

哈尔滨工业大学（深圳）

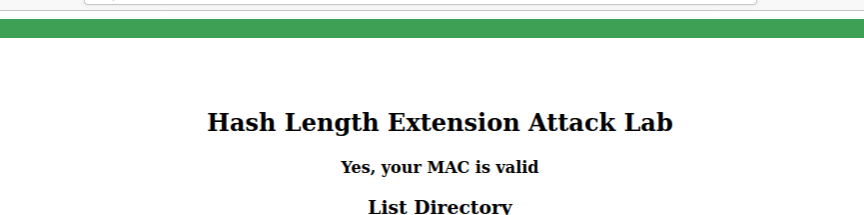
《密码学基础》实验报告

Hash 长度扩展攻击实验

学 院: 计算机科学与技术
姓 名: 王木一
学 号: 200210231
专 业: 计算机科学与技术
日 期: 2022-10-26

- ### 1. 计算 mac

2. 访问



Length Extension Lab

Length Extension Lab

SEEDLabs

Hash Length Extension Attack Lab

Yes, your MAC is valid

List Directory

1. secret.txt
2. key.txt

File Content

TOP SECRET.

DO NOT DISCLOSE.

2、 为消息 `<key>:myname=<name>&uid=<uid>&lstcmd=1` 创建对应 padding, 其中`<key>`和`<uid>`的实际内容应该从`LabHome/key.txt`文件中得到, myname 依然用你自己的姓名。

```
123456:myname=SEEDManual&uid=1001&lstcmd=1
%80%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%01%50
```

1

- 3、 为下面的请求生成一个有效的 MAC，其中`<key>`和`<uid>`的实际内容应该从`LabHome/key.txt`文件中得到，name 就是自己的姓名拼音。

`http://www.seedlab-hashlen.com/?myname=<name>&uid=<uid>
&lscmd=1&mac=<mac>`

```
[10/26/22] seed@VM:~/crypto_hash_extension$ echo -n "123456:myname=MuyiWang&uid=1001&lscmd=1" | sha256sum  
66432acc8c90a39017106944ecaae184e76a0fe88be8f8b4b792d663adacaef6 -
```

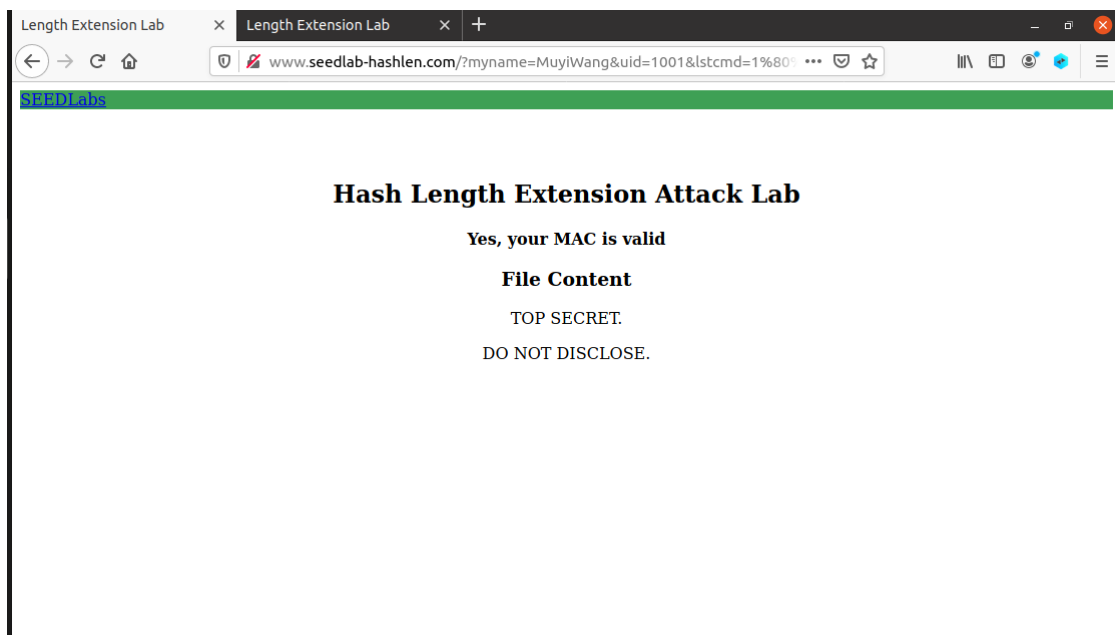
- 4、 发送构造好的新请求到服务器，padding 是上面获取到的信息，记录收到的服务器响应并截图。

`http://www.seedlab-hashlen.com/?myname=<name>&uid=<uid>
&lscmd=1<padding>&download=secret.txt&mac=<new-mac>`

1. new-mac 生成

```
[10/26/22] seed@VM:~/crypto_hash_extension$ a.out  
dd5916b6dd34b08dff55f45c3358cd21da282599dd4c4e0ea9d92cd03dcad7e8
```

2. 进行长度攻击



1. 正常访问 (改为 HMAC 后正常使用 lscmd=1 命令)

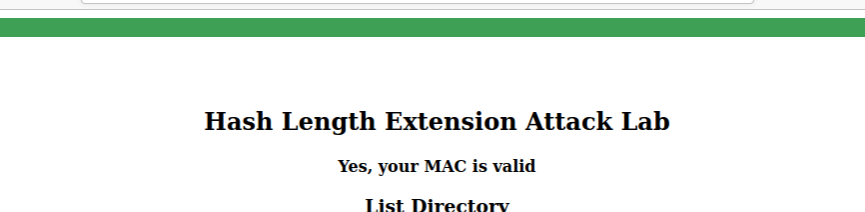
```
#!/bin/env python3

import hmac
import hashlib

key='123456'
message='myname=MuyiWang&uid=1001&lstcmd=1'
mac = hmac.new(bytearray(key.encode('utf-8')),
                msg=message.encode('utf-8', 'surrogateescape'),
                digestmod=hashlib.sha256).hexdigest()

print(mac)
```

```
[10/26/22] seed@VM:~/crypto_hash_extension$ python3 -u ./hmac_new.py
99eaf65572da384f39d61f357265dceb79b81b13f8ee93f26ee5d307a7e37100
```



Length Extension Lab

Length Extension Lab

www.seedlab-hashlen.com/?myname=MuyiWang&uid=1001&lscmd=1&mac=...

SEEDLabs

Hash Length Extension Attack Lab

Yes, your MAC is valid

List Directory

1. secret.txt
2. key.txt

2. 敌手在不知道已经换成 HMAC 的情况下进行长度攻击，仍和之前一样计算 padding，计算新 mac

生成 new-mac

```
seed@VM: ~/crypto_hash_extension
#include <stdio.h>
#include <string.h>
#include <arpa/inet.h>
#include <openssl/sha.h>

unsigned char *additionalMsg = "&download=secret.txt";

// The MAC for the valid URL
int a[8] = { 0x99eaf655, 0x72da384f, 0x39d61f35, 0x7265dceb,
            0x79b81b13, 0xf8ee93f2, 0x6ee5d307, 0xa7e37100 };

int main(int argc, const char *argv[])
{
    int i;
    unsigned char buffer[SHA256_DIGEST_LENGTH];
    SHA256_CTX c;

    SHA256_Init(&c);

    /* We assume that the padded original message has 64 bytes (i.e., 1 block).
     * If that is not true, modify 64 accordingly, e.g. use 128 for 2 blocks.
     * This step is important, because that is how we tell the hash function
     * the length of our message. */
    "url_length_extension.c" [dos] 38L, 1057C                               11,0-1      Top

[10/26/22]seed@VM:~/crypto_hash_extension$ a.out
7cb0e650033f18b9745c6819c16a20f6eb393381ee564892133043e63fbeb210
```

访问失败

