Computer Security and Privacy (COM-301)

Discretionary Access Control

Interactive exercise solving

youAllGetASix

In order to make assignment grading easier, the COM-301 TAs have set up a grading portal at `https://youAllGetASix.com`. Students submit their assignments in PDF format via this portal.

Upon receiving a file, the grading script on the server takes the assignment as input. It reads the SCIPER from the first page of the assignment, performs the grading, and stores a report and grade associated to that on the server. This grade report is later reviewed by the TAs.

Describe one attack a student could carry out against this system. Explain the vulnerability that enables this attack. What would you advise the COM-301 TAs to do to prevent the attack

ACL vs Capabilities

Because of COVID-19, EPFL has decided to restrict access to the study rooms on campus: each student needs to book on the EPFL app a seat for the day in a study room to be able to get into the given room. Propose a high-level mechanism for access control of the study rooms. List subjects, objects, and rights.

Does your mechanism use the capability or access-control list model?

Name one advantage and one disadvantage of your proposal.

Least Privilege and Access control

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.