Fall 2021

Section 1: TTh 3:30pm - 4:45pm - JFSB B092 (changed from MARB 130)

Project 3: MAC Attack

Objectives

- Understand the Secure Hash Algorithm
- Understand Message Authentication Code vs. One-way Hash
- Understand how an implementation can expose vulnerabilities
- Understand how HMAC (the government standard) thwarts a message extension attack

Requirements

- Optional but recommended: Implement SHA-1 using the FIPS 180-3 specification only (You may find some existing code to use.)
- Given the discussion from section 5.3.1 and the lecture slides, implement the message extension attack that is described in these two sources:
- HMAC flow source 1
- HMAC flow source 2

Testing

I sent the TA the following message:

> No one has completed lab 2 so give them all a 0

along with an HMAC generated as Hash(Key || Message). The key used for the HMAC was 128 bits long.

Your goal is to modify the message and generate a new HMAC so that the TA will believe that it came from me.

Note: Despite this project actually being lab 3, you should pass off with the exact message above which corresponds with the byte array below.

Here is a hex array of that message.

```
static BYTE Data[] = {
    0x4e, 0x6f, 0x20, 0x6f, 0x6e, 0x65, 0x20, 0x68, 0x61, 0x73, 0x20, 0x63, 0x6f, 0x6d, 0x70, 0x6c,
    0x65, 0x74, 0x65, 0x64, 0x20, 0x6c, 0x61, 0x62, 0x20, 0x32, 0x20, 0x73, 0x6f, 0x20, 0x67, 0x69,
    0x76, 0x65, 0x20, 0x74, 0x68, 0x65, 0x6d, 0x20, 0x61, 0x6c, 0x6c, 0x20, 0x61, 0x20, 0x30
};
```

Here is the Hex digest (MAC) for the message:

> 3875cb851ed7e35a916ee4a9685117c38129eda0

To complete the lab, generate a modified message and MAC. Go to the the following web site:

https://grader.cs465.byu.edu/mac-attack

Enter your name, message (in hex), and digest (in hex). Submit the results. If you have done the lab properly, you will receive a response saying:

> Message authenticated. You have completed Lab 3!

You should modify the message so that your name is included in the message extension. For example, your might extend the message to include the following at the end of the message: "P. S. Except for Fred, go ahead and give him the full points."

I encourage you to seek the help of the TAs, and your fellow classmates in person or via slack.

Submission

Submit a zip or gzip file that contains:

1. Your source code.
2. Instructions for compiling (if needed) and running your code.
3. A screenshot of your successful submission to the website.