MP4 Report

First Part Design ideas:

Basically, there are six functions in this MP

- First three functions, *mp4_cred_prepare, mp4_cred_free*, *mp4_cred_alloc_blank* allocate memory for the security blob.
- *mp4_bprm_set_creds* initialize the blob for a particular binary file when it is launched.
- Mp4_inode_init_security set the external attributes for a newly created inode. If the inode is created by a target process the external attribute is set as read-write otherwise we do not set anything for it. In function get_inode_sid, the empty external attribute is considered as MP4_NO_ACCESS 0.
- mp4_inode_permission judge whether current process has permission to access a particular inode. osid & ssid are obtained and passed into mp4_has_permission which is the core of mandatory access control policy.

Second Part Test Policy

Test Case 1: *MP4_NO_ACCESS 0 & MP4_READ_OBJ 7*

```
setfattr -n security.mp4 -v target /bin/cat
setfattr -n security.mp4 -v dir /home
setfattr -n security.mp4 -v dir /home/yuguang2
setfattr -n security.mp4 -v read-only /home/yuguang2/file.txt
```

Basically, just label cat as target and file.txt as read-only

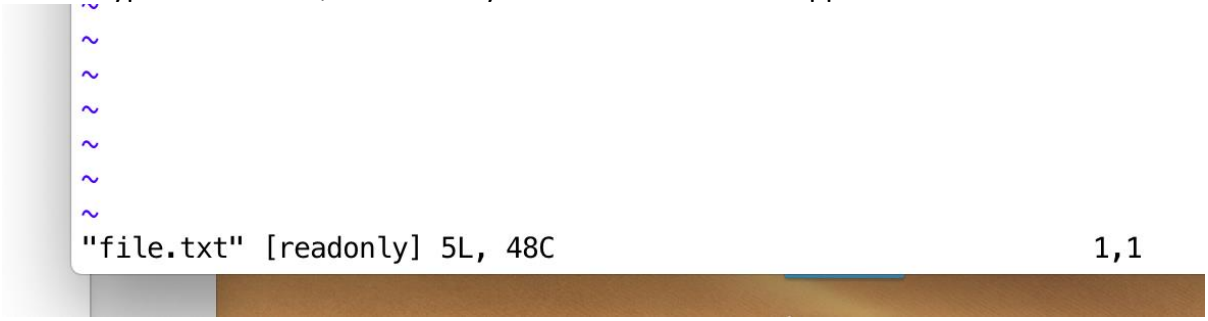
```
root@sp19-cs423-061:/home/yuguang2# getfattr -d -m - /bin/cat
getfattr: Removing leading '/' from absolute path names
# file: bin/cat
security.mp4="target"
```

```
root@sp19-cs423-061:/home/yuguang2# getfattr -d -m - file.txt
# file: file.txt
security.mp4="read-only"
```

If let cat access a default file without any label, the policy would not the cat access to that file.

```
root@sp19-cs423-061:/home/yuguang2# cat fil2
cat: fil2: Permission denied
root@sp19-cs423-061:/home/yuguang2#
```

And if I type 'vim file.txt', its read-only file without write and append.



Test case 2: MP4_READ_WRITE 2 & MP4_RW_DIR 6

```
#test object attr MP4_READ_WRITE

setfattr -n security.mp4 -v target /usr/bin/vim
setfattr -n security.mp4 -v dir-write /home
setfattr -n security.mp4 -v dir-write /home/yuguang2
setfattr -n security.mp4 -v read-write  /home/yuguang2/file.txt
```

```
root@sp19-cs423-061:/home/yuguang2# getfattr -d -m - file.txt
# file: file.txt
security.mp4="read-write"

root@sp19-cs423-061:/home/yuguang2# getfattr -d -m - /usr/bin/vim
getfattr: Removing leading '/' from absolute path names
# file: usr/bin/vim
security.mp4="target"
```

In this case, file.txt can only be modified by target file.

If type echo "cs423_mp4" >>file.txt, the access is denied as followings

```
43800.666912] cs423_mp4: permission Denied ssid :0, osid 2 mask :10
```

Test case 3: MP4_WRITE_OBJ 3

```
#test object attr MP4_WRITE_OBJ

setfattr -n security.mp4 -v target /usr/bin/vim
setfattr -n security.mp4 -v dir /home
setfattr -n security.mp4 -v dir /home/yuguang2
setfattr -n security.mp4 -v write-only  /home/yuguang2/file.txt
```

After source the ***test.perm:***

```
root@sp19-cs423-061:/home/yuguang2# getfattr -d -m - file.txt
# file: file.txt
security.mp4="write-only"

root@sp19-cs423-061:/home/yuguang2# getfattr -d -m - /usr/bin/vim
getfattr: Removing leading '/' from absolute path names
# file: usr/bin/vim
security.mp4="target"
```

3.1Type "vim file.txt"

```
~
~
~
~
~
~
~
"file.txt" [Permission Denied]
```

dmesg:

```
[82722.351489] cs423_mp4: permission_Denied ssid: 7 , osid : 3 mask : 4
```

It can seen that the label file is only write by the vim but not read (mask=4)

3.2 Type echo "cs423_mp4" >> file.txt

The permission is denied and check the dmesg has followings, echo is no target binary file and file.txt is write-only by target, so the access is denied.

```
[84260.782059] cs423_mp4: permission_Denied ssid :0, osid 3 mask :10
```

3.3 Type cat file.txt

It can be read by non-targeted process correctly

4. Test Case 4 MP4_EXEC_OBJ 4

```
setfattr -n security.mp4 -v dir /home
setfattr -n security.mp4 -v dir /home/yuguang2
setfattr -n security.mp4 -v exec  /home/yuguang2/file.txt
```

```
root@sp19-cs423-061:/home/yuguang2# getfattr -d -m - file.txt
# file: file.txt
security.mp4="exec"
```

4.1 type vim file.txt

It only return read-only file without write and write permission was rejected as:

```
[ 9875.072005] cs423_mp4: permission_Denied ssid :0, osid 4 mask :2
```

Third Part Least Privilege Policy

there is user tobias which can be used to test

After source passwd.perm just do *passwd tobias*

Grant least privilege for each file which is required in passwd. Bascially , I use strace to see which files are open in this process and grant them the least access privilege to each file and dir.
It is mentioned that most directory is grant as “dir” only /etc is granted as “dir-write” other wise it will result permission denied.
Details about the policy is shown in passwd.perm.