

HW #2

Hash Length Extension Attack Lab

Computer Security

School of CSEE




Requirement

- 본 숙제는 SEED Lab에 있는 **Hash Length Extension Attack Lab**을 수행하는 것입니다.
- 아래의 홈페이지에서 Tasks (PDF 파일)를 참고하여 수행하면 됩니다.
 - https://seedsecuritylabs.org/Labs_20.04/Crypto/Crypto_Hash_Length_Ext

PDF 파일을
반드시 정독할 것!


Hash Length Extension Attack Lab

Overview



In this lab we will cover how the length extension attack works. Students will gain first hand experience how a Message Authentication Code (MAC) is calculated using one-way hash using a key and message. The lab explores how an attacker can intercept a client request, expand the message and calculate a correct MAC without knowing the key. Students will apply this knowledge to attack a server program. Students will also learn how to correctly generate a MAC using HMAC.

Activities: Students are given a server program that accepts a list of commands. The client and server share a secret key. The server expects a MAC argument in the request. This MAC is calculated in an insecure way by concatenating the key and request arguments. Students will exploit the insecure MAC calculation to add an additional command to a client request. Students will then fix the server program by calculating the MAC using HMAC.

 **Tasks (PDF)**

- **VM version:** This lab has been tested on our [SEED Ubuntu-20.04 VM](#)
- **Lab setup files**
 - [Labsetup.zip](#)
 - [Labsetup-arm.zip](#) (for Apple Silicon machines)

Requirement

- PDF에 있는 내용을 정독 후 Lab을 수행하되, 다음 페이지부터 나오는 Lab Summary를 참고하여 수행하세요.
- Lab Summary에서 초록색 글씨로 표시된 Task는 반드시 수행해야 하고, 그 결과와 이유에 대해 Report에서 설명해야 합니다.
- 공격 과정은 재현 가능해야 하며, 이를 위해 변경된 소스 코드와 파일을 모두 제출하세요.
- Web Browser를 스크린 캡처할 경우에는 주소창 (myname) 이 보이도록 캡처해주세요.

Lab Summary

■ Lab Environment 구축

- 1. Labsetup.zip (Arm CPU는 Labsetup-arm.zip)을 다운로드

☰ Tasks (PDF)

- **VM version:** This lab has been tested on our [SEED Ubuntu-20.04 VM](#)
- **Lab setup files**
 - Labsetup.zip
 - Labsetup-arm.zip (for Apple Silicon machines)
- **Manual:** [Docker manual](#)

- 2. 다운로드한 Labsetup.zip 압축 해제
- 3. Labsetup (or Labsetup-arm) 디렉토리로 이동

Lab Summary

■ Lab Environment 구축

■ 4. 아래와 같은 명령어를 활용하여 Docker Container Setup

```
[11/12/24]seed@VM:~/hw2/Labsetup$ docker-compose build
```

```
Building web-server
```

```
Step 1/4 : FROM handsonsecurity/seed-server:flask
```

```
----> 384199adf332
```

```
Step 2/4 : COPY app /app
```

```
----> Using cache
```

```
----> 4349fcdde419
```

```
Step 3/4 : COPY bashrc /root/.bashrc
```

```
----> Using cache
```

```
----> 508789d01808
```

```
Step 4/4 : CMD cd /app && FLASK_APP=/app/www flask run --host 0.0.0.0 --port 80 && tail -f /dev/null
```

```
----> Using cache
```

```
----> 704111e4fdee
```

```
Successfully built 704111e4fdee
```

```
Successfully tagged seed-image-flask-len-ext:latest
```

```
[11/12/24]seed@VM:~/hw2/Labsetup$ docker-compose up
```

```
Starting www-10.9.0.80 ... done
```

```
Attaching to www-10.9.0.80
```

```
www-10.9.0.80 | * Serving Flask app "/app/www"
```

```
www-10.9.0.80 | * Environment: production
```

```
www-10.9.0.80 | WARNING: This is a development server. Do not use it in a production deployment.
```

```
www-10.9.0.80 | Use a production WSGI server instead.
```

```
www-10.9.0.80 | * Debug mode: off
```

```
www-10.9.0.80 | * Running on http://0.0.0.0:80/ (Press CTRL+C to quit)
```

Arm용 Ubuntu에서 docker-compose 가
설치되어 있지 않다면 아래의 명령어를
사용하여 docker-compose 설치 후 진행
\$ sudo apt install docker-compose

Lab Summary

■ Lab Environment 구축

■ 5. /etc/hosts 파일에 아래와 같이 host 정보 추가

- 이를 통해 VM의 Web Browser에서 `www.seedlab-hashlen.com` (Docker에서 운영 중인 Web server) 접속이 가능해짐

```
[11/12/24] seed@VM: ~/hw2/Labsetup$ sudo vi /etc/hosts
```



```
10.9.0.80      www.seedlab-hashlen.com
```

```
"/etc/hosts" 33L, 813C
```

■ 6. Sending request 에 있는 Server program command 의미 파악 하기

Sending requests. The server program accepts the following commands:

- The `lstcmd` command: the server will list all the files in the `LabHome` folder.
- The `download` command: the server will return the contents of the specified file from the `LabHome` directory.

Lab Summary

■ Task 1: Send Request to List Files

- 1. 새로운 터미널을 연 뒤, 아래의 명령어를 입력하여 Server program command 에 대한 HASH 값 가져오기
 - 아래 명령어 중 “myname” 부분에는 자기 이름을 넣을 것!

myname 부분에 자기 이름을 넣을 것!

```
[11/12/24] seed@VM: ~/hw2/Labsetup$ echo -n "123456:myname=Yunmin&uid=1001&lstcmd=1" | sha256sum  
0bdcf9f6bc215c076fb0d0eb008961f1c83554cf80bea4d0d3fe96963716eafd -
```

본 Lab에서 SHA256 사용
(출력Hash=256bits)

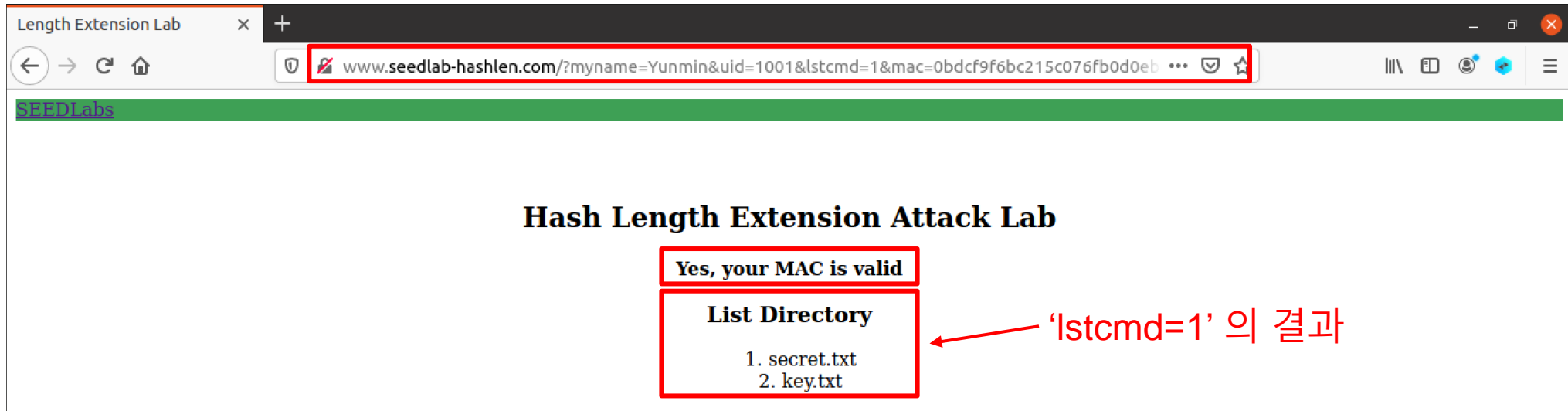
- 2. 이전 단계에서 얻은 HASH 값을 “mac” 이후에 집어 넣어 Request URL을 생성

```
www.seedlab-  
hashlen.com/?myname=Yunmin&uid=1001&lstcmd=1  
&mac=0bdcf9f6bc215c076fb0d0eb008961f1c83554c  
f80bea4d0d3fe96963716eafd
```

Lab Summary

■ Task 1: Send Request to List Files

- 3. VM 내에서 Web browser (Firefox)를 실행한 뒤 이전 단계에서 생성한 Request URL을 주소창에 입력
 - URL에 'https'가 아니라 'http'가 들어가 있는지 확인 필요



- Task: Download command를 서버에 전송하고 그 결과를 스크린 캡처한 후 설명할 것!

Lab Summary

■ Task 2: Create Padding

- Task: 아래 형식에 맞춰 적절한 메시지를 생성하고, 생성된 메시지에 대한 padding 을 생성할 것. 또한 padding이 왜 그렇게 생성된 지에 대해 설명할 것!

<key>:myname=<name>&uid=<uid>&lstcmd=1

 /LabHome/key.txt 에 있는 Mapping 값들을 사용해야 함.

예: 123456:myname=Yunmin&uid=1001&lstcmd=1

Request URL 내에 Padding을 포함시키기 위해서는
"\x80\x00\x00\x99" 대신 "%80%00%00%99" 를 사용해야 함.

Lab Summary

■ Task 3: The Length Extension Attack

- Task: length_ext.c를 수정하고 이를 기반으로 secret.txt를 가져오기 위한 Malicious Request URL 생성하세요. 생성된 URL을 이용하여 secret.txt를 가져오는 공격을 시도하세요. 수정된 length_ext.c는 제출하고, 전체 공격 과정을 스크린 캡처와 함께 설명하세요.

공격 성공 시 예상 결과

Task3은 Length extension attack을 수행하는 것이므로, Task 1과 2에서 만들어진 hash와 padding을 활용해야 합니다. 즉, key와 secret.txt를 가져오는 명령어가 포함된 string을 직접 hash하여 사용하면 안됩니다.

Hash Length Extension Attack Lab

Yes, your MAC is valid

File Content

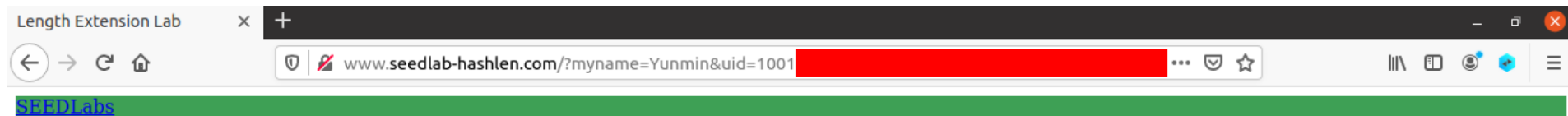
TOP SECRET.
DO NOT DISCLOSE.

secret.txt의 내용

Lab Summary

- Task 4: Attack Mitigation using HMAC
 - Task: lab.py가 HMAC을 사용하도록 변경하고, 그 실행 결과를 보이세요 (HMAC을 이용하여 File list를 Request한 결과). 또한 서버가 HMAC을 사용할 때 왜 Malicious Request가 Fail하는지에 대해 설명하세요.

HMAC 사용으로 인한 Malicious request 예상 결과



Hash Length Extension Attack Lab

Sorry, your MAC is not valid

Requirement

- Intel CPU 사용자의 경우 Seed VM에서 실행되어야 하며, Arm CPU 사용자는 Arm 버전 Ubuntu 22.04에서 실행 가능해야 합니다.
- Report는 Word로 작성 후 PDF 파일로 제출하세요.
- 제출하는 파일들은 아래와 같은 형태로 ZIP으로 압축하여 LMS에 제출하세요.
 - 파일 이름: hw02_student id.zip (ex: hw02_20400022.zip)
- ChatGPT 등 AI Tool과 기존 Open Source에 대한 직접적인 사용이 적발될 경우 0점 처리됩니다.
- Due date: 11:59pm, 11/22 (Fri)