One-Way Hash Function and MAC

Murtadha Alobaidi

April 2022

1 Introduction

This lab on IV1013 Introduction to Computer Security course. The purpose of this lab is to understand and get familiar with one-way hash functions and Message Authentication Code (MAC).

2 Tasks

2.1 Generating Message-Digest and MAC

Question1. Describe your observations. What differences do you see between the algorithms?

The difference between all these three algorithms(MD5, SHA1, and SHA256) is the different digests seem to be the length of them. MD5 has 128 bits, SHA1 has 160 bits and SHA256 has 256 bits.

Question2. Write down the digests generated using the three algorithms.

- MD5: bbcf35c25ff21ce56c1b434f391324bf
- SHA1: 5a82132529ac1fe0237c9c2d9cfea7d0ff9ff6
- SHA256: 07266ea52d162d64a8fa94645fc336cf9d69ac17342975d6fabf39f17

2.2 Keyed Hash and HMAC

Question3. Do we have to use a key with a fixed size in HMAC? If so, what is the key size? If not, why?

I tried to use a different key and a different size. The key size doesn't affect the result, the hash values generated a new value every time I tried with a new key. If the key length is shorter than the message it will use padding to make it work.

Question4. Now use the string IV1013 key as the secret key and write down the keyed hashes generated using the three algorithms.

- HMAC-MD5: 75a27a1bc22e8c6c8c337fafeebecfa6
- HMAC-SHA1: 340162572258e6de8e36e76da3adfebbec087e72
- HMAC-SHA256: 5ccff7d0958b40bfc6035735a3d199a63f129cf38016da9d6ee4a08e44ea5967

2.3 The Randomness of One-way Hash

Question 5. Describe your observations. Count how many bits are the same between H1 and H2 for MD5 and SHA256 (writing a short program to count the same bits might help you). In the report, specify how many bits are the same.

- Using H1→ md5 : bbcf35c25ff21ce56c1b434f391324bf
- Using H2→ md5 : d8a67b636c4bf232ac0daa6c0e4cc924
- Using H1→sh256: 07266ea52d162d64a8fa94645fc336cf9d69ac17342975d6fabf39f17
- Using H2→sh256: b6852e072ed7549130b99b6e8f4f081d5321db0afc4cf12ca517b3096d5d719f

With help of a short java-program “counter” that counts all similar bits from two **InputFiles** (H1 and H2) and the result are:

Using md5: 57-Bits similar

Using sh-256: 107-Bits similar

2.4 Collision Resistance

Question 6. Investigate how many trials it will take to break the weak collision property using the brute-force method. Below is a list of five messages. For each message, report how many trials it took before you could find a message with the same hash.

IV1013 security: 2 6370 363 trials

Security is fun: 896 704 trials

Yes, indeed: 24 145 654 trials

Secure IV1013: 682 046 trials

No way: 3 921 472 trials

3 Conclusion

This lab has focused on one-way hash functions and Message Authentication Code (MAC). I had a problem with the first task “2.1” when I used the **OpenSSL command.** It did not work on the Mac book but I fixed it by updating the Mac book and I used Ubuntu VirtualBox to solve this problem. On task 2.2 was interested to see how the **OpenSSL command** work and to solve the task. The test of different keys lengths with several keys to generate a keyed hash by using HMAC-MD5 HMAC-SHA256 and HMAC-SHA1. Task 2.3 the hard part was to flip the first bit but I solved it by using an online converter to get it right.