Name: _____

INF 523 Final 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 **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 on each page**.

There are **100 points** in all and **2 questions.**

	Q1	**Q2**			**Total Score**
Score					

Name: _____

1. Short and long answer.

   a) (10 points) When guards are used to restrict access to citations in the RECON database: i) where is the cryptographic checksum generated; ii) to which citations is it applied; iii) where is it checked or validates; iv) what is it checked for (i.e. what is validated); and iv) what is the behavior that occurs if the check that occurs in item (iv) is valid, and what happens if it is not.

   b) (10 points) When considering confidentiality, covert channels are eliminated if processes running with a low clearance can't be affected in any way by data or processes with a higher security label. What is this principle called and provide examples of some of the affects that might be exploited to create a covert channel?

   c) (10 points) When covert channels are known to exist, what are the steps that we can take to mitigate the impact of the channel? (answer on back of page)

Name: _____

d) (20 points) Explain some of the steps that can be taken at various stages of the software development lifecycle to prevent subversion. Be sure to consider steps at the design, implementation, distribution, installation, and maintenance phases.

e) (10 points) Explain the role of minimization in providing stronger (or additional) assurance arguments regarding the security of a system. In answering this question, provide examples where minimization allows for stronger assurance arguments and explain why. Also provide examples where lack of minimization can make a system more difficult to secure. (answer on back of page)

Name: _____

f) (10 points) The TCB of a system defines those components on which the correct enforcement of policy depends. As a result, the TCB boundaries are dependent upon policy, and a single system might have different TCB boundaries for different policy sets. Describe the different boundaries of the TCB for the two policy sets implement in GEMSOS. By this I mean that you should describe each policy set and for each describe where the TCB boundary lies.

Name: _____

2. Assurance for Cloud Storage (30 points)

   You have been hired to advise a new startup 523box.com on the design of their new cloud storage service. You have been asked to consider alternative designs and to explain which designs will provide stronger assurance to end users, convincing the end users that the service will keep their data secure. Fortunately, you have taken the Information Assurance course at USC (it is purely coincidental that the number of the course is part of the name of the company for which you are now working). You remember the importance of minimization from your assurance class, and you believe that your assurance arguments will be stronger if you have a minimized TCB. What you might not have learned is that it is not just the size of the TCB that matters, but your confidence that it is free from subversion, and that might depend on how much control the end user has over the TCB itself.

   a) (10 points) What are some of the security policies that might need to be implemented by a TCB for the cloud storage service that 523Box will deploy? As a hint, consider CIA. For each of the policies you suggest, succinctly state what that policy means in terms of the 523Box cloud storage service.

Name: _____

b) (20 points) For each of the policies identified in part (a), discuss alternative placements of the TCB boundary in a system that correctly enforces the policy you have identified. For each alternative, discuss how minimization and the selection of components that are part of the TCB affects the assurance that the system can meet the policy as viewed by the end user of the system. Explain also what technological features (in your design) support the placement of the TCB boundary in a way that meets the policy objective.

[A few notes to help you with this: for this question, you will multiply the number of policies from (a) by the number of alternative TCB boundaries you suggest, and you will answer that many times – therefore if you had 5 policies and 4 alternative sets of boundaries, you would answer how the system correctly enforces the policy and the technological features 20 times. Fortunately, you will likely have fewer than 5 policies and probably no more than 3 sets of boundaries. A second note, unlike GEMSOS, the TCB boundaries might not be subsets of one another, they could be disjoint. Spend some time thinking about these hints…]