Project 2: Bitflipping

Computer Security – Marquette University

Spring 2018

Preparation

In order to do this project, you will need Python 3 installed (just get IDLE) and a hex editor. I think that by far the best hex editor for a windows machine is WinHex from X-Ways software. You can evaluate WinHex free of charge for up to 45 days. On my Mac, I am using iHex as downloaded from the app store.

Tasks

You are asked to use bit-flipping on an encrypted datum simulating a row of a database. There are two encryptions of the same text below. One uses an 8B block-code DES with CBC. The other one uses a stream cipher. You are not supposed to modify the encoding software and the key, but rather operate on the encoded text such that its contents change. In both cases, you need to use the enclosed python programs (main.py and xorcode.py) calling encode() to generate a file called data.hex and datax.hex respectively. The file data.hex is encrypted with the 8B-DES block code in CBC mode. The file datax.hex is encrypted with a stream cipher. In both cases, you have to change the first digit in the last number (4900) from four to five (5900) by changing the encrypted file (data.hex or datax.hex, respectively).

You need to describe in a write-up how you changed the binary file in order to achieve this task. For example, you could say that you replaced the bytes 0XA8 and 0XAE in positions 16 and 17 with 0X98 and 0X34, though if you use the decrypt function in both python codes, you will see that this did not contribute anything to the solution.

```
Thomas Schwarz, Jesuit Community, Marquette University,
Milwaukee, Wisconsin, USA, 4900.
```

It is understood that part of the address information is going to be mangled by the attack.

Deliverables

A short description of how you need to change the cipher text. You should be able to do this exercises by March 1, 2018.