# *CYBR371: ASSIGNMENT 1*

File System Access Control (ACL)

*Grace Forsyth*

*forsytgrac | 300529611*

Task 1.

| | WellingtonClinic | staff | scripts | patients |
|---|---|---|---|---|
| owner | administrators | administrators | administrators | administrators |
| administrators | rwx | rwx | rwx | rwx |
| Registered doctors | r-x | r-x | r-x | r-x |
| Unregistered doctors | r-x | r-x | r-x | r-x |
| nurses | r-x | r-x | r-x | r-x |
| receptionists | r-x | r-x | r-x | rwx |

Administrators:
Administrator is a root user. They create the directories by running file-system-setup.sh. They have rwx permissions on every file in the system including the staff info, scripts and patient info. To have those permissions on each file they would subsequently need rwx permissions on every directory.

Doctors:
Doctors can read staffs sbasicinfo.log therefore they need r-x permissions on the staff directory and the WellingtonClinic directory since they need to access directories and files inside.
Doctors need to read check-medication.sh and run visit.sh so they need r-x permissions on the scripts directory to access the scripts inside it.
Doctors need to read a patient's pbasicinfo.log and need to read and write to a patient's pmedicalrecord.log so they must have r-x permissions on the "patients" directory to access their patient's details inside.

Unregistered Doctors:
Unregistered doctors are the same as doctors (they are in the same group). Unregistered doctors don't have permissions to some specific patients they are not registered to inside the "patients" directory.
Nurses:

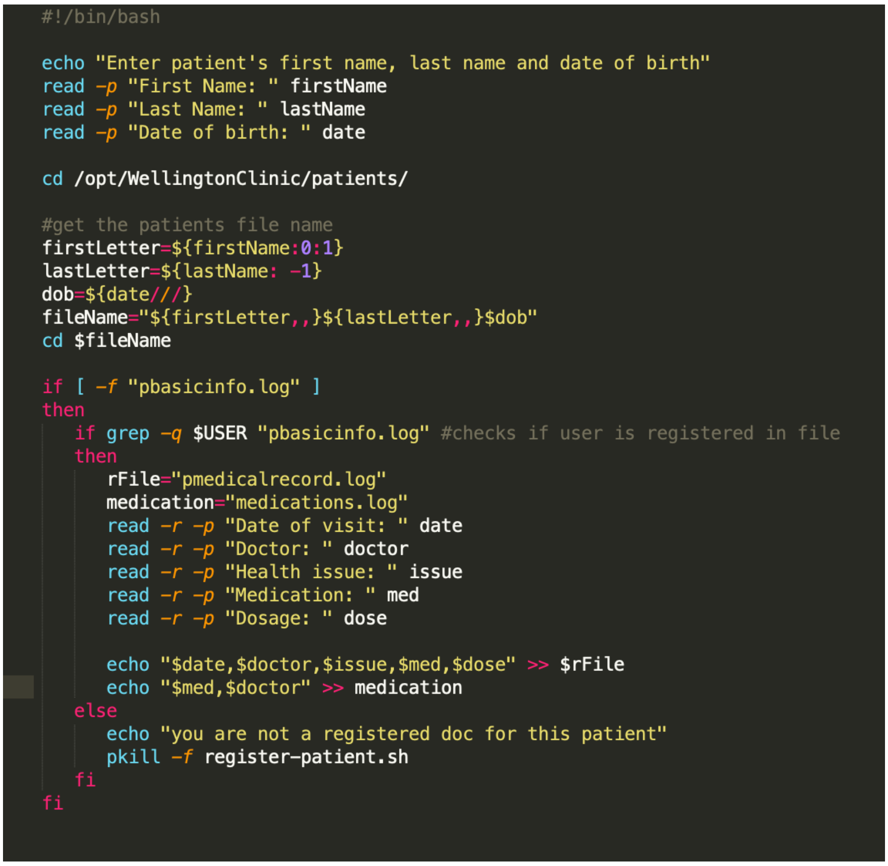
Nurses need r-x permissions on the WellingtonClinic directory because they need to access some directories and scripts inside of it.
Nurses can read staffs sbasicinfo.log files therefore they need r-x permissions on the staff directory.
Nurses need to run the check-medication.sh script to check a patient's information and can read a patient's basic info, therefore they need r-x access to the scripts directory and r-x access to the "patients" directory.

Receptionists:
Receptionists need r-x permissions on the WellingtonClinic directory because they need to access directories and scripts inside of it.
Receptionists can read staffs sbasicinfo.log therefore they need r-x permissions on the staff directory.
Receptionists need to execute several scripts inside of the scripts directory, so they need r-x permissions on the scripts directory.
Receptionists run the register-patient.sh script to create a patient's directory inside of the "patients" directory and can see the patient's info, so receptionists need rwx permissions on the "patients" directory.

Task 4.
(5 Marks) Explain in detail where the ACL information of an object is saved on a Linux system (EXT2, 3 and 4 file systems) and how your system keeps track of them.

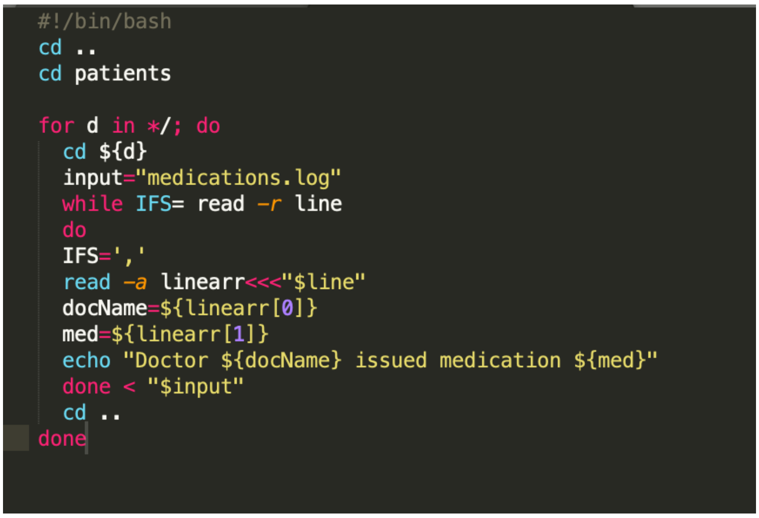
The file system in Linux saves ACLs on inodes which contain data that relate to files/folders. ACLs are small, comprised of bits of data that specifies read write and execute permission entries of a folder/file. On a typical Linux system, they are implemented as EAs (extended attributes) on an inode. Ext2 & 3 requires all EAs to fit on a single disk block if the EA (or permissions) are similar. If they are unique, the EAs can be put on different disk blocks.
On our system, the script file acls.sh assigns the ACL permissions for our files and folders. This confirms which users and groups are permitted to access the directories and files in the system. If a user tries to access a file/folder, the system can either permit or deny them access based on the permissions that will be stored in the inode of a file once the acls.sh file is executed.

Task 13.
Nurses only need to see the patient's past and current medication and the doctor that prescribed them. However, nurses currently have read access to the patients whole medical record (pmedicalrecord.log) because they use check-medication.sh which reads it.
A solution to this would be to store a patient's medications and the doctor that prescribed them in a separate file in the patient's directory called medications.log.
Therefore, when the nurses run check-medication.sh the script would read the medications.log file instead of the whole pmedicalrecord.log file
The doctor of a patient would need to run visit.sh to set up the medications.log at the same time as they update the pdmedicalrecord.log.
The visit.sh script run by the doctor to document the patient's medical information would be as follows:



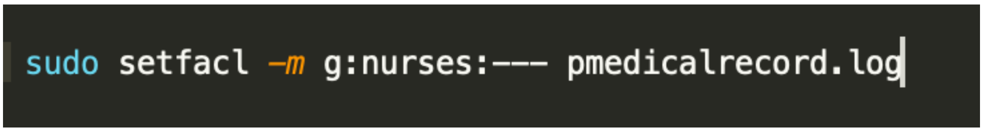
```
#!/bin/bash

echo "Enter patient's first name, last name and date of birth"
read -p "First Name: " firstName
read -p "Last Name: " lastName
read -p "Date of birth: " date

cd /opt/WellingtonClinic/patients/

#get the patients file name
firstLetter=${firstName:0:1}
lastLetter=${lastName: -1}
dob=${date///}
fileName="${firstLetter,,}${lastLetter,,}$dob"
cd $fileName

if [ -f "pbasicinfo.log" ]
then
   if grep -q $USER "pbasicinfo.log" #checks if user is registered in file
   then
      rFile="pmedicalrecord.log"
      medication="medications.log"
      read -r -p "Date of visit: " date
      read -r -p "Doctor: " doctor
      read -r -p "Health issue: " issue
      read -r -p "Medication: " med
      read -r -p "Dosage: " dose

      echo "$date,$doctor,$issue,$med,$dose" >> $rFile
      echo "$med,$doctor" >> medication
   else
      echo "you are not a registered doc for this patient"
      pkill -f register-patient.sh
   fi
fi
```

The check-medication.sh script run by a nurse would now only need to read the medications.log file instead of pmedicalrecord.log.
The check-medication.sh script to check the patient’s medication information would then be as follows:



```
#!/bin/bash
cd ..
cd patients

for d in */; do
  cd ${d}
  input="medications.log"
  while IFS= read -r line
  do
  IFS=','
  read -a linearr<<<"$line"
  docName=${linearr[0]}
  med=${linearr[1]}
  echo "Doctor ${docName} issued medication ${med}"
  done < "$input"
  cd ..
done
```

Consequently, nurses would no longer need read access to a patient’s whole pmedicalrecord.log so we can remove their access by running:



```
sudo setfacl -m g:nurses:--- pmedicalrecord.log
```