Name: _____ **USC ID:** _____

CSci530 Final Exam

Fall 2013

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. (40 points) Intrusion Detection and Trusted Computing

Please answer the following short questions:

a) Why is signature-based intrusion detection poorly suited for the detection of zero-day attacks? (10 points)

b) What are the strengths of a network-based collector in an intrusion detection system? (5 points)

c) What are the strengths of a host- or application-based collector in an intrusion detection system? (5 points)

Name: _____ **USC ID:** _____

d) What is the difference between attestation and accreditation? (10 points)

e) Explain what it means to "Extend a PCR"? (5 points)

f) What is the function of the "endorsement key", and how do we know that the correct endorsement key was used for the claimed function? (5 points)

Name: _____ **USC ID:** _____

2. (20 points) Privacy and user Tracking

For each of the following techniques used to protect privacy or to breach user's privacy, match them with relevant terms or approaches used to either implement or defend against the technique. 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. Traffic Analysis
2. User tracking
3. Data mining / inference
4. Spyware (including unexpected functions in installed software)
5. Linkability
6. P3P, DoNotTrack, and Privacy Policies

i. Cookie: ____ ____ ____ ____ ____ ____

ii. Anonymization: ____ ____ ____ ____ ____ ____

iii. Onion Routing: ____ ____ ____ ____ ____ ____

iv. User Education: ____ ____ ____ ____ ____ ____

v. Personally Identifiable information: ____ ____ ____ ____

vi. Encryption: ____ ____ ____ ____ ____ ____

vii. Aggregation: ____ ____ ____ ____ ____ ____

viii. User Location: ____ ____ ____ ____ ____ ____

Name: _____ **USC ID:** _____

3. (40 points) Design Problem - Securing your own IT Infrastructure

You have a paranoid streak and have gotten tired of relying on service providers to secure your information. You are no longer willing to depend on someone else the cloud for backup and storage and you are determined to set up your own IT infrastructure to manage your own data. Fortunately, there are now a large number of products available that can assist you in doing just that. Unfortunately, many of these products leave some inherent vulnerability in your resulting system. In this problem, you are going to explore those issues and begin to understand just how hard it is to make your system truly secure.

The requirements for your system are:

i. You will support a file system (or file systems) capable for storing at least 2 TB of data. Some of this data you consider to be highly sensitive (e.g. tax returns, credit card statements), some is critically sensitive such as passwords and encryption keys, while other data is less sensitive, and you will want to ability to share such less sensitive information with other users on the Internet. There will be data of intermediate sensitivity, which you want to be able to access while away from your home, but which you do not plan to share with others.
ii. You require the ability to backup your data, including support for periodic off-site backup of data.
iii. Your home network supports many "appliances" including security cameras, DVR systems such as Tivo, Televisions, Entertainment systems, and home automation systems capable of controlling lights and unlocking doors.
iv. Your network supports multiple home computers, including tablets, smartphones, laptop computers, and desktop computers.
v. You have a single connection into your network through a cable modem, DSL, or FiOS or similar capability, and you will deploy a router and wireless system for your network.

At this point, I could ask the single question, how will you secure this system, and you could write 200 pages and the question would be impossible for us to grade. As such, I can't ask such an open ended questions and instead ask a few specific questions which by no means cover the entire space of options.

a) In designing the network that will meet the requirements about file systems above, how will you protect the critically sensitive information differently than the other classes of information? How will you share the less sensitive information with other users on the internet? How might you support your own personal access to data of intermediate sensitivity, which you need to access when traveling? How will you protect the highly sensitive data, which needs to be readily accessible from your computers when you are at home? (10 points - please place your answer on back of page)

Name: _____ **USC ID:** _____

b) I mentioned that your network will have a router, most likely at the point of connection to the internet, but which is also responsible for forwarding packets among the other devices on your network. Tell me what capabilities you will require on this device, in order to improve the security of your home network as a whole. Please be sure to note that while it will obviously have firewall functionality, there should be a lot more that it does too. (10 points)

c) Defense in Depth - There will inevitably be security vulnerabilities on the devices in your home network. Group the devices into classes based on the impact of a device vulnerability on the security of the system as a whole, explain the impact, and describe how you can reduce the impact (or if aspects of your design above already reduce that impact, explain how it does so). (10 points answer on front and back of page)

Name: _____ **USC ID:** _____

d) System Updates - With all the devices listed above, you are certain to require software updates for many of these devices. Discuss for which devices you are likely to enable automatic software updates, explain any vulnerabilities created by said choice, and how the impact of those vulnerabilities might be mitigated elsewhere in the system. Understand that for some of these devices, you will not be able to change the way updates are processed or validated, but can only enable or disable automatic updates. (10 points)