Name: _____ **USC ID:** _____

CSci530 Final Exam

Fall 2012

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) Isolation

The most effective technique for protecting information and control systems is isolation. Isolation is provided in computer systems in many ways. For each of the techniques or tools described below, describe what is isolated, and from what. Is the isolation typically one-way, or bidirectional? Is the isolation absolute, or dependent on policy? If dependent on policy, how or where is the policy specified? What are the limits or shortcomings present in the isolation provided?

Characteristics Method	What is isolated from what	1-Way or Bi-direct	Absolute? Or how the policy is specified	Limitations/ weaknesses
Virtual Memory				
Firewalls (network, hostbased, and Application proxies)				
Virtualization				
Data Encryption				
VPN's, tunnels, IPSec, Or IPv6 security approaches				
The TPM for Trusted Computing applications				

Name: _____ **USC ID:** _____

2. (30 points) Matching of Security Technologies

For each of the following technologies, match the technology with the threats it is effective against. This is **not** a one-to-one mapping; more than one technique may be effective against a particular threat. We are looking for specific matches for which you will receive credit. 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. Firewalls
2. Signature based Intrusion Detection
3. Trusted Computing
4. System Architectural Design
5. Anomaly based intrusion detection
6. User education
7. Onion Routing
8. Encryption
9. Digital Signatures

a) Computer Virus: ____ _____ _____ _____ _____ _____

b) Worm: ____ _____ _____ _____ _____ _____

c) Eavesdropping: ____ _____ _____ _____ _____ _____

d) Phishing: ____ _____ _____ _____ _____ _____

e) Traffic Analysis: ____ _____ _____ _____ _____ _____

f) Modification of data: ____ _____ _____ _____ _____ _____

g) Zero Day Threats: ____ _____ _____ _____ _____ _____

h) Data theft: ____ _____ _____ _____ _____ _____

i) "insider" threats: : ____ _____ _____ _____ _____ _____

Name: _____ **USC ID:** _____

3. (40 points) Design Problem - Security for a short trip car rental service

You have been hired to design the security architecture for a competitor to the zipcar® service. Like the zipcar® service, registered customers will have a device they use to unlock and start a vehicle, and they will be able to reserve, pay for and track their usage of vehicle online. The system must maintain information needed to assess the risk of renting to a user, authorize use of vehicle, bill customers, and receive payment from customers.

a. List the entities in your system which will have access to read, or to update the data in your system. For each entity mention briefly some of the characteristics of access (e.g. how often, or from where they might read or write data). (5 points)

b. List the data you believe must be managed by your system. List this data in groups according to the policy that applies for access to such data (for example, one group is data that can be updated and read by the individual customer, another group is data that can only be modified by the service itself, plus there will be other groups). Label each group and tell me the policy that applies for access to such data. For each group, list also the consequences of a failure to enforce such a policy. (15 points)
[Please answer on back of page]

Name: _____ **USC ID:** _____

c. List the protection domains in your system. Specifically, which groups of data (from b) will be stored on which servers, or in which parts of your network? Describe the protection methods (you can draw upon the table in question 1) you will use to protect the data in each protection domain. (10 points)

d. Tell me about the device that will be used to unlock and start the vehicle? I am not concerned about the radio-frequency and optical communication of the device (I will assume that), but please tell me about the data on the device, what happens with that data, and what information is communicated by the device and when. (10 points)
[Please answer on back of page]