Name: _____ **USC ID:** _____

INF 523 Midterm Exam

Spring 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**. 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:** _____

Mobile Device Assurance - After shocking revelations that despite Apple's claims to the contrary they can actually break the security of the encrypted storage, you have been asked to assess the assurance of the current generation of iPhones and to suggest changes that would improve the assurance of the device.

It is interesting to note that the vulnerability present in the iPphone 5c which law enforcement seeks to exploit falls squarely in the realm of realm of assurance. Here is what we know:

Farook's phone, issued by San Bernardino County for his use as a county employee, was uploading data to a cloud account until about six weeks prior to the shooting. Some of this data was made accessible to law enforcement when requested with an appropriate order. Backups of other data on the phone are uploaded to the cloud and it is not certain which of that data is accessible. At issue in this matter is the data on the phone itself, including location data, and data from communications apps, when such data was not stored in the iCloud account.

The iPhone encrypts data in its memory, using AES encryption with a key that is derived in part from a random key stored on the phone, and in part from the users passcode which is usually a 4 to 6 digit number (although users can configure their phone to use stronger passcodes). While it would seem that one could try these 10,000 to 1,000,000 passcodes to decrypt the data, this is not the case because of the combination with the random key stored on the phone. The operating system on the phone itself must be used to derive the key used to encrypt data, and the phone is set up to erase the random part of the key if the wrong passcode is entered 10 times.

The government wants Apple to provide them with a new version of the software for the phone that is configured to 1) run only on Farook's device, 2) bypass the auto-erase capability after 10 incorrect attempts, and 3) eliminate the intentional delays between password guesses. There are other changes that have been asked for which are less relevant to this question. For new software to be installed on the phone it must be signed by Apple.

Assurance is evidence that a system strongly and reliably enforces a security policy. In assessing assurance for the iPhone **you are to consider the policy that data from the phone should be accessible only to the user of the phone.** In this case, that is Farook. I am not asking you to comment on whether that is the correct policy, simply use that as the policy for the basis of your assurance arguments.

Please answer the following questions:

Name: _____ **USC ID:** _____

1. Threat modeling - (40 points) Given the policy described earlier,

a) Describe the classes of adversaries who might try to defeat the policy. I am asking that you group the adversaries into classes based upon their access to different parts of the system such as physical access to the device, access to servers, access to monitor data on a network, as well as any special capabilities the class of adversary might possess

b) Create an attack defense tree for access to data from the phone by an unauthorized user. Consider both access to data which has been uploaded to the cloud as well as access to the data on the phone. Be sure to consider the defensive steps taken by Farook himself among the defense mechanisms. The attack defense tree should use values of 0 and 1 only. You do not need to assign values for cost or likelihood. (answer on back of page).

Name: _____ **USC ID:** _____

2. Stride and DFDs (40 points)

a) Create a data flow diagram for the system described above.

b) Apply the STRIDE model to identify threats in the system described above (and as illustrated in the data flow diagram you just provided). (Answer on back and on additional pages.)

Name: _____ **USC ID:** _____

3. Layering (30 points)

Note that the ability to update software on a phone is a functional requirement that must be retained - so you cannot answer this question by simply requiring iOS to be fixed for the life of the phone. In answering this question, consider (hint) that the software update process for the current iPhone 5C appears to allow changes to passcode security measures if the new code is signed by Apple.

a. Describe the TCB boundary of the iPhone 5C with respect to the policy it is supposed to enforce as described earlier. Describe the characteristics of iOS on this phone in terms of desirable characteristics that allow for stronger arguments of assurance.

b. Suggest changes to the software architecture of the iPhone that would improve the assurance arguments that could be made regarding the phone and its software. These changes should still allow for updates to the phone operating system, but retain assurance with respect to the policy to be enforced by the phone (as described earlier). Describe the characteristics of iOS on this new phone in similar terms as for part (a) and explain how the new architecture exhibits stronger assurance than the original 5C architecture.
(Answer on back of page)