Basic Security Concepts

CIS-4040 Homework #1

Peter C. Chapin, Vermont Technical College

Due: Wednesday, September 4, 2019

Read Chapter 1 of the text. The entire chapter is of interest, but be particularly certain to read sections 1.1 through 1.4. The last question of this assignment is about steganography. You will have to do some reading online about it to answer the question.

1. Consider the Dolev-Yao adversary model as described in class. See the class slides for details. When evaluating the security of a network protocol (e. g., the SSL protocol) it is common to assume the adversary is a Dolev-Yao attacker. How accurate do you think that assumption is? In what way are real adversaries likely to be less powerful? In what way are real adversaries likely to be more powerful?

2. This is Problem 1.1 in the text: Consider an automated teller machine (ATM) to which users provide a personal identification number (PIN) and a card for account access. Give examples of confidentiality, integrity, and availability requirements associated with the system and, in each case, indicate the degree of importance of the requirement.

3. Run the count.exe program provided on the web site over a plain text file of your choosing. Try to run it over a fairly large file (for example the RFC document describing the HTTP protocol [http://www.ietf.org/rfc/rfc2616.txt]). Don't use a word processor document. Take note of the top ten most commonly occurring characters.

   Encrypt the file with the substitution cipher program ss.exe. Run the count.exe program over the encrypted file and take note of the top ten most commonly occurring characters. What can you conclude from this experiment? I'm looking for a general statement that applies to all substitution ciphers.

4. What is steganography, and under what conditions is steganography useful? Avoid just quoting text from a source. Try to understand the essential point of steganography, and write down your own words to explain that point. Don't forget to reference any source(s) you found particularly useful.