Homework #1

Due: April 14, 2025 **Points:** 100

Questions

1. (*18 points*) How do laws protecting privacy impact the ability of system administrators to monitor user activity?
2. (*25 points*) This exercise asks you to consider the consequences of not applying the principle of attenuation of privilege to a computer system.
   (a) What are the consequences of not applying the principle at all? In particular, what is the maximal set of rights that subjects within the system can acquire (possibly with the cooperation of other subjects)?
   (b) Suppose attenuation of privilege applied only to access rights such as *read* and *write*, but not to rights such as *own* and *grant_rights*. Would this ameliorate the situation discussed in part 2a? Why or why not?
   (c) Consider a restricted form of attenuation, which works as follows. A subject q is attenuated by the maximal set of rights that q, or any of its ancestors, has. So, for example, if any ancestor of q has r permission over a file f, q can also$r$ f. How does this affect the spread of rights throughout the access control matrix of the system?
3. (*25 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?
4. (*30 points*) Prove or give a counterexample: The predicate $can\bullet share(\alpha, \mathbf{x}, \mathbf{y}, G_0)$ is true if and only if there is an edge from $\mathbf{x}$ to $\mathbf{y}$ in G_0 labeled α, or if the following hold simultaneously:
   (a) There is a vertex with an $\mathbf{s}$-to-$\mathbf{y}$ edge labeled α.
   (b) There is a subject vertex $\mathbf{x}'$ such that $\mathbf{x}' = \mathbf{x}$ or $\mathbf{x}'$ initially spans to $\mathbf{x}$.
   (c) There is a subject vertex $\mathbf{x}'$ such that $\mathbf{s}' = \mathbf{s}$ or $\mathbf{s}'$ terminally spans to $\mathbf{s}$.
   (d) There is a sequence of subjects $\mathbf{x}_1, \ldots, \mathbf{x}_n$ with $\mathbf{x}_1 = \mathbf{x}'$, $\mathbf{x}_n = \mathbf{s}'$, and $\mathbf{x}_i$ and $\mathbf{x}_{i+1}$ $(1 \leq i < n)$ being connected by an edge labeled t, an edge labeled g, or a bridge.
5. (*12 points*) The discussion of acyclic creates imposes constraints on the types of created subjects but not on the types of created objects. Why not?