Questions

1. (20 points) Consider the construction of the three-parent joint create operation from the two-parent joint creation operation. In an early paper on this, $cr_C(s, c) = c/R_3$ and $link_2(S, A_3) = A_3/t \in \text{dom}(S)$. Why is this not sufficient to derive the three-parent joint create operation from the two-parent joint creation operation? (text, §3.9, exercise 9)

2. (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 author’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.
   (text, §4.11, exercise 5)

3. (30 points) Prove Theorem 4-1. Show all elements of your proof. (text, §4.11, exercise 10)

4. (10 points) In the DG/UX system, why is the administrative region above the user region? (text, §5.8, exercise 5)

5. (24 points) Paul needs to read and write some documents. In the following, assume the system security policy is described completely by the Bell-LaPadula model. Note that the situation described may be impossible, in which case you should say so and show why.
   (a) Please give the least clearance that Paul can have if he wishes to read a document with classification (SECRET, {NUC, EUR}) and a document with classification (CONFIDENTIAL, {ASI}).
   (b) Please give the greatest clearance that Paul can have if he wishes to write to a document with classification (TOP SECRET, {EUR}) and a document with classification (SECRET, {EUR, NUC}).
   (c) Please give the greatest clearance that Paul must have if he wishes to read a document with classification (SECRET, {EUR, NUC}), to write a document with classification (CONFIDENTIAL, {NUC, EUR}), and to read another document with classification (TOP SECRET, {ASIA, EUR}).

Extra Credit

1. (20 points) Consider the UC Davis policy on reading electronic mail. A research group wants to obtain raw data from a network that carries all network traffic to the Department of Political Science.
   (a) Discuss the impact of the electronic mail policy on the collection of such data.
   (b) How would you change the policy to allow the collection of this data without abandoning the principle that electronic mail should be protected?
   (text, §4.11, exercise 9)