Name: _____ **USC ID:** _____

INF 523 Final 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:** _____

1. Minimization - (40 points) [Read all parts of this question before writing so that you can answer each part in the appropriate section of your response]

   a) What do we mean by minimization? In general words (i.e. not specific to a particular system), what are the things that are being minimized? (10 points)

   b) Provide Examples of minimization in each of the following systems, and where appropriate also provide examples of lack of minimization: (20 points):

      Trusted Computing
      Apple iPhones
      GEMSOS and Garnets
      Windows 10
      Linux

      (answer on back of page, and additional pages if necessary)

Name: _____ **USC ID:** _____

c) How does the correct application of minimization to the design and implementation of a system affect its assurance? Give examples of why our assurance of some systems is stronger than others based on whether the system is minimal or not. (10 points)

Name: _____ **USC ID:** _____

2. Channels and the cloud - (35 points)

a) Why are covert channel attacks and side channel attacks so much more of an issue for cloud computing than they are in traditionally isolated systems? Provide examples of such attacks in the cloud. (10 points)

b) Why is covert channel analysis only useful in a system that uses MAC? In what case can covert channel analysis be used in a system that uses DAC? (10 points)

c) Explain the difference between the two types of covert channels (be sure to name the types and provide examples in explaining the difference). Provide an example of each of the kinds of channels in a side channel attack.
(15 points - answer on back of page)

Name: _____ **USC ID:** _____

3. Testing and Verification - (25 points)

a) You have been hired to perform assurance testing for an embedded medical device like a pacemaker. The functional specification of the device requires that data be readable via a wireless monitor, and that certain changes to its configuration are also possible through this external device. Identify the different parts of the system that might need to be tested and the interfaces (and limitations on those interfaces) between those parts of the system that lead to a more securable system. (5 points)

b) In order to provide a comprehensive security evaluation for the device, you should test for all types of attacks against that device. Explain how to choose the order of execution for your test cases? (5 points)

c) Why do some security evaluation criteria require more rigorous assurance arguments to achieve higher assurance levels? Give an example for such a requirement. (5 points)

Name: _____ **USC ID:** _____

d) For each of the following testing or verification tools, identify if they are a white box technique, a black box technique, or both. Explain your choice in a single sentence. Finally, for each form of test, explain in a few words what you might learn from such a test - i.e. what kinds of vulnerability might be uncovered. Also explain which parts of the system would be subject to such a test. (10 points)

Identify whether each of the following testing or verification tools are white box or black box tests, or both? Circle the answer and explain in 1 sentence.

i) Fuzzing (white, black, both)
Why?
What Parts?
What will you learn?

ii) Formal Verification (white, black, both)
Why?
What Parts?
What will you learn?

iii) Static Testing (white, black, both)
Why?
What Parts?
What will you learn?

iv) Penetration Testing (white, black, both)
Why?
What Parts?
What will you learn?

v) Vulnerability Scanning (white, black, both)
Why?
What Parts?
What will you learn?