Name: _____ **USC ID:** _____

INF 523 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. **(20 points) Matching -** For each of the following numbered words or phrases match the word or phrase with the lettered characteristics or terms with which it is associated. This is **not** a one-to-one mapping. So more than one numbered word of phrase may match a characteristic or term, and a single characteristic or term may also match more than one phrase. We are looking for specific characteristics and terms, for which you will receive credit. If you list what is a minor characteristic, while you will not lose credit, you will not get credit either. You will lose a point if you associated a term with a characteristic that does not apply to the method. There are more blanks in the page below than actual correct answers, so you do not need to fill in all the blanks.

    1. GEMSOS Mandatory Access Controls
    2. GEMSOS Discretionary Access Controls
    3. GARNETS Fie System
    4. Sun Network File System on Linux in the Subversion Case Study
    5. Linux Network Stack in the Subversion Case Study

    a) Inside the Trusted Computing Base boundary

    _____ _____ _____ _____ _____

    b) Inside a verified kernel

    _____ _____ _____ _____ _____

    c) Untrusted

    _____ _____ _____ _____ _____

Name: _____ **USC ID:** _____

2. Short Answer (55 points)
   a) List several vectors for subversion of computer systems and several techniques that limit the susceptibility of system components to subversion. (15 points).

   b) Explain how "guard" technologies prevent the exfiltration of sensitive data from a network even when system high components on the network might be subject to subversion (10 points)

Name: _____ **USC ID:** _____

c) Explain the process of "fuzzing" as an approach to testing systems. What kinds of vulnerabilities is fuzzing most likely to detect and what is it least likely to detect? Explain why. (10 points)

d) Covert Channels - Give an example of a timing covert channel. Give an example of a storage covert channel. Explain the meaning of non-interference when applied to cover channel analysis and modeling. (10 points)

e) Formal Modeling - Explain why a system (e.g. a security Kenerl) that has passed formal verification might not be 100% secure. (10 points - Answer on back of page)

Name: _____ **USC ID:** _____

3. Security Kernels for Critical Cyber-Physical Systems (25 points)

a) A common theme throughout this class has been minimization. Our assurance arguments are improved if we can minimize the amount of code within the TCB, and well designed systems will have several concentric TCB's each of which enforces specific policies, the more critical the policies, the smaller the TCB. For example, a system might have a security kennel that to enforce more fundamental security policies, and that kernel may be embedded within a slightly larger operating system that enforces more complex policies. Provide as many examples as you can think of from class (including the student assurance presentations) for these "security kernels", i.e. components that do less, but provide the foundation of assurance for larger systems. In some cases they have been referred to as security Kernels, but in other cases they go by different names. (5 points)

b) When considering critical cyber-physical systems such as a power plant, a medical device, or a vehicle or aircraft, suggest some of the policies that should be enforced by these "security Kernels". Explain why these are the right set of policies to be enforced within this deepest part of the system. (10 points - Answer on back of page)

Name: _____ **USC ID:** _____

c) We have seen several instances of subversion through software upgrades. Consider the implications of such "upgrades" in critical cyber-physical systems. Suggest how the structure of the system, and in particular, the implementation of minimization and the policies enforced within these "security kernels" can mitigate the impact of such subversions. Provide examples to illustrate your arguments. (10 poins)