CS 6393 SPRING 2012
PROF. RAVI SANDHU
EXAMINATION 1
DUE TUESDAY MARCH 13, 2012 BY5:00PM

- Each examination is to be solved by students individually. Students can access whatever material they choose but cannot discuss with other students or colleagues.
- It is highly unlikely that web browsing will help with the solution. Anything you find on the web may well be wrong. Spend the time and effort thinking. Don't waste your time browsing.
- Each solution must be within the length limits provided.
- Solutions are to be submitted by email in pdf to ravi.cs6393@gmail.com.
- Text must be typed. Hand drawn figures are acceptable if appropriate but must be scanned and incorporated in submitted pdf. Figures must fit within the specified size limit for the entire answer. Scanning can be done using ICS scanner during normal business hours (bring a USB flash drive to store the scan). Figures can be submitted on separate pages if you are unable to incorporate in a pdf page, but will be counted for overall length allowance.
- I am not looking for a specific or "correct answer." I am looking for demonstration that you can think through the question and answer in coherently based on my lectures and supporting material.
- Discussion and mention of irrelevant issues will be penalized.

Answer all questions. All questions have equal weight.
All questions have max ½ page allowance for answer in 11 point font.
Each solution must be accompanied by the following statement:
I have not taken any help on this examination from anybody and have not given any help to anybody.

1. Consider the high water and low water mark policies defined as follows for an LBAC system.
    - Security labels on objects do not change. They are fixed when the object is created and remain constant thereafter. (BOTH)
    - Each subject is associated with a single user called its creator. (BOTH)
    - Security label on subjects may go up in the lattice (but no higher than the creating user's clearance) but cannot go down or change to incomparable values. (HIGH WATER MARK)
    - Security label on subjects may go down in the lattice but cannot go up or change to incomparable values. (LOW WATER MARK)

   Discuss why low water mark is considered "more dangerous" than high water mark.

2. Discuss high water mark and low water mark as applied to users rather than subjects. Are these "useful" policies? Are they "secure"?

3. In the NIST RBAC model the DeleteRole function (page 251) deletes all sessions which have that role activated. Is this practical? Discuss possible alternatives that may be "more practical."

4. Discuss the expressive power of $RBAC_1$ (from RBAC96) in comparison to uni-$RBAC_1$ defined as identical to $RBAC_1$ with the restriction that each user can only be assigned to a single role in the URA relation. Is it possible to simulate $RBAC_1$ in uni-$RBAC_1$? Vice versa?

5. The GD formalization of the access matrix model is default-deny. Only the presence of a right can actually authorize operations such as read and write. Some commercial systems actually operate as default-permit. Attempt a default-permit formalization of the access matrix analogous to GD.