Computer Security and Privacy (COM-301)

Discretionary Access Control

Interactive exercise solving

Least Privilege and Access control

Answer template on the next slide

Access control policies should be implemented in such a way that subjects are never “overprivileged”. In other words, subjects should have the minimal access to an object in order to perform a task.

Imagine a simple permission system where one can have the following permissions:

r: read the content of an object

w: write to an object

x: execute an object

Imagine the system has two directories submission and grading.

How would you assign permissions from principals to objects implementing least privilege to:

1- Students that need to submit their report to the directory submission

2 - TAs that need to grade reports and write the result on a file grades in directory grading

3 – Professor that needs to execute a script averaging in folder grading that uses the results in the file grades in directory grading

Least Privilege and Access control

Your solution should be of the form

Principal	Object	Permission
Student		
TA		
Professor		

Think adversarially to decide on least principles.

Remember there is not only one correct solution, it depends on your threat model.

Building a messenger

Alice and Bob want to build a messenger. When Bob wants to send a message to Alice, he will run the executable `msg`, which will write to `msgfile`. Alice can later read the messages from `msgfile`.

Consider these two propositions:

```
                -rwx--x---  Alice Alice+Bob msg
(1)             -rwx------  Alice Alice+Bob msgfile

                -rwx--x---  Alice Alice+Bob msg
(2)             -rwx-w----  Alice Alice+Bob msgfile
```

What is wrong with each proposition?

Propose a solution.