Name: _____ **USC ID:** _____

CSci530 Final 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**.

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) Intrusion Detection

A fairly recent approach to intrusion detection is known as "Specification -Based" instrusion detection (SpecID). Specification-based intrusion detection is well suited to physical systems where the correct, and non-compromised, functioning of the system is well understood. It can be applied to computer systems too, when the the interactions that occur we well-constrained and can be modeled manually by the system designers or system operators.

a. Where does specification-based intrusion detection fit relative to anomaly-based (AnomID) and signature based ID (SigID)? Is it closer to anomaly-based or to signature based, and how close is it to the one you select? (10 points)

b. How does it differ from the approach to which it is closest? How do the differences affect the ease of implementing the approach? (10 points)

c. Compare SpecID with each of AnomID and SigID in terms of its false positive rate and it false negative rates. Consider the false positives that occur in SpecID: what is your definition of a false positive, in what conditions do such false positives occur, and is there anything interesting about the false positives? (10 points)
[answer on back of page]

Name: _____ **USC ID:** _____

2. (30 points) Matching Systems and with Vulnerabilities

For each of the following systems or approaches to security, note the vulnerabilities that remain unaddressed. In particular, tell me what weaknesses remain and might be exploited by an adversary. If a weakness remains in most systems, but either fixes exist that may be deployed, or exploitation of the weakness is dependent upon other factors, then still list the weakness, but circle the number when you write it in the blank.

This is **not** a one-to-one mapping; more than one system may suffer from a vulnerability or weakness 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 a system a vulnerability that does not exist. There are more blanks in the page below than actual correct answers, so you do not need to fill in all the blanks.

1. The Domain Name System
2. SSL or TLS to connect to web sites
3. Network Based Intrusion Detection
4. IPSec
5. Signature Based Intrusion Detection
6. PGP or S/MIME
7. SecureID (or other time varying authentication tokens)
8. Onion Routing
9. SSH (using the users password to login)

a) Modification of returned data: ____ _____ _____ _____ _____ _____

b) Traffic Analysis: ____ _____ _____ _____ _____ _____

c) Man in the Middle: ____ _____ _____ _____ _____ _____

d) System Corruption: ____ _____ _____ _____ _____ _____

e) Encrypted Attacks: ____ _____ _____ _____ _____ _____

f) Spoofing or Phishing: ____ _____ _____ _____ _____ _____

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

h) Stolen Credentials: ____ _____ _____ _____ _____ _____

i) “insider” threats: : ____ _____ _____ _____ _____ _____

Name: _____ **USC ID:** _____

3. (40 points) Design Problem - Security in a Cloud Based File Store

You have been hired to redesign the security mechanisms for a cloud based file service (similar to DropBox). Your main concern is ensuring the confidentiality and integrity of data stored in the cloud. Ideally, files stored in the cloud will only be readable to authorized users, and not accessible to others including employees of the cloud storage company itself.

Files stored in the cloud will be accessed by their owner on various devices, including desktop and laptop computers, smartphones, and from the web. Certain "shared" directories (and the files they contain) may be accessible to selected other users with whom the owner has chosen to share a directory. Files should remain accessible to authorized users on their devices even when the users are disconnected from the network. The owner of a shared file or directory must be able to revoke access to other users that were previously authorized.

a. Define the protection domains in your system. What data is stored in each domain? hat parties will have complete control to read or modify the data stored in each of the domains? (10 points) [note: the answer to part (a) depend on your answer to part (b) and vice versa, so please read question b - and think about your answer to both - before writing your answer to part a]

b. Where will encryption of data be performed in your system, and how will the keys used for the encryption be managed? How will the keys be made available on multiple devices, and how will they be provided to other users authorized to access a directory by the directories owner? (15 points) [please answer on back of page]

c. The requirement that files should remain accessible to authorized users on their devices even when the users are disconnected from the network means that copies of the data must be stored locally on each device. Given this requirement suggest measures that can be taken to prevent an adversary from retrieving data from a device (e.g. a smartphone or laptop) that is lost or stolen. (5 points) Such devices also run other applications, so suggest techniques and technologies that will prevent such data from being accessed (and potentially redistributed by other apps, including malicious code). (5 points) Finally, discuss approaches to balance the potentially conflicting policies allowing access to be revoked to data, while the device storing that data is disconnected from the network? (5 points). (15 points total for question c).