Name: _____ **USC ID:** _____

CSci 530 Final Exam

Fall 2009

Instructions:

Show all work. No electronic devices are allowed. This exam is open book, open notes. You have **120 minutes** to complete the exam.

Please prepare your answers on separate sheets of paper. You may write your answers on the sheet of paper with the question (front and back). If you need more space, please attach a separate sheet of paper to the page with the particular question. **Do NOT extend your answer on the back of the sheet for a different question, and do NOT use the same extra sheet of paper to answer more than one question**.

In particular, **each numbered questions must appear on separate pieces of paper so that the exam can be split for grading**. If part of the answer to one of the questions (Q1, Q2, or Q3) is on a sheet of paper also used for one of the other questions, then that part of your answer might not be graded and you will NOT receive credit for that part of your answer.

Be sure to include your **name** and **USC ID** number **on each page**.

There are **100 points** in all and **3 questions.**

	Q1	**Q2**	**Q3**	**Total**	**Letter**
Score					

Name: _____ **USC ID:** _____

1. (30 points) Offense in Breadth

We have talked about defense in depth as a technique for improving the security of a computer system. In contrast to defense in depth, the adversary would rather we implement defense in breadth, i.e. use different techniques to protect different parts of the system in such a way that a breach of any of the defenses leaves us vulnerable. In this section I will list several security technologies, and you are to think like an attacker. Under the assumption that they can't break the particular technology mentioned, you are to suggest how they step around the defense and attack in a different way. Note that there may be several answers to each, and you should list more than one if appropriate. (6 points each)

a) SSL protection of email messages retrieved using POP.

b) Firewalls in home routers that that block inbound connections.

Name: _____ **USC ID:** _____

c) SSL authentication of web servers showing the user the name of the server to which they have connected.

d) Confidentiality of data handled by a trusted application which has been attested to by the TPM.

e) A host based root-kit detection mechanism.

Name: _____ **USC ID:** _____

2. (30 points) System Integrity

One of the most difficult problems in computer security has to do with ensuring the integrity of the system and software that one uses. Your personal computer at home may be compromised and part of a bot-net. The software you download may have been modified by an attacker to do other things. The web site that you connect to may be collecting information and sending it elsewhere. In this question I list several technologies that might be helpful in assessing the integrity of your system (including the software that is running on the system). For each, you are to briefly state how it helps provide assurance of integrity or discovery of integrity breaches and who can be informed of such compromise. Also describe any limitations: you need to indicate when or against what kinds of attack or malicious code it might not be effective. If the technique has particular strengths, describe them as well.

a) Signature based virus scanner

b) Network based intrusion detection system

c) Trusted computing

Name: _____ **USC ID:** _____

3. (40 points) Design Problem

You have been hired by a consortium of electric utilities to help them improve the security of the power grid. In particular, you have been asked to look at security for the meters that will be place at customer's homes, and for the communication between the meters and the central infrastructure. The meters will communicate with the utility through a wireless link, and the meters themselves report on accumulated power use. The meters can be remotely control to turn power on or off to the residence. The meters themselves are remotely programmable, and it is planned that their software will be upgraded in the future to enable new functionality, including the ability for the meters to communicate through a home area network with devices in the home. This link may be used to relay commands to control such devices in the home, or to provide real time pricing data that may be used by a home power management system.

a. Which of the basic three security goals (CIA) are important in this system? For each, give an example of why that goal must be met, and the consequence if it is not met. (15 points)

b. Suggest your approach to protecting communication in the system to meet the goals established in part a. Consider communication from the meters to the central systems of the utility, as well as communication of commands to the meters. As part of your answer, explain what information must be maintained and protected on the meters themselves. (10 points)

Name: _____ **USC ID:** _____

c. Suggest techniques for protecting the integrity of the software running on the meters. Consider the mechanisms by which the meter decides to accept remote programming, and also the method by which remote sites can be certain the integrity of the meter has not been compromised. As in part b, your answer should include a discussion of the information that must be maintained and protected on the meters themselves, and in this case, also HOW that that information is to be protected. (15 points)