Name: ______________________ **USC ID:** ______________________

CSci 530 Final Exam

Fall 2017

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 questions 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. (35 points) Short Answer:
   a. Explain how the use of IPSec to protect the confidentiality and Integrity of communications between a web browser and a web server differ from the use of SSL (or TLS). In answering this question, assume you are using only one method - even though one could employ both. In you answer, be sure to discuss key management issues and identify the end-points that are authenticated. (10 points)

   b. Which type of Firewalls are least vulnerable to subversion by malicious code (note that there are several that you should list). Explain why these types of firewalls are less vulnerable in terms of the attack surface that they present. (you may want to start by enumerating - for your own benefit - all the firewall types discussed in class and then consider each type. This enumeration is not part of the answer, but it will help you to organize your own thoughts and avoid leaving out important considerations). (10 points - Answer on back of sheet)

Name: ______________________ **USC ID:** ______________________

c. Effective phishing attacks require that the victim connect with a malicious site while they think that they are connecting to a legitimate site. Describe as many ways as you can think of for a criminal to direct users to a phishing site. For each approach, what are the conditions that must be present for the redirection to work (example, will the redirection work for SSL/TLS protected connection, or only for unencrypted connections). (10 points)

d. List the reasons that a purely network based intrusion detection system may be less effective than approaches that incorporate host and application based data collection. (5 points – Answer on back of sheet)

Name: ______________________ **USC ID:** ______________________

2. (30 points) Slightly Longer Answer:
   a. Attestation – Explain how a remote process can verify the authenticity and identity of the components of the software stack (from BIOS through application) on a computer that implements trusted computing technologies. In answering, you may assume that the remote process already knows what software it expects to be running, we are only concerned with verifying the claim. Be sure to identify the steps that occur on both sides of the communication, i.e. at the remote process, and on the computer whose software is being validated. (15 points)

   b. One limitation with traditional PKI (Public Key Infrastructure) as commonly deployed in today's systems is how to decide which identities (or names) a particular CA (Certification Authority) is authorized to certify. This is why we have so many "root certificates" in our browsers, and why most domains (host names) are considered authentic if certified by any of the root CA's whose keys we know.

      Explain why this would be less of a problem when using the certification hierarchy present in DNSSEC? (15 points - Answer on back of page)

Name: ______________________ **USC ID:** ______________________

3. (35 points) Design problem - Bitcoin

The value of bitcoin (BTC) has increased dramatically in the past month. With greater acceptance of bitcoin, bitcoin balances have quickly become a target for thieves. Bitcoin is a form of "notational money" meaning that the balance of account (in bitcoin) is recorded in a ledger, and value changes hands when signed instructions to move funds are added to the public block chain. These instructions are effectively signed by the private key of the account, and the account is named and identified solely by its corresponding public key. With respect to security, a chief downside of this approach is that discovery of the private key of an account gives complete access to the funds in that account, which can be readily transferred to a different account. Therefore protection of the private key is critical.

A) Privacy - How private are bitcoin transactions? How difficult is it to follow the flow of funds from one account to another? Discuss some of the ways that we can discover the owner of a Bitcoin account. Suggest some steps that bitcoin users can take to hide their identity. (10 points)

B) Theft from Bitcoin Wallets - As mentioned earlier, preventing theft from Bitcoin wallets is an important issue that needs to be addressed with the use of Bitcoin. Explain some of the approaches through which criminals are able to steal funds (effectively all funds) from a particular bitcoin account. (10 points - Answer on back of page)

C) Protecting the private key – One approach to protecting the private key is to use a special hardware device (you should suggest/list several kinds of devices that can be used) to generate the public private key pair, and for the device to use the private key internally for transactions, but for it never to send this private key outside of the device. List one serious shortcoming of this approach, and then suggest some modifications to the approach that will improve its applicability for protecting the private key of a bitcoin account. (15 points)