Name: _____ **USC ID:** _____

CSci 530 Final Exam

Fall 2018

IMPORTANT: FOR REMOTE PROCTORS
Please Scan Both Sides of all Pages
Students have been instructed to answer some questions on the back of the page.

Instructions:

Show all work. This exam is open book, open notes. You may use electronic devices if your references materials are stored on the device, and as long as communication is disabled (e.g. Airplane mode). You may not use your device for communications and you may not use it to retrieve information from the web or from files stored elsewhere. 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**. The exam will be split apart for grading by different people, and if part of your answer for one question appears on a page given to a different grade because the sheet contains parts of the answer to more than one question, then you will NOT receive credit for that part of the answer not seen by the grader. In particular, **each numbered question must appear on separate pieces of paper so that the exam can be split for grading**.

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 Score
Score					

Name: _____ **USC ID:** _____

1. (30 points) Who Said That?

The security of many functions in computer systems is dependent on the ability to verify the integrity of statements made by third parties, second parties (the party with which one is interacting), or one's own statements. This is certainly the case for key management, where a trusted third party makes a statement about a particular key that is to be used. It also applies to attestation, accreditation, and digital signatures. In the questions that follow, I will describe a statement that is made in a system and you are to tell me who made that statement. More specifically, you are to tell me what key is used to protect the integrity of the statement and if there is a specific name for the key that is used, provide that name. You should also make it clear in your answer, who is in possession of the key needed to protect the integrity of the statement.

For example, if I were to ask: The Kerberos ticket tells us what session key has been assigned for use between a particular client and server.

You are to respond that the ticket is issued by the KDC and that the ticket is encrypted using the key shared between the KDC and the server (sometimes referred to as the server key or Ks).

Now, let's begin:

a) A Resource Record Set in DNSSec containing an A record for www.usc.edu

b) The quoted PCR from a trusted platform module provides information about the checksum of the software running in a process.

Name: _____ **USC ID:** _____

c) The DS Record for USC.EDU in the EDU Zone using DNSSec provides the public key signing key for the USC.EDU domain/Zone.

d) Information for the security associations (including session keys and checksums) negotiated during phase 2 of IKE (in IPSec).

e) The Volume Encryption Key stored on a hard drive, which provides the key for decryption of the rest of the data on the hard drive.

f) An SSL or TLS Certificate contains the domain name of a web server and the public key that may be used to verify the identity of the server with the specified name.

Name: _____ **USC ID:** _____

2. Short Answers (30 points)
   a) Viruses and Worms are both self-propagating. Explain the difference in the way that each infects its host. (10 points)

   b) What is the main advantage gained from the use of a host-based firewall vs. the use of a firewall appliance at the boundary of your local area network. (5 points)

c) Privacy (5 points) - Explain some of the ways that an IP address can be linked to a users identity. (note: I expect more than one way to be described).

d) Why is the use of Onion routing in TOR generally more effective at protecting privacy than the use of an anonymizer (a single hop anonymizing web proxy). (It might be useful to answer this by describing the steps an adversary would need to complete in order to breach the anonymity provided.) (10 points)

Name: _____ **USC ID:** _____

3. (40 points) Design problem - Hotel reservations and frequent guest systems

The latest high-profile security breach involved the compromise of the Starwood Hotels reservation and frequent guest systems. (the new has reported this as Marriott, which is technically correct, but Marriott recently bought the Starwood hotel chain and the systems that were affected were the legacy systems from the Starwood chain). You have been hired by Marriott to design a replacement for their reservation and frequent guest systems.

This time around, the number two goal is security. Yes, it would be nice if this was their number one goal, but customer retention and ability to conduct their business operations is usually where their focus will be. As a developer interested in security of their system, you too must recognize that allowing customers to manage their accounts and make reservations online means that you cannot secure their system by taking it off the network. The more access you give to customers, the more opportunities an adversary will have to break in (i.e. you have increased the attack surface).

Among the specific security requirements that are in place for the system you will design are the need for effective tools to detect security breaches, and the ability to limit the extent of a breach (how much and what kind of information is stolen) if a breach occurs. Also of concern are the steps you would take to prevent a successful breach.

a) The Data Architecture (10 points)

What are the kinds of data managed by a hotel reservation system, a frequent guest system, and the information kept about guests at individual hotels (note that there is more information kept about some guests than others - e.g. for some customers, passport information may have been compromised). For each type of information, indicate who should have access, and from where access might be made. Finally, suggest a set of protection domains within the hotel network and describe the placement/storage of data within those domains to improve your ability to provide appropriate protection to the different classes of data.

Name: _____ **USC ID:** _____

b) Identity Management (10 points)

Who are the users of the system? Do users fall into different classes? If so, what are the classes? Suggest the technologies that you recommend for authentication of users in the system. This may involve different technologies for different classes of users. What are the advantages (and disadvantages) of using a particular technology for a particular class of users.

c) Protection at the boundaries (10 points)

Suggest policies that can be enforced at the boundaries between the protection domains described in (a) to prevent large scale exfiltration of data, and to prevent infiltration/subversion of systems on the inside. What technologies will be most effective in enforcing the policies that you describe. (answer on back of the page)

Name: _____ **USC ID:** _____

d) Intrusion detection (10 points)

Although the Starwood breach was only recently discovered, it is believed that the breach dates back to 2014. This highlights the need for effective intrusion detection, which apparently was not in place. Please suggest the approaches (plural) that you will take to intrusion detection in the system you recommend deploying. From what locations will data be collected, where will it be stored, how will it be analyzed (i.e. what techniques and approaches will be used). How will the approaches you suggest allow you to stop an attack while it is ongoing, how will the data collected help you determine the extent of an attack (e.g. what systems were affected and what data was taken or modified) if discovered after the attack is complete, and how might this data help you with attribution of the attack (determining where it came from and who is behind it). We understand that no system is perfect, and you will not achieve all of these goals, but we want to see your approach.