CSc 4222/6222 – Assignment #3

Deadline: Monday, September 25th / Late Deadline: Thursday, September 28th

Make sure to justify all your answers clearly.
No handwritten submissions

---

1. Barack often sends funny jokes to Hillary. He does not care about confidentiality of these messages but wants to get credit for the jokes and prevent Bill from claiming authorship of, or modifying them. He can achieve this by using public-key cryptography and digitally signing his jokes and send each one with its signature. However, as public-key cryptography is computationally intensive and drains the battery of Barack's device, he comes up with an alternative approach. First, he shares a secret key k with Hillary, but not with Bill. Next, together with a joke x, he sends over the value $d = h(k||x)$, where each h is a cryptographic hash function. Does value d provide assurance to Hillary that Barack is the author of x and that x was not modified by Bill?

2. Alice and Bob shared an n-bit secret key some time ago. Now they are no longer sure they still have the same key. Thus, they use the following method to communicate with each other over an insecure channel to verify that the key K_A held by Alice is the same as the key K_B held by Bob. Their goal is to prevent an attacker from learning the secret key.

   i. Alice generates a random n-bit value R.

   ii. Alice computes $X = K_A \oplus R$, where $\oplus$ denotes the exclusive-or Boolean function, and sends X to Bob.

   iii. Bob computes $Y = K_B \oplus X$ and sends Y to Alice.

   iv. Alice compares R and Y. If $R = Y$, she concludes that $K_A = K_B$, that is, she and Bob have indeed the same secret key.

Show how an attacker eavesdropping the channel can gain possession of the shared secret key.

3. Suppose you could use all 128 characters in the ASCII character set in a password. What is the number of 8-character passwords that could be constructed from such a character set? How long, on average, would it take an attacker to guess such a password if he could test a password every nanosecond?

4. If a password is salted with a 24-bit random number, how big is the dictionary attack search space for a 200,000 word dictionary?

5. Eve has just discovered and decrypted the file that associates each userid with its 32-bit random salt value, and she has also discovered and decrypted the password file, which contains the salted-and-hashed passwords for the 100 people in her building. If she has a dictionary of 500,000 words and she is confident all 100 people have passwords from this dictionary, what is the size of her search space for performing a dictionary attack on their passwords?

6. Dr. Blahblah has implemented a system with an 8-bit random canary that is used to detect and prevent stack-based buffer overflow attacks. Describe an effective attack against Dr. Blahblah's system and analyze its likelihood of success.

7. In the Tim Lloyd logic bomb attack on Omega Engineering, what type of vulnerability was the existence of the user, "12345," an example of?

8. Viruses that perform no explicit malicious behaviors are called *bacteria* or *rabbits*. Explain how such seemingly benign viruses can still have negative impacts on computer systems.

9. You are given the task of detecting the occurrences of a polymorphic virus that conceals itself as follows. The body, C, of the virus code is obfuscated by XORing it with a byte sequence, T, derived from a six-byte secret key, K, that changes from instance to instance of the virus in a random way. The sequence T is derived by merely repeating over and over the given key K. The length of the body of the virus code is a multiple of six – padding is added otherwise. Thus, the obfuscated body is $T \oplus C$, where $T = K \| K \| \ldots$ and $\|$ denotes string concatenation. The virus inserts itself to the infected program at an unpredictable location. And infected file contains a *loader* that reads the key K, unhides the body C of the virus code by XORing the obfuscated version with the sequence T (derived from K), and finally launches C. The loader code, key K, and the obfuscated body are inserted at random positions of infected programs. At some point of the execution of the infected program, the loader gets called, which unhides the virus and then executes it. Assume that you have obtained the body C of the virus code and a set of programs that are suspected to be infected. You want to detect the occurrences of this virus among the suspected programs without having to actually emulate the execution of the programs. Give an algorithm to do this in polynomial time in the length of the program. Assume that the loader of the virus is a short piece of code that can be commonly found in legitimate programs. Therefore, it cannot be used as a signature of our virus. Hence, looking for the loader is not an acceptable solution. Remember, the loader is in binary, and as such, extracting information from it is nontrivial, i.e., wrong.

10. Suppose you want to use an Internet café to login to your personal account on a bank web site, but you suspect that the computers in this café are infected with software keyloggers. Assuming that you can have both a web browser window and a text editing window open at the same time, describe a scheme that allows you to type in your userID and password so that a keylogger, used in isolation of any screen captures or mouse event captures, would not be able to discover your userID and password.