Directions: Collaborate with the same group members you had before. Problems take long to read but can be answered very concisely (all in a few lines). They are meant to make you think. Don’t worry if you can’t solve them all, but put down your ideas. Write up your solutions as a PDF file and follow the instructions from last time to upload your homework.

1. Computer Security: Stefan Savage’s lecture on security was on spam but was prefaced by a statement that “security is not extra functionality but an attitude towards any functionality. We must think the way the bad guy thinks and see how her or she could misuse the system and then look for countermeasures”. For example, you may be tempted to leave your keys in the ignition and jump out of the car to buy a burger with your door unlocked. However, realizing a bad guy could drive off with your car makes you want to lock the car. Similarly, we want you to try and work through some implications of this statement for the following two computer examples.

A. Email security: Let’s assume you have a secure password to your Gmail account. However, you tend to keep your computer on in your dorm room and leave the email on the screen.

– How could a bad guy exploit your habits?

– Assuming that many people tend to do this, how could a software designer of an email program add some defense against such attacks from the bad guy.

B. Cardiac Defibrillator: A cardiac defibrillator is a device that is implanted in some heart patients that can send some “good” shocks to restore a potentially fatal heart rhythm back to normal. However, the defibrillator allows wireless signals to be sent to it by say doctors before surgeries that can control the intensity and duration of shocks.

– Imagine a head-of-state that is known to have such a defibrillator at a reception. How could Dr. Evil potentially manipulate this device?

– How could the person designing the defibrillator or writing software for the defibrillator processor add some defense against such attacks from Dr. Evil.

2. Distributed Algorithms: Keith Marzullo’s lecture on distributed algorithms described two simple almost puzzle-like problems called the Two Generals problem and the Byzantine Generals Problem that have profound implications for reliability and security. As in the case of security, reliability is an attitude that affects how you think of all functionality, especially in distributed systems. In these exercises we ask you to think through some relatively simple implications of what you heard.

A. Two generals and ATM machines: You want your ATM to give you $100. Your ATM has two separate processing steps: it must record a debit for $100 and it must give you the cash. By the two generals problem, it cannot do both at the same time. It can do these steps in either order and a crash can occur any time.

– Suppose it gives you the cash first. What can go wrong?
- Suppose it does the debit first. What can go wrong? How might the problem eventually be fixed.
- Based on your analysis, which option would banks choose.

**B. Byzantine Generals:** Consider solving the Byzantine Generals Problem with 1 one commander and 3 lieutenants. As usual, we want all loyal generals to agree on whether to "attack" or "retreat", and, if the commander is loyal, then the loyal lieutenants agree on the commander's command. We assume that no more than one general can be a traitor.

In this solution, first the commander sends its command to the lieutenants. We call this the first round. Once a lieutenant gets a command from the commander, it forwards what it heard from the commander to the other lieutenants. We call this the second round. So, at the end of the first round, each lieutenant has received one command (from the commander) and after the second round, each lieutenant has received three commands: the one from the commander, and one forwarded by each of the other two lieutenants. Since a command is either "attack" or "retreat", at least two of the commands will be the same (Of course, a traitorous general could send some random command, like "ice cream", or even fail to send a command. If this happens, we'll treat it as if it had sent "retreat"). Have each lieutenant decide on the majority command. For example, if it receives "attack" from the coordinator and "retreat" from the two lieutenants, it would decide on "retreat".

- Suppose that a lieutenant decides on the command it receives directly from the commander. Show how doing this could lead to erroneous behavior.
- Consider the case we gave above: a lieutenant heard "attack" from the commander and "retreat" from both lieutenants. Show that in this case that the commander is a traitor and all three lieutenants agree on "retreat".
- Consider the case where a lieutenant heard "attack" from the commander and from one lieutenant, and "retreat" from the other lieutenant. Show that either the commander or the lieutenant that said "retreat" is a traitor, and that all loyal generals decide on "attack".