CS181S – Systems Security Fall 2020

Problem Session 10: Discretionary Access Control (DAC)

Monday, November 2, 2020

1. **Authorization Relations.** For each of the following, (i) devise a sensible authorization policy, (ii) model it by using an authorization relation Auth and a set C of commands, and (iii) explain whether the authorization policy is DAC.

   (a) Every user U of a file system has a separate directory D_U which, for each file that it lists, associates either a read (r) or read/write (rw) privilege as well as a list of all users authorized to link that file. D_U is updated by the system whenever (i) U invokes a system call to create or delete a file or (ii) U invokes a system call to link or unlink to a file in another users directory. So D_U contains an entry for every file that U has created (but not yet deleted) or linked (but not yet unlinked). Execution of system calls to read, write, create, delete, link, and unlink is restricted in the expected way.

   (b) The users of a course-management system are students, graders, and professors. The objects it manages include assignment descriptions, student-submitted solutions, answer keys, and grades. Operations are supported so that a student may submit a solution, read the answer key, and/or look-up the grade; a grader may read the answer key, read and annotate a student solution, and/or assign a grade (but cannot change that grade, thereafter); a professor may post an assignment description, post an an- swer key, and/or review a student solution for which a grade has already been assigned and then post an updated grade.

2. **Capabilities.** Get a start on this week's homework assignment.