CS 6393 SPRING 2012
PROF. RAVI SANDHU
EXAMINATION 2
DUE FRIDAY MAY 11, 2012 BY5:00PM

- Each examination is to be solved by students individually. Students can access whatever material they choose but cannot discuss with other students or colleagues.
- It is highly unlikely that web browsing will help with the solution. Anything you find on the web may well be wrong. Spend the time and effort thinking. Don't waste your time browsing.
- Each solution must be within the length limits provided.
- Solutions are to be submitted by email in pdf to ravi.cs6393@gmail.com.
- Text must be typed. Hand drawn figures are acceptable if appropriate but must be scanned and incorporated in submitted pdf. Figures must fit within the specified size limit for the entire answer. Scanning can be done using ICS scanner during normal business hours (bring a USB flash drive to store the scan). Figures can be submitted on separate pages if you are unable to incorporate in a pdf page, but will be counted for overall length allowance.
- I am not looking for a specific or "correct answer." I am looking for demonstration that you can think through the question and answer in coherently based on my lectures and supporting material.
- Discussion and mention of irrelevant issues will be penalized.

Answer all questions. All questions have equal weight.
Each question should be answered in about 3/4 of a page in 11 point font.
Much shorter or much longer answers will be penalized.
Please provide citations for ANY material used from the literature

Each solution must be accompanied by the following statement (one statement suffices for entire exam):
I have not taken any help on this examination from anybody and have not given any help to anybody.

1. Explain the difference between a side channel and a covert channel. Discuss the claim that every side channel can be converted to a covert channel and vice versa.

2. Explain the difference between intrusion prevention and intrusion detection systems. Discuss the implications of the base-rate fallacy for intrusion prevention.

3. Consider the concept of "continuous" enforcement in UCON. Discuss how this concept might be implemented in practice. Develop your answer in context of specific application contexts.

4. Read the paper: Hiltgen, A., Kramp, T. and Weigold, T., "Secure Internet banking authentication." *IEEE Security & Privacy*, vol.4, no.2, pp.21-29, March-April 2006. Write a 3-part review of this paper explaining (1) what you liked or disliked about the paper, (2) something you learned by reading the paper, and (3) some weakness in the paper.