Name: ______________________ **USC ID:** ______________________

CSci530 Final Exam

Fall 2016

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) Short Answer

   a. What is the main difference in our focus for security with respect to Critical Infrastructure/Cyber Physical Systems as compared with our focus for security in traditional data processing? Explain why these differences are important. (5 points)

   b. Why is linkability such an important consideration in understanding privacy? (5 points)

   c. List three ways that information is linked in systems that provide inadequate protection of privacy. (5 points)

d. Why do attacks that affect the correctness of name resolution through the domain name system have an impact on security of so many systems? For this and the next question, please do not tell me about denial of service or availability. (5 points)

e. Describe two attacks against the domain name system that impact the correctness of name resolution. (5 points)

f. How does DNSSEC protect the integrity of the name resolution process against the threats you just described. (5 points)

Name: ______________________ **USC ID:** ______________________

2. (30 points) Why is it a Match – Matching for Intrusion Detection

For each of the following kinds of attacks, match the attack with the one or two intrusion detection system characteristics most effective for detecting or responding to the attack and provide a brief (no more than 8 word) justification for your choice(s) 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. You gain a point for a proper explanation of your reason.

1. Insider Threat
2. Zero day attack
3. Malicious code (Virus or Worm, other than zero-day)
4. Attacks on process control and cyber-physical systems
5. Use of stolen login credentials across multiple machines
6. Distributed Denial of Service Attack
7. SQL injection over an SSL protected connection

a) Host based Data Collection: ____ ____ ___________________________

b) Network based Data Collection: ____ ____ ___________________________

c) Signature based: ____ ____ ___________________________

d) Anomaly based: ____ ____ ___________________________

e) Specification based: ____ ____ ___________________________

f) Security Incident Event Management: ____ ____ ___________________________
(SIEM)

Name: ______________________ **USC ID:** ______________________

3. (40 points) Design Problem – IoT – The Internet of Threats

Following last month' s denial of service attack on the Dyn Domain Name System infrastructure, we learned how Internet of Things (IoT) Devices in the homes of consumers can be subverted and used as nodes in a Mirai botnet to attack other systems on the Internet (Mirai is the name of the software used by the attackers to create the botnet). While the effects of this particular attack were felt primarily outside the home network on which the compromised attacks were placed, it serves as a wakeup call for users of Internet of Things devices because such compromised devices can do much worse things if the attacker chooses. In this question you will explore the potential impact of compromised / subverted IoT devices, and propose steps you can take to mitigate the impact of such attacks.

a. Vulnerabilities (10 points) – Discuss some of the characteristics of IoT devices as they are usually implemented and deployed that makes them more vulnerable to compromise?.

b. Impact of compromise (10 points) – List some of the consequences that are possible from an IoT subversion. By this I am asking what are the activities attackers can perform from a compromised IoT device on the typical home network, and how does this affect security. (Answer on back of page).

Name: ______________________ **USC ID:** ______________________

c. Design of IoT Devices (5 points) - If you were hired by a company developing devices that are intended to operate effectively as appliances connected to a home network, list some of the improvements in the design of such devices (i.e. certain requirements for the implementation of these devices) that will reduce the vulnerability of the devices to compromise.

d. Securing your home network (15 points) - There will always been devices you want to use in your home that have not been appropriately protected by their manufacturer, In this question, discuss some of the steps that you can take on your home network to improve the resistance of IoT devices to attacks, and also to improve the security of the rest of your systems against attacks that might be initiated through a compromised IoT device. (answer on back of page)