

CSCI 283-172 - Computer Security I - Fall 2008
George Washington University

Final Exam

DUE on 16 December 2008, by 6 pm., on Blackboard

50 points, 25% of grade

Open Book Exam

No consulting anyone else

Cite all your sources. Your answer to each question should not be more than 2-3 typewritten pages. While you may not use exactly the complete solution of an authentication system (problem 1) or a secure/private auction system (problem 2) published/used by someone else, you may look at published material for methods that address the separate issues if you wish.

1. Design an authentication system that “learns” information about the user and uses it to enhance its capabilities (you do not need to describe the learning algorithms, simply describing what is learnt is enough). Analyze the scheme - what are attacks on the scheme, is there an “optimal” “amount” of information it should use? Your scheme is not allowed to ask the user any questions. It should base its learning on material it can collect without explicitly asking the user to do anything at all for the express purpose of providing it with the information. The only information it can obtain from the user is when the user signs up for an account. At this time, the questions asked of the user should be standard questions required for a standard authentication scheme. Your design should address the effect of the initial (standard) authentication method, such as PKI-based authentication, password-based authentication, etc. You may assume that the user is a lay user who uses the account for various “regular” activities, such as email, chat, word processing, financial accounting and records, web browsing, and multimedia access, such as music and films.

2. Suppose you were to design a system for conducting electronic auctions among students at GW. First describe the goals of the system. Then, in more detail, describe the privacy and security issues that would need to be addressed, and the methods you would use to address them (make sure to include all references). Justify your choice of each method, and indicate its strengths and weaknesses. Assume that firewalls and malware protection are standard and available, i.e. do not include these in your list of issues to address.