INFS 767 FALL 1999

Ravi Sandhu

1st Midterm Examination

This is an open-book open-notes take-home exam. The exam questions should not be discussed with anyone. You must solve the exam on your own. Discussion of the general topic area with your fellow students and colleagues is permitted.

Due: Hard copy solution due on 10/21/99 in class

Please sign and submit the following statement along with your solution: *As per the GMU honor code I have not given nor received any help on this examination.*

Solve all questions. All questions have equal weightage. Limit your answers to 1 page maximum. Explain your answer so it is self contained. Hand written answers are acceptable but must be neatly presented. Make your answers crisp and to the point. Please do not discuss the questions with me. Make and state any assumptions necessary to progress on the solution.

1. **RBAC96 is based on the additive approach. The permissions available in a session are the union of permissions from the roles activated (explicitly or implicitly) in a session. Consider an alternate approach (call it anti-RBAC) where the permissions available in a session are the intersection of permissions from the roles activated (explicitly or implicitly) in a session. Discuss the merits of anti-RBAC.**

2. **Consider the URA97 model. Without changing RBAC96 how can we do grant-dependent revocation in URA97? Discuss. Would it make sense to have grant-dependent and grant independent revocation within the same model?**

3. **Answer the following questions.**

   A. **The range notation in URA97 and PRA97 has ability to include or exclude the end points of the range. In RRA97 the range notation always excludes the end points. Explain why.**

   B. **Explain the difference between a create range and an encapsulated range in RRA97.**

   C. **Is it useful to deploy URA97 when we have a small number of roles (say, less than 20).**

4. **In URA97 and PRA97 the prerequisite condition is checked only at the moment of granting. If the prerequisite condition changes from true to false at some later time the grant stays in effect. Consider alternative models (call them URA97' and PRA97') where the grant is automatically revoked when the prerequisite condition becomes false. Discuss the merits and demerits of this alternative compared with URA97 and PRA97.**

5. **Discuss how ARBAC97 and related models could apply to secure electronic commerce where more than one organization is involved.**

6. **Analyze the following role hierarchy where the solid lines denote inheritance hierarchy and the dashed lines denote activation hierarchy. Clearly and completely state the constraints under which your analysis is done. How does the overall policy compare with the hierarchy of slide 37 of lecture 5?**