Name: _____

CSci 530 Final Exam

Fall 2019

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: _____

1. **(30 points) Fill in the blank** or short answer:

    a. Authentication is to Attestation as _____ is to Accreditation. (5 points)

    b. Where will you find the storage root key and what is it used for? (10 points)

    c. What part of an IPSec implementation corresponds to the firewall rules that specify which address ranges can communicate through the firewal. Explain your choice and how they are similar? (5 points)

    d. List some of the reasons that inclusion of host and application-based data collection in an intrusion detection system allows the detection of certain kinds of attacks that might be more difficult to discover when using a purely network based system. (10 points – answer on back of page)

Name: _____

2. **(30 points) Slightly longer answer**:

a) Discuss the approaches by which an adversary can modify the software that runs on a computer system. For each of these approaches (commonly referred to as a subversion vector) explain when the change is made to a system, which part of the system is affected, how it is accomplished, and techniques that may be used to detect or prevent such changes. (10 points)

b) Names are important to security. There are many attacks that can be facilitated by an adversary who can change the mapping or binding of names to other types of data. List places where names are used in ways that affect the security of a system. There are multiple places where this occurs. For each, explain the mapping that occurs: a) what is the name; b) what is it mapped to or bound to; c) how is the security (integrity, and if relevant, confidentiality) of the mapping provided; and d) what are the consequences if this security is not provided.
(20 points – answer on back of page)

Name: _____

3. (40 points) Design Problem – Information Technology (IT) in your home

The FBI recently issued a warning regarding smart televisions: "*A bad cyber actor may not be able to access your locked-down computer directly, but it is possible that your unsecured TV can give him or her an easy way in the backdoor through your router*." We have also seen many recent reports in the news of ring doorbell's, Nest Thermostat's, and other security cameras that have been compromised and used to harass, frighten, or extort individuals in the home. These events should serve as a wakeup call that we need to do a better job securing our home IT. In this question you will explore the potential impact of attacks on your home IT and propose steps you can take to mitigate the impact of such attacks.

a. Inventory – Provide an inventory of common information technology devices in the home. What are the devices to be protected, what data is accessible from these devices, and who is supposed to have access to that data? (5 points)

b. Discuss the ways that adversaries can compromise the devices and data on/from our home network. For the different the kinds of devices, tell me which approach is likely the most common (This calls for speculation based on what you have learned this semester, or on news reports you have seen. You will not find this in our lectures). Note that there will be many kinds of attacks that are possible. Do not list or focus on just one.
(10 points – answer on back of page)

Name: _____

c. Impact of compromise – List some of the consequences that are possible from attacks on our IT at home. By this I am asking what activities attackers can perform on/from a compromised IoT device or the consequences of data that might be retrieved or changed on any device. (5 points).

d. What changes to the security features on home IT devices might help to prevent or mitigate the impact of these attacks? More specifically, what should be done in the implementation or operation of these devices to make them more secure? Some of these changes might be implemented by the vendor, other changes might be to the way the devices are operated or configured by the user. (10 points – answer on back of page)

Name: _____

e. Architecture – Discuss the containment architecture (layout of protection domains) in a home network and how your suggestions (how you think the domains should be structure) regarding this architecture would affect the impact and/or success of the attacks we have been describing. (10 points)