CS361 Questions: Week 1

Type your answers and submit them on Canvas by 5pm on Friday, September 6, 2019. Don’t write an essay on these. Usually, 2–3 sentences will suffice. Sometimes 1 sentence will be enough.

1. What uses of the term “security” are relevant to your everyday life?
2. What do these have in common?
3. Have you been a victim of lax security?
4. What is the likelihood that your laptop is infected?
5. What security measures do you employ on your laptop?
6. Do you think they are probably effective?
7. Consider the quote from the FBI official. Do you think it overstates the case? Justify your answer.
8. Consider the five reasons given why security is hard. Can you think of other factors?
9. Is there a systematic way to enumerate the “bad things” that might happen to a program? Why or why not?
10. Explain the asymmetry between the defender and attacker in security.
11. Examine the quotes from Morris and Chang. Do you agree? Why or why not?
12. Explain the statement that a tradeoff is typically required.
13. What is “risk”?
14. Do you agree that software security is about managing risk?
15. Name and explain a risk you accept, one you avoid, one you mitigate, and one you transfer?
16. Evaluate annualized loss expectancy as a risk management tool.
17. Consider your use of computing in your personal life. Which is most important: confidentiality, integrity, availability? Justify your answer.
18. What does it mean “to group and categorize data”?
19. Why would authorizations change over time?
20. Some of the availability questions seem to relate more to reliability than to security. How are the two related?
21. List at least one context in which each of authentication and non-repudiation would be considered important?