Basic Security Concepts

CIS-3240 Homework #1

Peter Chapin, Vermont State University

Due: Friday, September 5, 2025

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 it is common to assume the adversary is a Dolev-Yao attacker. In what way are real adversaries likely to be less powerful than the theoretical D-Y attacker? In what way are real adversaries likely to be more powerful?

2. Consider an automated teller machine (ATM) to which users provide a personal identification number (PIN) and a card for account access. Give examples of reasonable confidentiality, integrity, authentication, and availability requirements associated with the system.

3. A *substitution cipher* is an encryption method where bytes of plaintext are replaced with (i.e., "substituted" with) different bytes to form the ciphertext. The "key" in such a system is the mapping of plaintext bytes to ciphertext bytes. For example, such a mapping might state that every 'x' in the plaintext is to be replaced by 'H' to form the ciphertext (and every other possible plaintext byte has a corresponding replacement of some kind). Substitution ciphers are very simple to implement and run very quickly. However, they are not secure. In this question, you will explore the issues with them.

   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. The ss.exe program transforms a password into a mapping from 8-bit bytes to 8-bit bytes in a deterministic way. In other words, using the same password will produce the same mapping.

   Now run count.exe over the encrypted file and take note of the top ten most commonly occurring characters. Can you see why substitution ciphers are not secure? Explain. Also include in your answer the details of the top most commonly occurring characters both before and after the encryption.

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.