Week 1 Questions

Lecture 1

1. Personal security, computer security.
2. The common thread in security is that it is the protection of some asset against threats. Those assets could be data, software, your possessions, or even your life.
3. Yes, my parents car have been broken into before. It was because of lax security on our part; we left some valuable items in the car.
4. My laptop is most likely infected but I have no way of know for sure that it is.
5. Antivirus software, firewall, password (authentication), visiting authentic webpages
6. Not against someone who knows what they are doing and really want to get information from my computer.
7. No, more and more things using technology—electric grid, transportation network. As more things come to rely on technology and if they are in anyway shape or form connected to the internet, there is the possibility that someone could get into the system and take it out. If a catastrophe like that were to happen, it would be very large in magnitude and take some time to get back up and running.
8. Learning about computer security is important to enhance your own protection, the quality and safety of interpersonal and business transactions, as well as improve the overall security in cyberspace.

Lecture 2

1. Attackers find new way to exploit a system everyday. Defenders must constantly be vigilant and search for any vulnerabilities not yet defended in their system.
2. There is no systematic way to enumerate the "bad things" that might happen because each program is different. There may be some overlap in vulnerabilities between programs but each will have its own unique list of vulnerabilities.
3. The defender must think of all possible exploitable vulnerabilities in the system where as the attacker only has to find the one vulnerability that you did not think of. If you have 3 weak points in your security, you must defend all 3 points to ensure that your system is secure. However, if you only defend 2 points, the attacker only needs to find the 1 point that you are not defending to exploit.
4. Yes. If you are connected to the internet, you can be tracked based on your connection to the internet. Websites also collect data on your internet usage for advertisement, personalization, etc.
5. Completely securing a software may prevent good things from happening. Therefore, there are some tradeoffs are required. These tradeoffs are about managing risk; a decision about which risk can be taken on so that something good can happen in the software.

Lecture 3

1. Risk is the possibility that something bad will happen.
2. Yes. If a software was completely secure, it would no longer be useful. In creating security for the software, the risks will be assessed to see which ones are not as risky and can be left alone, so the software could work.
3. Accept the risk of driving, avoid the risk of skydiving, mitigate risk by backing up hard drive, and transfer risk by having a home security system.
4. Annualized loss expectancy is a table of possible losses, their likelihood, and the potential cost for an average year. You can use the table to evaluate which possible loss would be the most costly and spend security money accordingly.
5. Technical, economic, and psychological factors.

Lecture 4

1. Confidentiality, integrity, and availability are major aspects of computer security. Whereas, passwords, cryptography, etc. are all mechanisms used to protect one of the major aspects.
2. Integrity is the most important. When I write a paper, I expect my paper to be intact and the same as when I last saved it.
3. Grouping and categorizing data means to parcel out data into groups, so that certain groups can have more protection than others.
4. Authorizations can change over time because someone who is authorized to view and change a set of data may be fired. Therefore, that person's authorization needs to be revoked so that they can not go back in and change the data even though they no longer work for the company.
5. For something to be reliable, it must be available. If you can not count on it to be able to be used, it’s not available. Therefore the two are related.
6. If someone gets into your Amazon account and purchases items with your credit card. Authentication would be important to identify that it was not you. Non-repudiation would be important because even if authentication failed, you would like to have the charges reversed on your card since it was not you who bought the items.