

Homework 1

Due: January 23, 2019

Points: 100

Questions

1. (24 points) Consider the set of rights $\{ read, write, execute, append, list, modify, own \}$.
 - (a) Using the syntax in Section 2.3, write a command $delete_all_rights(p, q, o)$. This command causes p to delete all rights the subject q has over an object o .
 - (b) Modify your command so that the deletion can occur only if p has *modify* rights over o .
 - (c) Modify your command so that the deletion can occur only if p has *modify* rights over o and q does not have *own* rights over o .
2. (20 points) The proof of Theorem 3.1 states that we can omit the **delete** and **destroy** commands as they do not affect the ability of a right to leak when no command can test for the absence of rights. Justify this statement. If such tests were allowed, would **delete** and **destroy** commands affect the ability of a right to leak?
3. (20 points) Prove or disprove: The claim of Lemma 3.1 holds when x is an object.
4. (20 points) Consider the construction of the three-parent joint creation operation from the two-parent joint creation operation shown in Section 3.5.2. Suppose we set $cr_C(s, c) = c/R_3$ and $link_2(\mathbf{S}, \mathbf{A}_3) = \mathbf{A}_3/t \in dom(\mathbf{S})$. Why is this not sufficient to derive the three-parent joint creation operation from the two-parent joint creation operation?
5. (16 points) Classify each of the following as an example of a mandatory, discretionary, or originator controlled policy, or a combination thereof. Justify your answers.
 - (a) The file access control mechanisms of the UNIX operating system
 - (b) A system in which no memorandum can be distributed without the creator's consent
 - (c) A military facility in which only generals can enter a particular room
 - (d) A university registrar's office, in which a faculty member can see the grades of a particular student provided that the student has given written permission for the faculty member to see them.