Homework #1

Due: January 19, 2024 **Points:** 100

Questions

1. (*18 points*) A network in the College of Engineering is set up so that individual hosts (really, virtual machines) can run HTTP (web) servers that are available to the outside. (Here, *available* means the ability to read and write data.) The hosts can also run email (SMTP) servers available to other hosts on the CoE network, but these are *not* available to the outside. Instead, all outside mail is routed to a machine named "smtphost", which forwards it to the internal host, and all internal mail addressed to external hosts is routed to "smtphost", which forwards it to the destination. There are no other servers available to the outside on "smtphost".

   In what follows, use "g" to represent the HTTPS "get" right, "p" the HTTP put right, "s" the email "send" right, and "r" the email "receive" right.

   (a) Please model this using an access control matrix. Use three hosts, "smtphost", "innie" for a host on the CoE network, and "outie" for an outside host.

   (b) Write a command that allows "innie" to exchange email directly with "outie", bypassing "smtphost" entirely.

   (c) Now consider a second host called "reallyinnie" on the CoE network. This host has just been added to the network and has no rights initially. Write a command that gives it the ability to send email to "outie" if, and only if, "innie" can send mail directly to "outie".

2. (*20 points*) Minsky states that "privileges should not be allowed to grow when they are transported from one place in the system to another." Does this differ from the Principle of Attenuation of Privilege as stated in class? If not, show they are the same; if so, how do they differ?

3. (*12 points*) Someone asks, "Since the Harrison-Ruzzo-Ullman result says that the security question is undecidable, why do we waste our time trying to figure out how secure the Linux operating system is?" Please give an answer justifying the analysis of the security of the Linux system (or any system, for that matter) in light of the HRU result.

4. (*30 points*) Theorem 3.1 states: "Suppose two subjects s_1 and s_2 are created and the rights in $A[s_1,o_1]$and $A[s_2,o_2]$ are tested. The same test for $A[s_1,o_1]$ and $A[s_1,o_2] = A[s_1,o_2] \cup A[s_2,o_2]$ will produce the same result." Justify this statement. Would it be true if one could test for the absence of rights as well as for the presence of rights?

5. (*30 points*) Consider the construction in Section 3.5.2 that shows how to simulate three-parent joint creation using two-parent joint creation. In the original paper, $cr_C(s,c) = c/R_3$ (that is, the t right was omitted) and $link_2(\mathbf{S},\mathbf{A}_3) = \mathbf{A}_3/t \in dom(\mathbf{S})$ (the second part was omitted). Why won't this work?