getuid (), getgid (),

geteuid(), getegid());

FILE \*fp = fopen("mysecrets", "r");

if (fp == NULL) {

printf("Error: Could not open file");

exit(EXIT\_FAILURE);

}

char c;

while ((c=getc(fp)) != EOF) {

putchar(c);

}

putchar('\n');

return EXIT\_SUCCESS;

}

### Example 32



Save your changes and quit (Esc, “:wq”). You may use any other text editor (e.g., editor):





Compile the program (which uses the C code to create an executable):

gcc accessmysecrets.c -o accessmysecrets

Set the permissions for the file (using chmod) to setuid:

chmod u+s accessmysecrets

Check the permissions include SUID:

ls -l accessmysecrets

### Example 33



Run the program:

./accessmysecrets

### Example 34



Note that the program outputs its real and effective identity.

Change to another user, and execute the program:

/home/yourusername/accessmysecrets

### Example 35



Note that the effective ID is that of the owner of the program. You should also see the

contents of the mysecrets file, even though you don’t have access to the secrets file

directly.

### Challenge 3

Switch to another user and use the SUID accessmysecrets program to

get read access to any one of the owner user’s files!

Hint: there is a security problem with this code.

Another hint: think about hard links.

**Solution:**

There is a security problem caused by not using an absolute filename when opening

the file, it opens “mysecrets” rather than “/home/user/mysecrets”. Remember, any

user can create a hard link to a file (therefore they can make a “copy” of the SUID

program wherever they like).

Make a hard link to the SUID program in a directory that the attacker can write to,

then also make a hard link to any file the SUID user owns, and name it “mysecrets” in

the same directory as the program, then when you execute the program it will write

out the contents of the file.

You can exploit this vulnerability as follows:

su - student

ln /home/user/accessmysecrets /tmp/access

ln /home/user/someotherfile /tmp/mysecrets

/tmp/access

### Challenge 4

Modify the program to correct the above vulnerability.

### Challenge 5

 Modify the program so that only the first line of the mysecrets file is

displayed to others.

### Challenge 6

 Modify the program so that the script checks the UID and only continues

for a specific user (for example, if the user is root).

Hint: “man getuid

## Linux Extended ACLs

We have explored standard Unix permissions. Modern Linux systems (and some other Unix-based systems) now have more complete (and complicated) ACL support. As previously mentioned, an access control list (ACL) is attached to an object (resource) and lists all the subjects (users / active entities) that are allowed access, along with the kind of access that is authorised.

Set a file ACL on your mysecrets file, using the setfacl command:

setfacl -m u:student:r ~/mysecrets

### Example 36



This grants the “student” user read access to the file.

Note that the stat program is not usually ACL aware, so won’t report anything out of

the usual:

stat ~/mysecrets

The ls program can be used to detect File ACLs:

ls -la ~/mysecrets

-rw-r-----+ 1 cliffe users 22 Feb 28 11:47 mysecrets

Note that the output includes a “+”. This indicates an ACL is in place.

Use getfacl to display the permissions:

getfacl ~/mysecrets

Use Linux File ACLs to grant one or more specific users (other class members) read access to your mysecrets file.

Using ACLs, grant any other group (you choose) read-write access to your mygroupshare file.

Remove the group permission you just added.

Example: setfacl -x g:staff file

## Conclusion

At this point you have:

1. Learned about file permissions, hard links, and inodes
2. Learned about octal representations of permissions
3. Changed Unix file permissions to grant access to specific users and groups, using chmod
4. Used umask to change the permissions applied to new files
5. Learned about Set UID (SUID), become more familiar with C, and compiled a SUID C program
6. You may have also done some more programming of your own
7. Used Linux Extended ACLs to configure more advanced security policies

Well done!

## References

1. Z. Cliffe Schreuders. Access controls and Linux/Unix file permissions, URL: z.cliffe.schreuders.org/edu/ADS/Access%20Controls.pdf