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

Correct answer is (D): The detective is no tricking any privileged process into doing something against the security policy

Note on the others:
(A) Browser is confused deputy
(B) E-mail client is confused deputy
(C) Banker is confused deputy

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.

Subjects: students
Objects: rooms
Possible access operation: enter room or not

Example:
ACL system: For each room, store a list of students who have booked access to this room.
Advantage of an ACL system: handling number of students per room, can easily check how many students per room.
One possible disadvantage of ACL system: difficult to update permissions which is needed often in this setting

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

Attack: student could submit a PDF with in another student's/incorrect/non-existent SCIPER, and produce a wrong grade report.

Vulnerability Lack of check that the SCIPER in the PDF corresponds to the student submitting the file.

Fix: The fix is to add a check for to make sure that students can only submit their own SCIPER. The TAs could add a login system that ensures students are who they claim and then check the SCIPER against Moodle's records.