Name: ________________________ **USC ID:** ________________________

CSci530 Final Exam

Fall 2014

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. (35 points) Intrusion Detection and Trusted Computing
Please answer the following short questions (5 points each):

a. For a cyber-physical system, provide an example of the propagation of a threat from a cyber-domain to a physical domain?

b. What are the two primary functions of the Trusted Platform Module?

c. How would you use accreditation in a cloud computing environment?

d. How does a social engineering attack get around the defenses of a system?

e. Why is it important to place some defenses outside the perimeter of a protected system?

f. Describe what we mean by the term linkability when we discuss privacy? (this one is worth 10 points - answer on back)

2. (25 points) Privacy and user Tracking

For each of the following countermeasures, match the technique with the attacks against which it is effectively applied. This is **not** a one-to-one mapping; more than one term may be relevant to a technique, and more than one technique may use the same term in its implementation or description. If you list a match that we are not looking for, but which is still correct, while you will not lose credit, you will not get credit either. You will lose a point if you associated an approach or technique with a threat that it is not effective against. There are more blanks in the page below than actual correct answers, so you do not need to fill in all the blanks.

1. User Education
2. Firewalls
3. Signature Based Intrusion Detection
4. Anomaly Based Intrusion Detection
5. Virtual Private Networks
6. SSL or TLS
7. Data Encryption
8. Trusted Computing
9. Digital Signatures

i. Viruses: ____ _____ _____ _____ _____ _____

ii. Worms: ____ _____ _____ _____ _____ _____

iii. Social Engineering: ____ _____ _____ _____ _____ _____

iv. Insider Threat: ____ _____ _____ _____ _____ _____

v. Distributed Denial of Service: _____ _____ _____ _____ _____

vi. Rootkit: ____ _____ _____ _____ _____ _____

vii. Spyware: ____ _____ _____ _____ _____ _____

viii. Network Monitoring: ____ _____ _____ _____ _____ _____

ix. Impersonation: ____ _____ _____ _____ _____ _____

Name: ______________________ **USC ID:** ______________________

3. (40 points) Design Problem

SONY is in the process of re-implementing their core IT infrastructure in response to the recent security breaches that have occurred. Since they will ultimately redeploy from scratch they are using the opportunity to change organization of their systems to better meet the needs of their diverse divisions, and to provide the best performance and scalability possible. You have been hired to assist them with their design, focusing on distributed system scalability and operating systems issues.

Sony Pictures has multiple divisions including divisions providing retail services (selling products), electronic games (including online interactive entertainment), television and movie production, and television and movie distribution. As with other movie studios, individual films are produced by new production companies dedicated specifically to a particular title and these companies will hire their own staff and contract for services with other providers, all of whom require access to the data files associated with a particular production. Parts of production occur "on location" in remote locales. Certain services needed for production may be provided by Sony Pictures itself in support of these organization dedicated to particular titles.

Your initial job is to develop an architecture for securing SONY's infrastructure.

a) List the different classes of data in the system (by classes, I mean those groups of data which are to be accessible in the same ways). List also the different classes of users of the system. Explain which users are to have access to which kinds of data, and whether that access is to read or modify data in the class, and if that access is to all data in the class or just to "their own" data from that class. (what I mean is that you should not list data of each separate individual as a different class even though I can access my own data from that class and you can access yours). (10 points)

b) Describe the network structure for your proposed design. In particular, tell me what kinds of data will exist of various servers throughout the system, who will have access to which servers, and which servers will be capable of communicating with other servers in your system. (15 points - answer on back of page)

c) Describe the techniques or methods which you will use to protect the data in the system, to prevent denial of service attacks on critical servers, and to protect the integrity of the system as a whole, and the integrity of individual servers and applications.
(15 points)