#### Network Security Term Project – Secure Message Board

Subproject 3: Website Authentication

1. **Description**

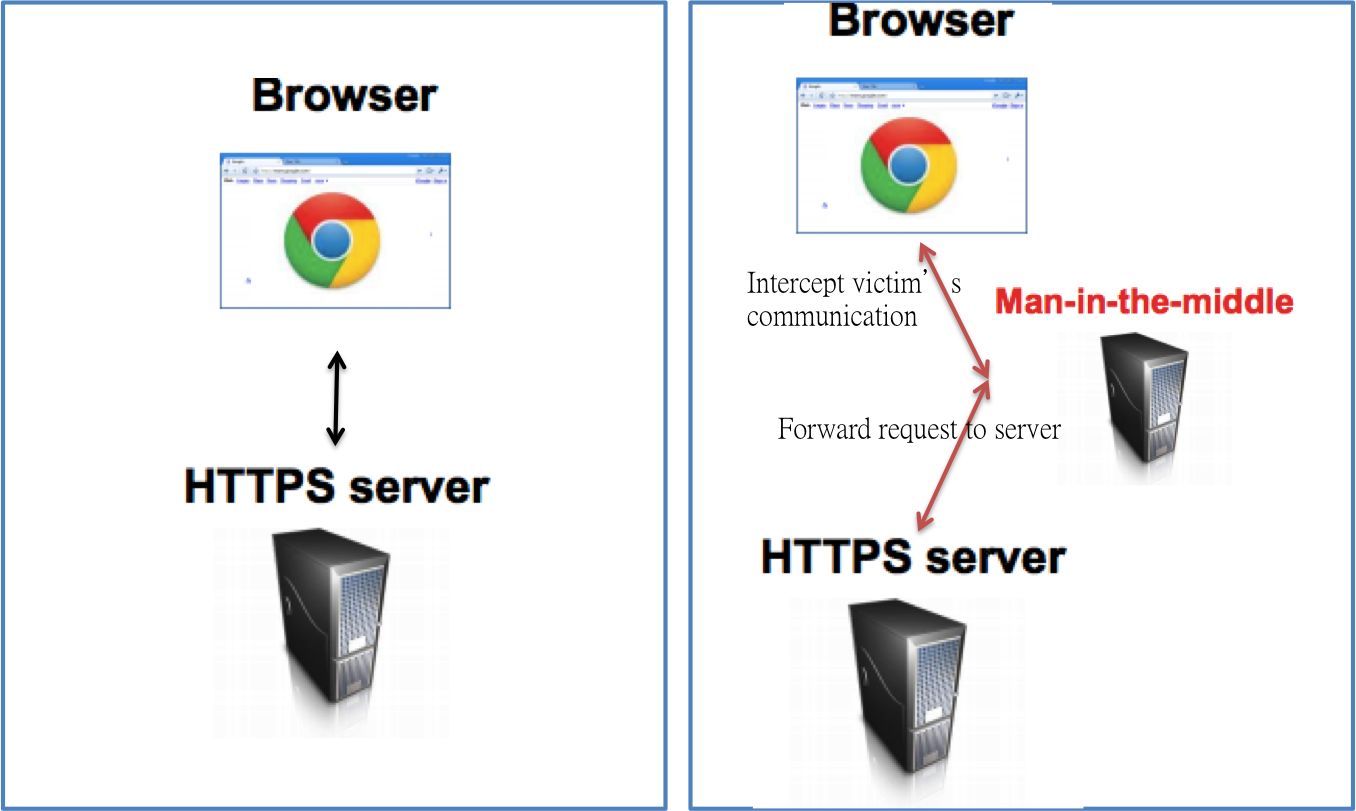
In previous project, we already build our website which can use SSL to encrypt network communication. However, without proper authentication mechanism, attacker can pretend as the server to raise the MITM(man in the middle) attack.

Therefore in this subproject, students are first asked to build a MITM program to attack their website. Then students need to construct a trusted certificate sign by TA’s certificate (and key) which can used to authenticate their website.

1. **Platform and Environment**  
   In this project, students will need three machine
2. Attacker’s machine (VM), recommend use Ubuntu. This machine is used to attack victim machine.

Must install openssl, python, python’s ssl package

1. Legal website (VM) with public ip address, recommend use Ubuntu. This machine is used to host your website in previous subproject
2. Victim Machine, Ubuntu or Windows. This is machine used by user to browse website



\* Note: You need to create at least two VM(Attacker’s machine and Legal website), and you real(physical) machine can be used as Victim Machine

1. **Requirement**
2. Build a proxy level MITM program, which can record user’s browsing result.
3. Generate a certificate signed by TA’s certificate.
4. Deploy the certificate to your website against MITM attack and compare the difference between normal situation and MITM attack.

After finishing this subproject, students should upload following things to E-campus

1. MITM program source code(with fake certificate)
2. Report
3. Address of you website, which contain a certificate signed by TA’s certificate (include in report).
4. **MITM**

MITM is an approach to attack website without strong authentication. The attacker first intercepts communicate between victim and server. Then attacker pretends itself as server and forward the message between server and victim. As the result, attacker can monitor and modify user’s communication. Procedure of MITM attack is shown in figure 1.

1. Create a fake certificate just like previous subproject. You need to setup the certificate’s common name as “attacker”

Country Name (2 letter code) [AU]:TW State or Province Name (full name) [Some-State]:Taiwan R.O.C Locality Name (eg, city) []:HsinChu Organization Name (eg, company) []:NCTU

Organizational Unit Name (eg, section) []: NS

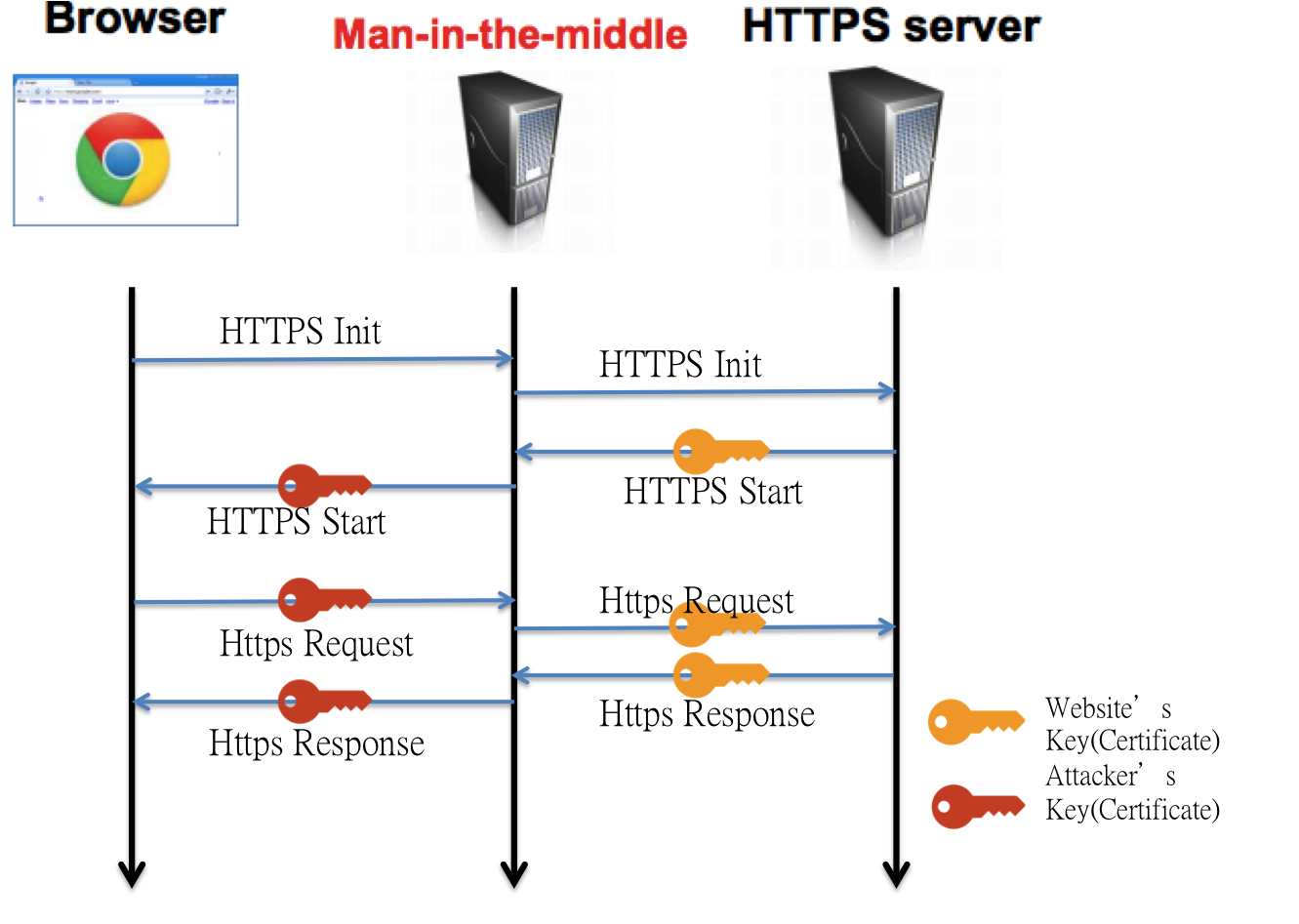
Common Name (eg, YOUR name) []:attacker

Email Address []:

Please enter the following 'extra' attributes to be sent with your certificate request A challenge password []:

An optional company name []:

1. Intercept user’s communication. In the subproject, we will implement a proxy level MITM attack, so students can directly configure the browser using attacker’s machine as proxy.
2. Implement MITM program based on the template program provide by TA. The template program contains details steps that can help you to finish this part. You can read reference 5 and 6 to understand the mechanism of http/https proxy.
   * Link: http://140.113.216.151/mitm.py

****

**Figure 1 Procedure of MITM**

1. **CA and Trust Chain**

To against MITM attack, students are asked to build a small trust chain. TA will provide a certificate and private key of that certificate. Students should use certificate and key to sign their website certificate as the root CA do. As the result, victim’s browser will trust certificate of website, but not attacker’s. Therefore, the warning will pop up when victim under MITM attack, while no warning in normal connection.

1. Download TA’s certificate and private key

* Key: <http://140.113.216.151/root.key>
* Certificate: <http://140.113.216.151/root.pem>

1. Use openssl command to generate private key of your website.
2. Use openssl to generate certificate request by your private key.

#openssl req -new -key <key file> -out <domain name or ip>.req

#openssl genrsa –out <website ip>.key 2048

This command will ask you to fill some certificate’s information. Please fill the information as fowllow.

Country Name (2 letter code) [AU]:TW State or Province Name (full name) [Some-State]:Taiwan R.O.C Locality Name (eg, city) []:HsinChu Organization Name (eg, company) []:NCTU

Organizational Unit Name (eg, section) []: NS

Common Name (eg, YOUR name) []:<domain or ip>

Email Address []:

Please enter the following 'extra' attributes to be sent with your certificate request A challenge password []:

An optional company name []:

1. Passing request to CA. Normally, this process is go through email or website. But in this project you are also play the role of CA, so this step can be ignored.
2. With the TA’s key and certificate, website’s certificate can be generate by the certificate request.

#openssl x509 -req -days 3650 -sha1 -extfile /etc/ssl/openssl.cnf -extensions v3\_req -CA <TA’s certificate> -CAkey <TA’s key> -CAserial rootca.srl -CAcreateserial -in <certificate request file> -out <ip or domain name>.crt

1. **Grading Policy**

TA will first import TA’s certificate into browser, then connect to your website to check if your website use SSL with proper certificate. Then TA start the MITM attack and check two things. First, warning pop up for untrusted authentication. Second, MITM program can record traffic in plaintext after we ignore the warning.

1. MITM program – 40 %
2. Website Certificate – 30 %
3. Report – 30 %, your report must contain
4. Implementation details about MITM program
5. Steps you used to generate website’s certificate
6. Further research/reading(you can find some by yourself or read some article listed in Further Reading in section 7) about authentication and MITM
7. **Reference**
8. <http://www.devsec.org/info/ssl-cert.html>
9. <http://en.wikipedia.org/wiki/Man-in-the-middle_attack>
10. <https://www.openssl.org/docs/HOWTO/certificates.txt>
11. <http://blog.philippheckel.com/2013/07/01/how-to-use-mitmproxy-to-read-and-modify-https-traffic-of-your-phone/>
12. <http://en.wikipedia.org/wiki/List_of_HTTP_header_fields>
13. <http://www.forensicswiki.org/wiki/Proxy_server>

Further Reading

1. <http://dl.acm.org/citation.cfm?id=1512329>
2. <http://link.springer.com/chapter/10.1007/978-3-642-33167-1_12#page-1>
3. <https://www.linshunghuang.com/papers/mitm.pdf>
4. <https://blackhat.com/presentations/bh-europe-09/Marlinspike/blackhat-europe-2009-marlinspike-sslstrip-slides.pdf>