Introduction to Computer Security
Final Exam
Winter 2007

This is a closed-book, closed-notes exam.

1. Short Answer. [12 points]

   Please give a **short** description of each of the following:

   (a) Covert channel.

   (b) Common criteria.

   (c) Software fault isolation

   (d) Virtualization

2. Access Control [12 points]

   (a) Describe what an access control list is.

   (b) Explain how UNIX permissions can be regarded as access control lists.

   (c) Describe capability based access control.

   (d) Contrast access control lists and capability based access control.

3. Identity [12 points]

   When doing commerce on the web, users expect to have some level of assurance that they are in fact interacting with the vendor associated with the web site they think they are visiting. Describe a mechanism that is used to establish identity for e-commerce transactions. Does the mechanism you describe have a tree structure with a distinguished root, or is it a general graph (web of trust) without a distinguished root.

4. Information Flow [12 points]

   (a) Give an example program that has at least three variables, a, b, and c. Construct the program so that there is an explicit flow from a to c and an implicit flow from b to c. There should be no explicit flow from b to c.

   (b) Use the type system presented in Sabelfeld and Myers (reproduced separately, but included with this exam) to show that if a and b are low variables and c is a high variable that the program you construct can be typechecked.

5. Malicious Logic [12 points] What is a polymorphic virus? What class of defensive mechanisms do polymorphic viruses circumvent? Justify.

6. Design Principles [40 points]

   In their 1975 paper, Saltzer and Schroeder articulated eight principles for "The Protection of Information in Computer Systems". These principles are:

   - Least Privilege
   - Fail-safe Defaults
   - Economy of Mechanism
   - Complete Mediation
   - Open Design
   - Separation of Privilege
   - Least Common Mechanism
   - Psychological Acceptability

   (a) [16 points] Give a short description of each of the principles.

   (b) [12 points] In class we have discussed the Feldman, Halderman, and Felten study of the Diebold voting machine. Evaluate the Diebold design as described in the paper with respect to the principles of (1) least privilege, (2) open design, and (3) psychological acceptability.

   (c) [12 points] In class and in previous exams we have discussed the application of the Biba and Clark-Wilson integrity models to the voting machine. Briefly summarize the two approaches. Discuss how the design principles could be applied to these two approaches. Specifically address the following principles in your discussion: (1) least privilege, (2) economy of mechanism, (3) complete mediation.