

Computer Security and Privacy (COM-301)

Week 3: Discretionary Access Control

Interactive Problem Solving

Confusion

Which of the following security incidents is **NOT** caused by a confused deputy?

- (a) A hacker gains access to a user's social network account by getting the user's browser to send the hacker this user's credential
- (b) A virus infects an email client to send spam
- (c) A journalist tricks a banker into revealing the bank statements of a famous singer
- (d) A detective leaks information to a criminal using a covert channel

ACL vs. Capabilities

We are back in COVID-19 times: 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.

Question: Propose a high-level mechanism to implement access control to 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.

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.

Question: 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