CSCI 283-172 - Computer Security I - Fall 2010
George Washington University

Final Exam
DUE on 21 December 2010, by 6 pm., on Blackboard
100 points, 25% of grade

Open Book Exam

No consulting anyone else

Cite all your sources. While you may not use exactly the complete solution published/used by someone else, you may look at published material for methods that address the separate issues involved if you wish, though this is not necessary. The exam has been designed so that you may solve it using the material you have learned in class; found in the class slides and the text book.

Design an Internet banking system as follows (provide the answer to each question on a new page):

A. (15 points) Define the security policy for the system. Who are the subjects? What are the objects? What should the access rights be? (Three-quarter page.)

B. (25 points) Assume that users obtain access through biometric authentication. There is a fingerprint reader that validates the identity and uses the fingerprint to construct a private key. You may assume that the fingerprint reader is accurate and that there is a means for securely computing the private key and keeping it only during the session, after which it is erased and recomputed the next time the user logs in. There is a certificate for the corresponding public key that exists beyond sessions. Describe the authentication protocol used between the bank and the user's computer to authenticate the user. (One page.)

C. (25 points) Provide an attack tree for the vulnerabilities of your system (one page) and a very brief description of the various possible attacks (half a page).

D. (20 points) Design audit logs for the system (what will the system maintain records of, for security purposes), along with an access control policy for the logs and a means of enforcing the policy (who or what process can read/write audit files; how is integrity of the audit log ensured). (One page.)

E. (15 points) How can the audit logs help reduce the impact of the vulnerabilities you found in (C)? Are there any other ways of reducing the impact of the vulnerabilties? (Half a page.)