Name: ______________________ **USC ID:** ______________________

CSci530 Final Exam

Fall 2015

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) IP Security

In class we discussed the capabilities of IP Security as one approach to securing network communication. We also discussed a wide range of technologies that are useful as countermeasures to various kinds of attacks. Although IPSec is not as widely used as it should be, it is interesting to note that it provides security functionality similar to many of the security services discussed as separate mechanisms. In this question you will explain in a couple of sentences how IPsec provides similar functionality to defense techniques implemented using the approach listed in the subequestion. You should also explain the differences in what is provided.

a. Virtual Private Networks (10 points)

b. Secure Sockets Layer (10 points)

c. Host based firewalls (especially as used for policy enforcement)
(10 points – answer on back of page)

2. (30 points) Matching Systems and with Characteristics

For each of the following systems or approaches to security, note the characteristics, terms, or techniques that are related to the approach. Being related includes cases where the approached defends against a particular weakness. This is **not** a one-to-one mapping; more than one system may have a common characteristic. 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 with a characteristic that is incorrect. There are more blanks in the page below than actual correct answers, so you do not need to fill in all the blanks.

1. PGP or S/MIME for email communication
2. IP Sec (or IPv6 Security)
3. SSL or TLS
4. Network Based Intrusion Detection
5. Onion Routing (e.g. TOR)
6. Trusted Computing
7. DNS Security

a) Public Key Infrastructure: ____ _____ _____ _____ _____ _____

b) Traffic Analysis: ____ _____ _____ _____ _____ _____

c) Authentication: ____ _____ _____ _____ _____ _____

d) Confidentiality: ____ _____ _____ _____ _____ _____

e) Protects multiple endpoints: ____ _____ _____ _____ _____ _____

f) Integrity: ____ _____ _____ _____ _____ _____

g) Cache Poisoning: ____ _____ _____ _____ _____ _____

h) Proxy: ____ _____ _____ _____ _____ _____

Name: ______________________ **USC ID:** ______________________

3. (40 points) Design Problem - Security for a Feet of Drones

You have been hired by Amazon to consider security issues surrounding and design security mechanisms for their future fleet of delivery drones. These drones may be used for delivery from warehouses, or they could potentially be used for the last steps of delivery from Amazon vehicles dispatched to a neighborhood. The drones might deliver a package to a designated drop point, or they might require interaction with the customer to confirm delivery. In this question you will be asked to consider requirements, potential threats, and technological solutions surrounding the problem.

a) Analysis of threats (10 points) - What are the potential goals of an adversary for your system. What can they hope to achieve through compromise of the security of your system? There are many more potential attack goals than might appear on first thought. Without much thought I come up with at least five potential goals and there are more than five.

b) Authorized control and access (15 points) - The Amazon drones operate as part of a fleet, and the control of many drones may be managed centrally. At the same time, there are certain limits on operation that may be imposed by air-traffic control systems, or public safety agencies. Localized control is also autonomous, from within the vehicle (drone itself). Discuss the structure of the management and control system that will prevent an adversary from gaining control of a drone. How is the security of your approach impacted by the need to process control information from multiple sources? Describe the technologies you will apply for authentication of control signals. How will keys be managed for such a system? In your design, what happens if unauthorized control signals are received, if control signals are modified, and if control signals are blocked? (answer on back of page)

c) Subversion (5 points) - Is there a risk of subversion in the system or other security compromise resulting from malicious code. Where are the most vulnerable points of subversion in your design and what aspects of the design can reduce the attack surface (the parts of the system) subject to the subversion threat?

d) Authenticated Delivery (10 points) for packages that might require confirmation by the customer that they are present and accepting delivery when the drone shows up above their doorstep, brainstorm and present some thoughts about such an “authenticated delivery protocol” . One hint to guide your thinking concerns the use of nuances in authentication protocols covered in class. (answer on back of page)