FIT2093 - Introduction to Cyber Security
Assignment 2 - User Authentication and Access Control

Prof. Ron Steinfeld

Lim Zheng Haur (32023952)

3rd May 2023

OPTION 2 chosen for Task 1a

Task 1: Two-Factor Authentication System

Task 1a: Biometric Authentication (OPTION 2)

Registered Person ('Alice') Testing Image ID	Similarity Probability Score	Closest Matching Registered User Name
1	0.996	Alice
2	0.997	Alice
3	0.984	Candice
4	0.977	Delta
5	0.996	Alice
6	0.999	Alice
7	0.982	Eve
8	0.986	Alice
9	0.990	Alice
10	0.995	Alice

Table 1. Results for Registered Person ('Alice') Testing Images

Un-Registered Person ('Charlotte') Testing Image ID	Similarity Probability Score	Closest Matching Registered User Name
1	0.952	Alice
2	0.937	Candice
3	0.931	Eve
4	0.918	April
5	0.915	June
6	0.937	Sara
7	0.926	Delta
8	0.909	Bella

9	0.982	Samantha
10	0.943	Samantha

Table 2. Results for Unregistered Person ('Charlotte') Testing Images

Based on the results in Table 1 and Table 2, the FAR and FRR metrics is computed using the threshold of:

1. 0.95

   Table 1:
   - False Accept/Positive (FP): 3
   - True Reject/Negative (TN): 0
   - True Accept/Positive (TP): 7
   - False Reject/Negative (FN): 0

   Table 2:
   - False Accept/Positive (FP): 2
   - True Reject/Negative (TN): 8
   - True Accept/Positive (TP): 0
   - False Reject/Negative (FN): 0

   False Acceptance Rate (FAR) = (3+2)/(10+10)
   = 5/20
   = 25%

   False Rejection Rate (FRR) = (0+0)/(10+10)
   = 0/20
   = 0%

2. 0.98

   Table 1:
   - False Accept/Positive (FP): 2
   - True Reject/Negative (TN): 1
   - True Accept/Positive (TP): 7
   - False Reject/Negative (FN): 0

   Table 2:
   - False Accept/Positive (FP): 1
   - True Reject/Negative (TN): 9
   - True Accept/Positive (TP): 0

- False Reject/Negative (FN): 0

False Acceptance Rate (FAR) = (2+1)/(10+10)
= 3/20
= 15%

False Rejection Rate (FRR) = (0+0)/(10+10)
= 0/20
= 0%

Calculations of FAR and FRR with two different threshold settings of 0.95 and 0.98.

The False Acceptance Rate (FAR) is a metric used to determine the number of false accept/positive that exist. The formula for FAR is the number of false accept/positive divided by the total number of tests. On the other hand, the False Rejection Rate (FRR) is a metric used to determine the number of false rejects/negatives that exist. The formula for FRR is the number of false rejects/negatives divided by the total number of tests. To determine whether a test is falsely accepted or not, we would use two different threshold settings of 0.95 and 0.98 where if the Similarity Probability Score is higher than the threshold, then we would determine if the test is accepted whereas if it is lower, it would be rejected. Then we would identify if the test accepted or rejected is True or False to compute the number of True Positives, True Negatives, False Positives and False Negatives. Finally, using the findings we have obtained so far, we could calculate the FAR and FRR for both threshold settings. These results are 25% for the FAR with threshold of 0.95, 15% for the FAR with threshold of 0.98 and 0% for the FRR with both thresholds.

Impacts of the choice of threshold on the <u>security</u> and <u>usability</u> of the authentication system.

The choice of threshold possesses a strong significance to an authentication system. This is because there exists strong impacts of the choice of threshold to the security and usability of the authentication system. Authentication systems should not allow unauthorised users to enter the system. This implies that authentication systems should have a low false acceptance rate (FAR) which means a low rate of unauthorised users gaining access to a system to provide a stronger security assurance. Reflecting on the calculations of FAR above, a higher threshold will decrease the FAR which decreased from 25% to 15% when the threshold setting increased from 0.95 to 0.98. Hence, we are able to conclude that a higher threshold will produce a more secure security for the authentication system as it decreases the FAR.

On the other hand, while an authentication system's goal is to provide security to systems, usability of the authentication system is also an important consideration. Authentication systems should not reject authorised users frequently as this would decrease the usability of

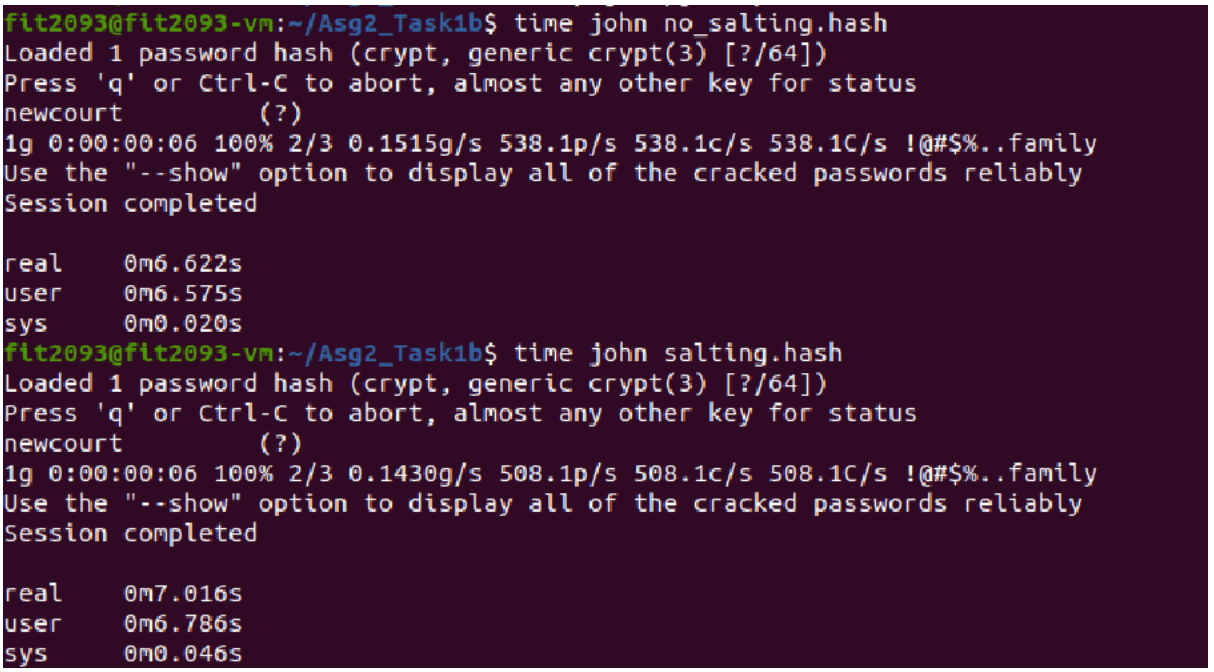
the system since users are not able to access the system easily. Therefore, authentication should have a lower false rejection rate (FRR) which means a low rate of authorised users being rejected from gaining access to a system to provide a better usability. According to the calculations of the FRR from the tables above, a higher threshold will not affect the FRR of the authentication system. However, theoretically the FRR should increase as we increase the threshold as there might be true acceptances below the threshold. This is most likely due to the lack of test cases from our test above. Thus, although the higher the threshold, the worse the usability as the FRR should increase, the results above do not prove this appropriately and instead show no difference in the FRR.

In conclusion, the choice of threshold should be considered with great significance as it is strongly responsible for the security and usability of the system. The best threshold setting is the one where the FAR and the FRR is the lowest as FAR is inversely associated with the security of the system while FRR is inversely associated with the usability of the authentication system.

Task 1b: Password Authentication

1. Time taken to find the password by a search:

    a. No salt with default no. of rounds (5000): 0m 6.622s
    b. With salt with default no. of rounds (5000): 0m 6.786s
    c. WIth salt with 1000 rounds (minimum): 0m 1.329s
    d. WIth salt with 50000 rounds: 1m 6.801s



```
fit2093@fit2093-vm:~/Asg2_Task1b$ time john salt_1000.hash
Loaded 1 password hash (crypt, generic crypt(3) [?/64])
Press 'q' or Ctrl-C to abort, almost any other key for status
newcourt         (?)
1g 0:00:00:01 100% 2/3 0.7462g/s 2650p/s 2650c/s 2650C/s !@#$%..family
Use the "--show" option to display all of the cracked passwords reliably
Session completed

real    0m1.372s
user    0m1.329s
sys     0m0.018s
fit2093@fit2093-vm:~/Asg2_Task1b$ time john salt_50000.hash
Loaded 1 password hash (crypt, generic crypt(3) [?/64])
Press 'q' or Ctrl-C to abort, almost any other key for status
newcourt         (?)
1g 0:00:01:06 100% 2/3 0.01494g/s 53.09p/s 53.09c/s 53.09C/s !@#$%..family
Use the "--show" option to display all of the cracked passwords reliably
Session completed

real    1m6.966s
user    1m6.801s
sys     0m0.065s
```

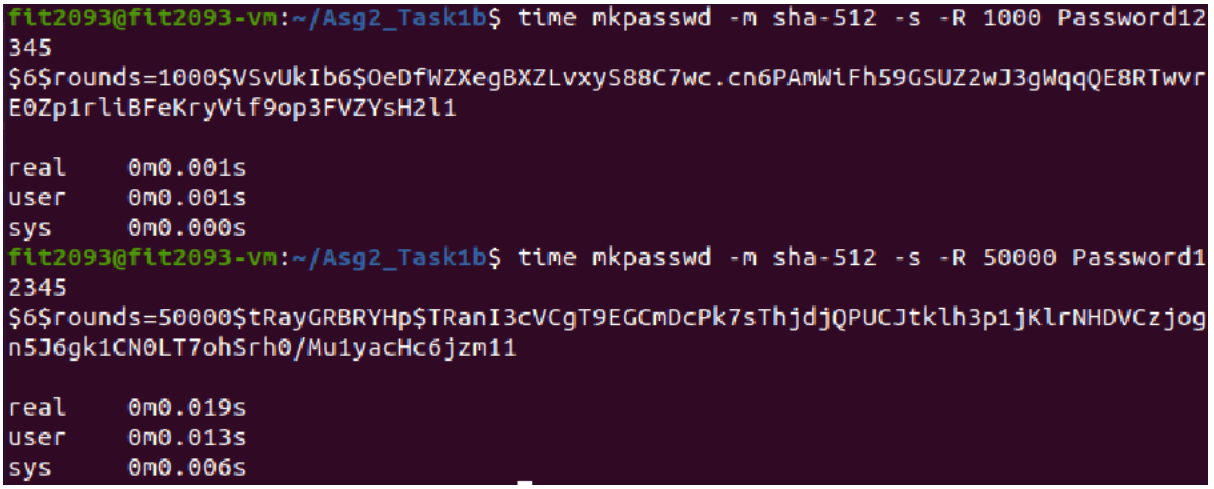
2. Time taken to hash a single password 'Password12345':

   a. No salt with default no. of rounds (5000): 0m 0.003s
   b. With salt with default no. of rounds (5000): 0m 0.003s
   c. WIth salt with preferred no. of rounds (1000): 0m 0.001s
   d. WIth salt with higher no. of rounds (50000): 0m 0.013s

```
fit2093@fit2093-vm:~/Asg2_Task1b$ time mkpasswd -m sha-512 Password12345
$6$3i1Ojkk2cR$H9fuNAom2P.V3Eu67Hp2i2yyDBsqNfLCkWCyL0LNPuTATv6H8bpbBv1GLDsQBMrAaB
n6CdY5bSlfn8RTanfif0

real    0m0.003s
user    0m0.003s
sys     0m0.000s
fit2093@fit2093-vm:~/Asg2_Task1b$ time mkpasswd -m sha-512 -s Password12345
$6$G9ReqMqNQYyRAJB$E3aV3rB6ZXhfxdaQbnTd20r2iGqRqNiwWBrwbgV6mE4Wut86gjoAFoe5sL/9J
AmOsYNAAqCsb.0hx6P8Ot8RZ0

real    0m0.003s
user    0m0.003s
sys     0m0.000s
```



Results of finding password and 'system' time taken to compute a single hash.

I have used John the Ripper tool to find the password of the four hashed passwords using the built in dictionary of John the Ripper. While doing this, I have recorded the time taken to successfully find the password of all four of these differently hashed passwords. The time taken to find the password hashed without salt and the default number of rounds which is 5000 rounds is 6.622 seconds. The time taken for the password hashed with salt and the same default number of rounds is slightly higher at 6.786 seconds. By using the minimum number of rounds which is 1000 rounds to hash the password with salt instead, we could observe that the recorded time taken to find the password is significantly shorter at 1.329 seconds. Lastly, when we increase the number of rounds to a higher value at 50000 rounds, we could see that finding the password will take a significantly longer amount of time at 1 minute 6.801 seconds.

I have also attempted to hash a single password using four different methods same as above and recorded the time taken to complete these hashes. The password that I have chosen for this test is 'Password12345'. The amount of time required to hash the password without salt and the default number of rounds which is 5000 rounds is 0.003 seconds. While using salt instead and retaining the same number of rounds, the time taken to hash the password is still 0.003 seconds as well. If we reduce the number of rounds to the minimum at 1000 rounds and hash the password with salt, we could observe that the time taken reduces to 0.001 seconds. Finally, if we increase the number of rounds significantly to 50000 and still hash the password with salt, the time taken also increases significantly to 0.013 seconds. Although 0.013 seconds might seem short, it is almost 5 times longer than the time taken to hash a password with 5000 rounds and 13 times longer than the time taken to hash a password with 1000 rounds.

Discussion and comparison of the differences among all 4 approaches.

From the observations of time taken to find a password and to compute a single hash, we could observe that using salt or not does not significantly affect the time taken. From the results, the time taken to find the password with no salt and with salt is 6.622 and 6.786 seconds respectively. This shows that salting our hash will make it slightly harder for attackers to find the password by a search. On the other hand, the time taken to compute the single hash is both 0.003 seconds. While we manipulate the number of rounds for each hash we could see that the time taken to find the password for 1000, 5000 and 50000 rounds are 1.329 seconds, 6.786 seconds and 1 minute 6.801 seconds. In addition, the time taken for computing the hash with 1000, 5000 and 50000 rounds are 0.001, 0.003 and 0.013 seconds. From this observation and the previous one comparing the difference between the presence of salting, we could conclude that salting does not significantly affect the time taken to find passwords by a search and compute a single hash but on the other hand, manipulating the number of rounds will significantly affect the time taken. In conclusion, the higher the number of rounds, the longer the time taken to compute a single hash and to find a hashed password by search.

Recommendation of which approach should be used for password hashing and reasoning based on usability and security considerations.

The time taken for the system to compute a single hash is similar to the time for a server to verify a single password login verification. Based on our observations above, when we increase the number of rounds to hash, the time taken for the system to verify a single password login verification would also increase. Salting on the other hand does not affect much of the time taken to verify a single password login but increases the time taken to brute force a password by search. Hence, my recommendation on the approach that should be used for password hashing is that systems that require higher security should implement more rounds in their password hashing while systems that require lesser security should use a moderate number of rounds for their password hashing. Both of these options should be used in conjunction with salting which does not affect much of the time taken for the system to verify a single password login verification but increases the difficulty to brute force to find a password by search.

Task 2: Access Control

Task 2a: Users and groups

Peter was unable to access the folder ‘hr’ to edit ‘hr.txt’ as he does not belong to the group ‘hr’. Although Peter has access to the folder ‘it’, Peter is still unable to modify the file ‘it.txt’ created by Mary. This is because the file created by Mary has the permission of ‘rw-r--r--’ by default. This implies that users from the same group are only able to read, but not write or execute the file created by Mary.

Task 2b: Permissions for files

The file ‘secret.txt’ has an original permission of ‘r--------’. This means that only the owner of the file is allowed to read it. To allow Peter and Mary to read the file ‘secret.txt’, I have changed the permission setting using the command ‘chmod 407 secret.txt’ to allow users from other groups to read, write and execute the file. After changing permission, it is possible for Mary and Peter to run the program ‘readsecret’ and read the file ‘secret.txt’.

Task 2c: Permission for folders

Peter is unable to read the file as the folder ‘employee’ was set to ‘rwxrwx-wx’. This means that users from other groups are unable to read the folder ‘employee’. To allow Peter to modify the file ‘readonly.txt’, I copied the file out from the ‘employee’ folder into ‘it’ folder, and since Peter is the owner of the new file, he could modify the contents.

Appendix

Task 2a: Users and groups.

Creating user ‘Peter’

```
fit2093@fit2093-vm:~$ sudo adduser --ingroup sudo peter
[sudo] password for fit2093:
Sorry, try again.
[sudo] password for fit2093:
Adding user `peter' ...
Adding new user `peter' (1001) with group `sudo' ...
Creating home directory `/home/peter' ...
Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for peter
Enter the new value, or press ENTER for the default
        Full Name []: Peter
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] Y
```

Creating user 'Mary'.

```
fit2093@fit2093-vm:~$ sudo adduser --ingroup sudo mary
Adding user `mary' ...
Adding new user `mary' (1002) with group `sudo' ...
Creating home directory `/home/mary' ...
Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for mary
Enter the new value, or press ENTER for the default
        Full Name []: Mary
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] Y
```

Adding user 'Peter' into group 'it' and user 'Mary' into group 'hr' and 'it'.

```
fit2093@fit2093-vm:~$ sudo adduser peter it
[sudo] password for fit2093:
Adding user `peter' to group `it' ...
Adding user peter to group it
Done.
fit2093@fit2093-vm:~$ sudo adduser mary hr
Adding user `mary' to group `hr' ...
Adding user mary to group hr
Done.
fit2093@fit2093-vm:~$ sudo adduser mary it
Adding user `mary' to group `it' ...
Adding user mary to group it
Done.
```

Showing the contents of the file /etc/group.

```
fit2093@fit2093-vm:~$ cat /etc/group
root:x:0:
daemon:x:1:
bin:x:2:
sys:x:3:
adm:x:4:syslog,fit2093
tty:x:5:syslog
disk:x:6:
lp:x:7:
mail:x:8:
news:x:9:
uucp:x:10:
man:x:12:
proxy:x:13:
kmem:x:15:
dialout:x:20:
fax:x:21:
voice:x:22:
cdrom:x:24:fit2093
floppy:x:25:
tape:x:26:
sudo:x:27:fit2093
audio:x:29:pulse
dip:x:30:fit2093
www-data:x:33:
backup:x:34:
operator:x:37:
list:x:38:
```

```
irc:x:39:
src:x:40:
gnats:x:41:
shadow:x:42:
utmp:x:43:
video:x:44:
sasl:x:45:
plugdev:x:46:fit2093
staff:x:50:
games:x:60:
users:x:100:
nogroup:x:65534:
systemd-journal:x:101:
systemd-network:x:102:
systemd-resolve:x:103:
systemd-timesync:x:104:
crontab:x:105:
messagebus:x:106:
input:x:107:
kvm:x:108:
render:x:109:
syslog:x:110:
tss:x:111:
bluetooth:x:112:
ssl-cert:x:113:
uuidd:x:114:
tcpdump:x:115:
```

```
avahi-autoipd:x:116:
rtkit:x:117:
ssh:x:118:
netdev:x:119:
lpadmin:x:120:fit2093
avahi:x:121:
scanner:x:122:saned
saned:x:123:
nm-openvpn:x:124:
whoopsie:x:125:
colord:x:126:
geoclue:x:127:
pulse:x:128:
pulse-access:x:129:
gdm:x:130:
sssd:x:131:
lxd:x:132:fit2093
fit2093:x:1000:
sambashare:x:133:fit2093
systemd-coredump:x:999:
vboxsf:x:998:
mysql:x:134:
docker:x:997:
hr:x:1001:mary
it:x:1002:peter,mary
```

Switch user to 'Mary'

```
fit2093@fit2093-vm:~$ su mary
Password:
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.
```

Modifying the file 'hr.txt' using nano text editor.

```
mary@fit2093-vm:/home$ ls
fit2093  mary  peter  share-folder
mary@fit2093-vm:/home$ cd share-folder
mary@fit2093-vm:/home/share-folder$ ls
common  employee  hr  it
mary@fit2093-vm:/home/share-folder$ cd hr
mary@fit2093-vm:/home/share-folder/hr$ ls
hr.txt
mary@fit2093-vm:/home/share-folder/hr$ nano hr.txt
mary@fit2093-vm:/home/share-folder/hr$ cat hr.txt
This is an hr file.
modified by mary.
```

Creating the file 'it.txt' using nano text editor.

```
mary@fit2093-vm:/home/share-folder/hr$ cd ..
mary@fit2093-vm:/home/share-folder$ cd it
mary@fit2093-vm:/home/share-folder/it$ nano it.txt
mary@fit2093-vm:/home/share-folder/it$ ls -l
total 4
-rw-r--r-- 1 mary sudo 16 May  8 15:27 it.txt
```

Switch user to 'Peter’.

```
mary@fit2093-vm:/home/share-folder/it$ su peter
Password:
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.
```

Unable to access folder, Permission denied

```
peter@fit2093-vm:/home/share-folder/it$ cd ..
peter@fit2093-vm:/home/share-folder$ ls
common  employee  hr  it
peter@fit2093-vm:/home/share-folder$ cd hr
bash: cd: hr: Permission denied
```

Unable to edit file, File 'it.txt' is unwritable

```
peter@fit2093-vm:/home/share-folder$ cd it
peter@fit2093-vm:/home/share-folder/it$ ls
it.txt
peter@fit2093-vm:/home/share-folder/it$ nano it.txt
peter@fit2093-vm:/home/share-folder/it$ ls -l
total 4
-rw-r--r-- 1 mary sudo 16 May  8 15:27 it.txt
```

Nano editor showing that the file ‘it.txt’ is unwritable.

```
                [ File 'it.txt' is unwritable ]
^G Get Help  ^O Write Out ^W Where Is  ^K Cut Text  ^J Justify   ^C Cur Pos
^X Exit      ^R Read File ^\ Replace   ^U Paste Text^T To Spell  ^_ Go To Line
```

Task 2b: Permissions settings for files

Switch user to 'Peter' and 'Mary' to attempt to run the program 'readsecret'.

```
fit2093@fit2093-vm:/home/share-folder/common$ ls -l
total 28
-rwxr-xr-x 1 fit2093 fit2093 17008 Mar 22 22:17 readsecret
-rwxr-xr-x 1 root    fit2093   480 Mar 22 21:58 readsecret.c
-r-------- 1 fit2093 fit2093    31 Mar 22 21:23 secret.txt
fit2093@fit2093-vm:/home/share-folder/common$ su peter
Password:
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

peter@fit2093-vm:/home/share-folder/common$ ls -l
total 28
-rwxr-xr-x 1 fit2093 fit2093 17008 Mar 22 22:17 readsecret
-rwxr-xr-x 1 root    fit2093   480 Mar 22 21:58 readsecret.c
-r-------- 1 fit2093 fit2093    31 Mar 22 21:23 secret.txt
peter@fit2093-vm:/home/share-folder/common$ ./readsecret
Program started - run by user 1001 with effective uid 1001
Error: file cannot be opened
peter@fit2093-vm:/home/share-folder/common$ su mary
Password:
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.
```

Changing permission to enable other groups to read, write and execute 'secret.txt'

```
mary@fit2093-vm:/home/share-folder/common$ ./readsecret
Program started - run by user 1002 with effective uid 1002
Error: file cannot be opened
mary@fit2093-vm:/home/share-folder/common$ su fit2093
Password:
fit2093@fit2093-vm:/home/share-folder/common$ chmod 407 secret.txt
fit2093@fit2093-vm:/home/share-folder/common$ ls -l
total 28
-rwxr-xr-x 1 fit2093 fit2093 17008 Mar 22 22:17 readsecret
-rwxr-xr-x 1 root    fit2093   480 Mar 22 21:58 readsecret.c
-r-----rwx 1 fit2093 fit2093    31 Mar 22 21:23 secret.txt
fit2093@fit2093-vm:/home/share-folder/common$ su peter
Password:
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

peter@fit2093-vm:/home/share-folder/common$ ./readsecret
Program started - run by user 1001 with effective uid 1001
Ha! You know my secret now....
peter@fit2093-vm:/home/share-folder/common$ su mary
Password:
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.
```

```
mary@fit2093-vm:/home/share-folder/common$ ./readsecret
Program started - run by user 1002 with effective uid 1002
Ha! You know my secret now....
```

Task 2c: Permission settings for folders

Switch user to 'Peter' to copy the file from 'employee' folder to 'it' folder and edit using nano text editor.