Name: _____ **USC ID:** _____

INF 523 Midterm Exam

Fall 2018

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** 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. Testing –

a) Why is fuzzing as a test technique likely to be ineffective against an intentionally inserted vulnerability in a system (i.e. a subversion). (5 points)

b) Which test techniques or tools (as discussed in our lecture on testing) are more effective at discovering previously known vulnerabilities? For each technique you list, explain why (5 points)

c) Which test techniques (as discussed in our lecture on testing) are at least partially effective at detecting a buffer overrun. For each technique you list, explain how it is effective. (10 points)

2. Many techniques that improve assurance in systems are related to the concept of minimization. Consider our discussion of structured design and the preference for "low coupling" and "high cohesion" in decomposition and modularization of a system. Consider also our use of information hiding and data abstraction. What is being minimized through the use of these concepts, and why does that result in a system about which we can make stronger assurance arguments? (20 points - answer on back of page)

Name: _____ **USC ID:** _____

3. Scenario - **Vehicle Control Systems –** After the movie “fate of the furious” hit theaters we saw much greater interest in issues surround assurance of vehicle control hardware and software. You have been hired by a new vehicle startup Alset to asses the security of a vehicle they plan to place into production. Fortunately, you have joined at the early stages of their design and you are expected to provide concrete suggestions to improve the assurance possible for their control architecture.

The system that is under design collects information from video and other ranging sensors, plus information from the engine, wheels and steering, and generates inputs to brakes, motors, and steering. The vehicle is also able to communicate with other nearby vehicles, and through other networks to communicate with the manufacturer and owner, and it may be able to accept over the air updates to the vehicle control system. There may be multiple “busses” on the vehicle, essentially vehicle area networks, over which communication between subsystems occur (e.g. vehicle control system to motor, vehicle control system to brakes, etc).

Given the description of the system, and the parts of the system described earlier,

a) Create a data flow diagram (DFD) for the system. For simplicity assume the on vehicle components are brakes, motor, video cameras, tires, steering wheel, dashboard displays, dashboard sensors (the vehicle controls/switches), and the vehicle entertainment / communication system. Consider off-vehicle components as other vehicles in close proximity, inputs to the vision sensors (e.g. signs, lights, etc), and computers reachable through the communications network including the manufacturer, cloud services used by the owner of the vehicle, and the owners personal communications devices, which might connect to the entertainment system through bluetooth connections. Remember that trust boundaries are shown in the DFD, and you can make recommendations about the placement of those boundaries (advising on the design of the vehicle) by your placement of those lines (or the placement of the other components with respect to those lines), so try to place them in places that make sense from a security perspective, but that also make sense from a practical implementation perspective. (15 Points)

Name: _____ **USC ID:** _____

b) Create an attack tree for the system. What are the end goals of an attacker? Make sure your tree shows how they might be achieved. Start this attack tree with your general understanding of the possible goals and capabilities of an adversary, but you may come back to add to this attack tree after (or during) your completion of question 3c. (15 points)

c) List the potential weaknesses in the system according to the STRIDE model as applied to the DFD created in 3a. (15 points – answer on back of page)

Name: _____ **USC ID:** _____

d) Defending the system – List some of the techniques and defensive measure you could apply that will result in improved arguments for assurance in the system. Please include among these techniques those that are 1) architectural – relating to the interrelation of components of the system, 2) software based – relating to the structure of software and the programing of the components, and 3) technological – specific technological techniques or components that can be applied to improve the security and assurance of the system. (15 points)