

CSCI 283 and CSCI 172- Graduate and Undergraduate Computer Security - Fall 2006
George Washington University

Homework 2

due 9 November, 6 pm.

100 points

Policy on collaboration: All examinations, papers, and other graded work products and assignments are to be completed in conformance with The George Washington University Code of Academic Integrity. You may discuss HWs among yourselves, and work on them in groups. However, each student is expected to write his or her own HW out independently; you may not copy one another's assignments, even in part. You may not collaborate with others on the test and final.

You are expected to cite all your sources in any written work that is not closed book: papers, books, web sites, discussions with others - faculty, friends, students. For example, if, in a group, one student has a major idea that leads to a solution to a HW problem, all other students in the group should cite this student.

You may not refer to solutions to previous years' problem sets, or ask for help students from previous years, except the TA.

Any violations will be treated as violations of the Code of Academic Integrity.

PLEASE submit all HW on Blackboard only. Name your files:
CS283_HW2_LASTNAME_FIRSTNAME.doc or .pdf or
CS172_HW2_LASTNAME_FIRSTNAME.doc or .pdf

1. (50 points) For the authentication protocol in the examination, Problem 3,
 1. At the polling booth, each individual wishing to vote produces his or her driver's license.
 2. The driver's license photograph is checked, and the name on it is checked against a list of registered voters.
 3. The individual is allowed to vote if and only if
 - The photograph on the license checks successfully
 - His or her name is on the list and
 - The list does not indicate that he or she has already voted.
 4. When a voter votes, his or her name is checked off on the list as having voted.

construct an attack tree, labelled with the expense associated with each node, and a probability estimate. The goal of the attack is to stuff the ballot box with illegitimate votes. Describe how you estimated the values.

2. (50 points) Describe a simple paper voting election protocol, that involves no scanners and no computers (just voting as our grandparents might have done it). Do not address the authentication protocol, assume it is perfect.

Construct an attack tree for this protocol, whose goal is to change the outcome of the election.