Name: ______________________ **USC ID:** ______________________

CSci 530 Final Exam

Fall 2005

Instructions:

Show all work. **If a question asks for a numerical or algebraical result, indicate your answer clearly (for example, by drawing a box around it)**. 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**.

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 Score**
Score				

Question 1 (25 points) - E-Mail Authentication

Kerberos can be used to authenticate the retrieval of electronic mail message using POP and IMAP. Explain why Kerberos is not well suited for authentication of the electronic mail messages themselves.

Name: ______________________ **USC ID:** ______________________

Question 2 (40 points) - Trusted Computing

If a system/platform is designed to provide support for trusted computing it is still possible for the systems to run untrusted or uncertified programs. In contrast, if a program is designed to run with trusted computing support, such a program is ***not*** trusted unless it runs on a trusted platform.

Consider a program designed to allow an employee at home to interact with a server over the network where the home program will have access to confidential customer information. This program must be considered as trusted by the server before confidential data will be returned.
Please answer the following questions:

a. (5 points) List the security requirements of such an application, with respect to remote access to confidential data.

b. (10 points) List all entities that must be trusted by the server (by entity, I am including any individuals or parts of the system that are necessary to perform the remote access).

c. (10 points) For each of the entities, explain why it must be trusted and give an example of what a malicious component might do to violate the security requirements listed in a.

d. (5 points) For each of the entities, give an example of how it might be compromised.

e. (10 points) For each of the entities, explain how it proves to the server that it can be trusted. In particular, what information is needed by the entity to prove that it can be trusted and has not been compromised, and how is this information presented to the server? Note: certain entities will need to repeat proofs from other entities, in addition to their own - please list all the proofs needed even if they are repetitive from previous parts of an answer (it is ok to list it by reference).

Question 3 (35 points) - Design Problem

You have been asked to design a system that will provide effective response to new attacks. The system you design will have two components, an intrusion detection component designed to detect attacks, and a dynamic policy enforcement mechanisms that will dynamically adjust policies based on what is learned about attacks from the intrusion detection component. Your system is supposed to provide an effective defense against viruses, worms, as well as attacker targeted penetration attempts to the systems in your organization.

This question, like all of the questions I ask, is intended to judge your understanding of the topics we have covered in class. In some cases, we will look for insight in your answers that will be clear to you if you understand the issues, but which will not be obvious to you if you are just reading back material in your notes. The best answer to this problem is to consider yourself in the position described in the scenario and tell us how you would best solve the problem described.

A. The Intrusion Detection Component (15 points)

i. (10 points) Which approach will you take to intrusion detection? Will your system be anomaly based or signature based, and will the collection of information be performed on the network, at the host, or within applications? Explain why you will take the approaches you select?

ii. (5 points) Explain how the information you collect will be processed (moved to where it is needed, filtered, scanned, etc)? How will you reduce the number of false alarms (false positive). How likely is your system to miss viruses, worms, and intrusions (false negatives)?

B. The Policy Enforcement Component (10 points)

i. (5 points) Where will policies be enforced in your system? Note that there are many policies to be enforced, but in this question we are concerned only with the policies designed to defend against viruses, worms, and penetration attempts that originate from outside your organization.

ii. (5 points) Where will the policies originate (i.e. where will they come from or how will they be created)?

C. Integrating the two components (10 points)

i. (5 points) Give an example of how information collected in the intrusion detection component of your system can be used to create a new policy that will defend against a newly observed attack.

ii. (5 points) Give an example of the use of the policy enforcement component of your system to improve the functionality or capability of the intrusion detection component of your system.

iii. (Extra credit) Tell us anything else you think would be really useful in the system you have designed.