INF 523 Final Exam

Fall 2018

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 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					

1. Short Answer (40 points)
   a) Assume that we have evaluated assurance evidence for an operating system and found that we are satisfied with level of assurance provided. Explain how we can be sure that the software to be installed on a computer (including the operating system) is the same software and version for which those assurance arguments applied? (10 points)

   b) Explain how MAC and DAC policies are enforced in GARNETS despite the code for GARNETS being untrusted. Please provide sufficient detail regarding access within the untrusted GARNETS components. (10 points)

   c) Suggest reasons that a system like the Sun Network File System (NFS) running over linux was so vulnerable to the subversion (insertion of the artifice) in the NFS Subversion case study. Suggest characteristics of systems that might make them less vulnerable to this kind of attack.
   (10 points – answer on back of page)

   d) Explain the difference between a "side-channel" and a "covert timing channel".
   (10 points – answer on back of page)

2. Slightly Longer Answer (30 points)
   a) Why is it that a system whose security model has been formally verified might still exhibit vulnerabilities? Consider the existence of covert channels as an example when answering this question. (15 points)

   b) For which packets is the crypto-sealing of a label critical and why? Under the Crypto Seal Guard Architectures, which devices are considered trusted? (15 points – answer on back of page)

3. Assurance for next generation telecommunication systems (30 points)

   You have been hired to perform an assurance evaluation for candidates for next generation telecommunications networks (5G). You are to focus your evaluation on the infrastructure side of such systems, but you are still to consider how changes to the application architecture on such devices can affect the assurance requirements for the infrastructure as well. It is critically important that in assessing assurance for such a system you consider the insider threat that might be present within infrastructure providers (services, or hardware or software vendors).

   a) Create an attack-defense tree for the telecommunications network. Be sure to consider all the possible goals of an adversary. For defensive technologies in your AD tree you may consider changes to the end devices including calling and communications apps that might mitigate some of the attacks. Be sure to highlight potential threats that you might NOT be able to mitigate through changes to the end devices and describe the impacts that might result from a successful attack. (10 points)

b) Provide some examples of subversion to which the described system might be vulnerable. Discuss both the operational impact (what policies might be violated) as well as possible activation methods, and what the system might do (or not do) upon activation. (10 points)

c) Describe some of the requirements you would advise be placed on the hardware, software, development processes, distribution, operation and maintenance of the system to strengthen the assurance arguments that can be made about the system once it is deployed. (10 points – answer on back of page)