Name: _____

INF 523 Midterm 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 a computer to view materials that you previously stored on your computer, but all communications must be disabled (e.g. Airplane mode). This means you can not use the web, D2L, Blackboard, or obtain files from Dropbox or similar services during the exam. You have **100 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: _____

1. Testing –

a) Why might static testing based on automated source code analysis using "lint-like" tools be ineffective against an intentionally inserted vulnerabilities in a system (i.e. a subversion). Note that there is more than one reason. (5 points)

b) Which test techniques or tools (as discussed in our lecture on testing) are more effective at discovering previously unknown vulnerabilities? For each technique you list, explain why it might identify unknown vulnerabilities. (5 points)

c) For each of the following test techniques, explain why it might be more effectively applied when the tester has knowledge of the implementation of the system being tested (e.g. in a white-box test):

i) Fuzzing (5 points)

ii) Penetration-testing / red-teaming (5 points)

(answer i and ii on back of page)

Name: _____

2. Please recall our discussion of Trusted Computing from Computer Science 530. In our discussion from 530 we covered how the hardware based **trusted platform module** (TPM) provides **attestation**. Specifically, the TPM maintains a running checksum (called a **measurement**) of the full software stack from the BIOS through the hypervisor (if present), the operating system, and the application, and it stores this value in **a platform configuration register (PCR)**. The TPM can then digitally signs the value of the PCR and that signed value can be used by the application in protocol exchanges with remote entities. Additionally, the TPM can compare the value of the PCR with acceptable values stored with other encryption keys to decide if those keys can be unlocked for use by an application, or applied to decrypt other data within the TPM itself.

Next, consider our discussion of secure distribution and secure update from this semester. Specifically, consider the use of digital signatures in the proper way to manage distribution and updates from that discussion (it should be in your notes). Consider also tools like tripwire and AFIK that also use checksums (bot not necessarily digital signatures) to determine whether software has changed after installation or legitimate updates.

In this question you will explain the differences in the assurances provided by (i) Trusted computing and the TPM, (ii) Digital Signatures used in software and update distribution, and (iii) tools that detect changes like Tripwire and AFIK? In providing your answer, be sure to tell me:

a) (10 points) **What entity provides the assurance (e.g. the attestation or statement)** and how the placement of the entity affects our confidence in the findings. In answering, consider how resistant the entity providing the assurance statement is to subversion itself.

b) (10 points) **Also tell me to whom such assurance statements are provided** (i.e. who is protected, e.g. a remote system, the local administrator, or is the assurance that condition on access to data will be followed, e.g. the assurance is provided to the owner of data). (answer on back of page)

Name: _____

c) (15 points) Also tell me differences or similarities in the kinds of attacks/changes that might be detected (e.g. virus, worm, trojan horse, changes installed by an attacker), and more specifically **the timeline of when changes are made by an attacker that might result in detection**, and which might go undetected.

Name: _____

3. Scenario – **Implantable Medical Devices –** You have been hired by a medical device manufacturer to asses the security of a series of **medical device**s to be **implanted in patients** to monitor and control certain aspects of their heart. Fortunately, you have joined at the early stages of their design and you are also expected to provide concrete suggestions to improve the assurance possible for their control architecture.

The system that is under design collects and stores data about the operation of the patients heart, **and allows that data to be read by physicians**. The system will also monitor the data in real time and based on the analysis of that data it may deliver electrical impulses to interrupt and correct dangerous conditions that might arise. Unfortunately, the rules that are to be followed for the real time analysis and the corrective actions are not known at the time the device is implanted, and therefore **certain aspects of the programming must be updated after the device is implanted**. This process **requires communication** with **other computer systems managed by the physician** and the **device manufacturer**.

Given the description of the system, and the parts of the system described earlier,

a) Create a data flow diagram (DFD) for the system. Remember that trust boundaries are shown in the DFD, and you can make recommendations about the placement of those boundaries (advising on the design of the device) by your placement of those lines (or the placement of the other components with respect to those lines), so try to place them in places that make sense from a security perspective, but that also make sense from a practical implementation perspective. (10 Points)

b) Create an attack tree for the system. What might be possible end goals of an attacker (hint: it might not always be to kill the patient)? Make sure your tree shows how such goals might be achieved. Start the attack tree with your general understanding of possible goals and capabilities of an adversary, but you may come back to add to this attack tree after (or during) your completion of question 3c. (10 points answer on back)

Name: _____

c) List the potential weaknesses in the system according to the STRIDE model as applied to the DFD created in 3a. (10 points)

d) Defending the system – List some of the techniques and defensive measure you could apply that will result in improved arguments for assurance in the system. Please be sure to include among these techniques those that are 1) architectural – relating to the interaction of components of the system (and the conditions under which some of those interactions may occur), 2) software based – relating to the structure of software and the programing of the components, and 3) technological – specific technological techniques or components that can be applied to improve the security and assurance of the system. (15 points) (answer on back).