Homework #2

Due: April 12, 2013 **Points:** 100

Questions

1. (*25 points*) Consider the construction in Section 3.5.2 that shows how to simulate three-parent joint creation using two-parent joint creation (this is on pp. 80–83 of the text). 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?
(*text*, problem 3.9, modified)

2. (*25 points*) Use DTEL to create a domain *d_guest* composed of processes executing the restricted shell */usr/bin/restsh*. These processes cannot create any files. They can read and execute any object of type *t_sysbin*. They can read and search any object of type *t_guest*.
(*text*, problem 4.7)

3. (*25 points*) Expand the proof of Theorem 4–2 to show the statement, and the proof, of the induction.
(*text*, problem 4.7)

4. (*25 points*) Prove Theorem 5–11.
(*text*, problem 5.11, modified)

Extra Credit

1. (*20 points*) Consider McLean's reformulation of the simple security condition, the *-property, and the ds-property (see page 146).

   (a) Does this eliminate the need to place constraints on the initial state of the system in order to prove that the system in secure?
   (b) Why do you believe Bell and LaPadula did not use this formulation?

   (*text*, problem 5.12)