CYBR 8410 – Distributed System Security – 2021 Spring

Lab 1

Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

NUID: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Please follow the requirements and due date specified in the Syllabus to submit your work.

Students need to answer the specified questions in the following lab content and steps, and submit your answers in a PDF or Word file.

You need to describe what you have done and what you have observed; you also need to provide explanation to the observations that are interesting or surprising.

During the lab, if anything is not clear to you, please contact the instructor.

1. **Lab Environment:**

A Linux machine. A virtual machine on Windows/Mac will also be fine.

Cryptography library OpenSSL. We will use openssl commands and libraries. Make sure you have openssl installed on your Linux machine.

Binary editor GHex. We need to be able to view and modify files of binary format. Make sure you have GHex installed. It would be fine if you could find another binary editor.

1. **Lab Content and Steps:**

**2.1 Encryption using different ciphers and modes (15 pts)**

In this task, we will experiment with various encryption algorithms and modes. You can use the following “openssl enc” command to encrypt/decrypt a file. To see the manuals, you can type “man openssl” and “man enc”.

% openssl enc <ciphertype> -e -in plain.txt -out cipher.bin -K 00112233445566778889aabbccddeeff -iv 0102030405060708

Please replace the <ciphertype> with a specific cipher type, such as -aes-128-cbc, -aes-128-cfb, -des-cbc, etc. You should create the “plain.txt” file with your own plaintext. In this task, you should try three different ciphers in three different modes. Please provide the inputs, outputs, as well as commands in your submission.

You can find the meaning of the command-line options and all the supported cipher types by typing “man enc”. We include some common options for the “openssl enc” command in the following:

-in input file

-out output file

-e encrypt

-d decrypt

-K/-iv key/iv in hex is the next argument

-[pP] print the iv/key (then exit if -P)

**2.2 Encryption Mode – ECB vs. CBC (20 pts)**

The file pic “original.bmp” contains a simple picture. We would like to encrypt this picture, so people without the encryption keys cannot know what is in the picture. Encrypt the file using the AES algorithm in ECB (Electronic Code Book) and CBC (Cipher Block Chaining) modes, and then do the following:

1. Let us treat the encrypted picture as a picture, and use a picture viewing software to display it. However, the first 54 bytes of a .bmp file contain the header information about the picture. We have to set these bytes correctly, so that the encrypted file can be treated as a legitimate .bmp file. We will replace the header of the encrypted picture with that of the original picture. You can use the ghex tool to directly modify binary files. Please provide the commands that you used to encrypt the picture in those two modes. (10 pts)
2. Display the encrypted picture using any picture viewing software. Can you derive any useful information about the original picture from the encrypted picture? Please explain your observations. (10 pts)

**2.3 Encryption Mode – Corrupted Cipher Text (60 pts)**

To understand the properties of various encryption modes, we would like to do the following exercise:

1. Create a text file that is at least 64 bytes long. Please provide the file content.
2. Encrypt the file using the AES-128 cipher. The encryption mode you should use is ECB, CBC, CFB, and OFB. Now we should have four encrypted files. Please provide the commands. (10 pts)
3. Unfortunately, you just need to corrupt a single bit of the 30th byte in the encrypted files. You can achieve this corruption using ghex. Please provide the information of which bit you got flipped.
4. Decrypt the corrupted files (encrypted) using the correct key and IV. Please provide the the commands and results. (10 pts)
5. Please answer the following questions:

(1) How much information can you recover by decrypting the corrupted file, if the encryption mode is ECB, CBC, CFB, or OFB, respectively? Please answer this question before you conduct this task, and then find out whether your answer is correct or wrong after you finish this task. (20 pts)

(2) Explain why. (10 pts)

(3) What are the implication of these differences? (10 pts)