CS 478/513: Computer Security
Spring 2022
Total Points: 100

Assignment 1

Due: Tue., 2/9/22, 11:59 pm

Please complete the following problems, being sure to explain your conclusions or show your work when such details are requested. Your solutions must be submitted to Canvas as a PDF file. You can use my posted template if you want to, but are not required to do so.

This assignment is to be completed individually. Please cite your references (except textbook, slides), as described in the syllabus.

Chapter 1:

1. (20 points) Consider the definitions of confidentiality, integrity, and availability.
   (a) When might each of these aspects of information security be more important than the others?
   (b) Describe a few situations where strengthening one of these might weaken another.

Chapter 2:

2. (10 points) Complete Problem 19 (a, b) from the text.
3. (20 points) Complete Problem 29 (a, b, c, d) from the text.
4. (30 points) Suppose a cipher uses an 8-character mixed-case alphanumeric key (0-9, a-z, and A-Z).
   (a) What is the size of the keyspace (i.e., how many unique keys are possible)?
   (b) What is the approximate strength of the key, measured in bits? *Hint: rewrite the size of the keyspace as a power of two.*
   (c) If a particular computer can test 2^{40} keys per second, how long will it take (on average) to guess the key of this cipher?
5. (20 points) Consider that the 8-character key from the previous problem would take up 64 bits if stored as an ASCII string. However, in this scenario, not every bit would contribute to the strength of the key. Assume the cipher is upgraded to use all 64 bits.
   (a) What is the new size of the keyspace?
   (b) How much time would it take to crack the new version of the cipher (if able to test 2^{40} keys per second)?