Homework #1

Due: January 23, 2014   **Points:** 100

Questions

1. (*21 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".

   (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. Don't forget to include the HTTP servers!

   (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. (*24 points*) Let c be a copy flag and let a computer system have the rights {*read, write, execute, append, list, modify, own*}.

   (a) Using the syntax in Section 2.3, write a command *copy_all_rights*(p, q, s) that copies all rights that p has over s to q.

   (b) Modify your command so that only those rights with an associated copy flag are copied. The new copy should *not* have the copy flag.

   (c) In the previous part, what conceptually would be the effect of copying the copy flag along with the right?

3. (*20 points*) Someone asks you, "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 UNIX operating system is?" Please give an answer justifying the analysis of the security of the UNIX system (or any system, for that matter) in light of the HRU result.

4. (*35 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 $\mathbf{s}'$ 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.

Extra Credit

1. (*20 points*) Prove Lemma 3.2.