INFS 767 FALL 1999

Ravi Sandhu

3rd and Final 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: on 12/16/99 before 5pm. Please deliver hard copy to my office or my mailbox in the department. Email is also acceptable to sandhu@gmu.edu. Please use MSWord, pdf, postscript or plain text.

Please 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 for each question. 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) **Consider the UST protocol discussed in lecture 8. In order to achieve its security objectives, this protocol makes some compromises regarding ease of use for subscribers, vendors and system developers. Identify these compromises and argue whether or not each one is justified.**

2) **Consider the DRBAC system discussed in lecture 9. Discuss the advantages and disadvantages of using user-pull and server-pull architectures for this RBAC policy.**

3) **We understand certificate to mean data that has been digitally signed (using public-key technology) by some certificate authority. Carl Ellison has identified 3 kinds of certificates as follows.**

   a) **Identity certificate: binds user identity and public key**
   b) **Attribute certificate: binds user identity and permission (or role)**
   c) **Authorization certificate: binds public key and permission (or role)**

   For each case discuss whether or not it would be useful to support this kind of certificate in a public-key infrastructure.

4) **Try to relate Java SDK1.2 as discussed in lecture 10 to the policy-model-architecture-mechanism discussed in earlier lectures.**