Name: _____ **USC ID:** _____

CSci 530 Midterm Exam

Fall 2011

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**. The exam will be split apart for grading by different people, and if part of your answer for one question appears on a page given to a different grade because the sheet contains parts of the answer to more than one question, then you will NOT receive credit for that part of the answer not seen by the grader. 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					

Name: _____ **USC ID:** _____

1. (30 points) Cryptography - For each pair of methods for encryption or key management, list the major differences in their characteristics or strength, indicating for each difference, which of the two methods is stronger or more secure for the selected characteristic and why. Examples of characteristics that are different for some of the pairings include strength for confidentiality, strength for integrity, size of the key-space, support for non-repudiation, dependence on a third party, performance, and whether authentication is provided. Only some of the characteristics will be different for many of the pairings.

   a) DES in CBC mode vs. DES in OFB mode.

   _____

   _____

   _____

   b) RSA with a 512 bit key vs. AES with a 128 bit key.

   _____

   _____

   _____

   c) Kerberos vs. Diffie Hellman Key exchange

   _____

   _____

   _____

   d) One time pad vs. AES with a 128 bit key.

   _____

   _____

   _____

   e) RSA as a block cipher with a 2056 bit key vs. DES in ECB mode.

   _____

   _____

   _____

   f) Kerberos vs. Public Key Based certification infrastructure (PKI).

   _____

   _____

   _____

Name: _____ **USC ID:** _____

2. (30 points) Malicious Code

Answer the following questions regarding malicious code:

a. How are each of the three primary classes of malicious code propagated? In answering this, explain what steps and conditions that are necessary for the malicious code to start executing on a new computer. (15 points)

b. How far is the impact of an infection by malicious code of each type likely to propagate? What affects this propagation and what steps can be taken to partially contain or limit the spread of the malicious code. Consider iterative infection in answering this question (i.e. once one system or part of a system is infected, will the malicious code spread further, and how can we reduce the spread). [please answer on back of page] (15 points)

Name: _____ **USC ID:** _____

3. (40 points) Design problem

The Hacker group Anonymous has recently threatened to mount attacks on the New York Stock exchange and other financial and other organizations in sympathy with the actions of the Occupy Wall Street movement. You have been hired to stop them. Well… more precisely, you have been hired for a longer term job of redesigning the infrastructure supporting the markets (the NY Stock Exchange, NASDAQ, commodity exchanges, etc) to make these systems more resilient and secure. For now you are only going to focus on a single stock exchange, and within the next 40 minutes (roughly) you will answer questions about the problem, and your preliminary design.

a. Discuss in general terms requirements of the system and how they impact, or are impacted by security considerations. More specifically, i) describe the kinds of data in the system, and the implications for unauthorized disclosure of each kind of data, as well as for unauthorized modification of such data, and disruption of availability of such data; ii) describe the services provided by the system and the security implications for unavailability (e.g. denial of service) of such services, or delays in providing such services. (10 points)

b. Discuss in general terms the classes of users of the system, the data and services that each must access, and from where they need to be able to access the data and services. Discuss in general terms also the classes of adversaries that might want to attack the system, and the access that they must have (yes, this seems strange - the access they must have - keep in mind that attackers may be indistinguishable from some classes of legitimate users). For these adversaries, discuss their different motivations for attack, and what it would mean for their attacks to be successful. (10 points).

c. In the design of your system, how will you structure the protection domains - e.g. what will be the distinct regions of your system, and which data will be stored and which services provided from each of these regions (5 points).

Name: _____ **USC ID:** _____

d. For each class of authorized user, discuss techniques that should be used for authentication of the users. Be sure to consider the cost of each method you use, the "factor" that is checked. How will data be protected as it crosses the network, and how is this form of protection tied to (or not tied to) the authentication methods that you have chosen. (10 points)

e. Discuss some of the "policies" to be applied for access to service and data. Where are these policies applied in the system, and which of them relate to the protection domains listed in [c]. Which of these policies are "discretionary", and which are "mandatory or role based. (5 points)