SELF-SIGNED SSL CERTIFICATE GENERATION

Anisha Lalwani
Department of Computer Engineering
Vivekanand Education Society Institute of Technology
Chembur, India
anisha.lalwani@ves.ac.in

Lakhan Bhagnani
Department of Computer Engineering
Vivekanand Education Society Institute of Technology
Chembur, India
lakhan.bhagnani@ves.ac.in

***Abstract-* SSL (Secure Sockets Layer) is a standard security technology for establishing an encrypted link between a server and a client—typically a web server (website) and a browser, or a mail server and a mail client. SSL allows sensitive information such as credit card numbers, social security numbers, and login credentials to be transmitted securely. This paper explains a way to generate a self signed SSL certificate to provide security.**

Keywords- SSL, security, self signed, certificate.

I. INTRODUCTION

TLS, or transport layer security, and its predecessor SSL, which stands for secure sockets layer, are web protocols used to wrap normal traffic in a protected, encrypted wrapper. Using this technology, servers can send traffic safely between the server and clients without the possibility of the messages being intercepted by outside parties. The certificate system also assists users in verifying the identity of the sites that they are connecting with.

A self-signed certificate will encrypt communication between your server and any clients. However, because it is not signed by any of the trusted certificate authorities included with web browsers, users cannot use the certificate to validate the identity of your server automatically. A self-signed certificate may be appropriate if you do not have a domain name associated with your server and for instances where the encrypted web interface is not user-facing. If you do have a domain name, in many cases it is better to use a CA-signed certificate.

Normally, data sent between browsers and web servers is sent in plain text-leaving you vulnerable to eavesdropping. If an attacker is able to intercept all data being sent between a browser and a web server, they can see and use that information. This link ensures that all data passed between the web server and browsers remain private and integral. SSL is an industry standard and is used by millions of websites in the protection of their online transactions with their customers.

Figure 1: Website having SSL certificate

Why SSL exists?

1. Encryption- Hiding what is sent from one computer to another computer.
2. Identification- Making sure the computer you are speaking to is the one you trust.

Why do I need SSL on my site?

1. The Internet has new global business

opportunities for enterprises conducting online commerce.

2. However, that growth has also attracted fraudsters and cyber criminals who are ready to exploit any opportunity to steal consumer bank account numbers and card details.
3. Unless the connection between a client (e.g. internet browser) and a web server is encrypted, then any moderately skilled hacker can easily intercept and read the traffic.

How can I tell when my site uses SSL?

1. When a digital certificate is installed on a web page, users will see a padlock icon in the browser address bar. When an Extended Validation Certificates is installed on a web site, the address bar will turn green during secure sessions.
2. Users on sites with SSL Certificates will also see https:// in the address bar.

II. WORKING

SSL certificates are a tool that provides website protection and guarantees the confidentiality of data transmitted electronically. Full security is a result of the use of encrypted communication between computers. SSL certificates are registered on a particular domain name that contains information about the domain owner, his address, etc. This data is cryptographically protected and cannot be independently changed.

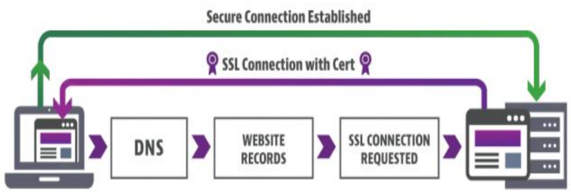


Figure 2: How SSL works?

How does SSL works?

1. When User/client wish to access secured website (HTTPS://) over the web.
2. Browser send a request to the server for establish a secured SSL connection.
3. Server responds back to the Browser with a copy of website's SSL certificate.
4. Browser checks the details of SSL Certificate, If the details matches and verifies than the Browser establish the HTTPS connections for that website. If Certificate details are fake or invalid the Browser display an error as "Connection is not secure/trusted".
5. Once the secure connection is established, the transferred information is encrypted over the internet using SSL Certificate.

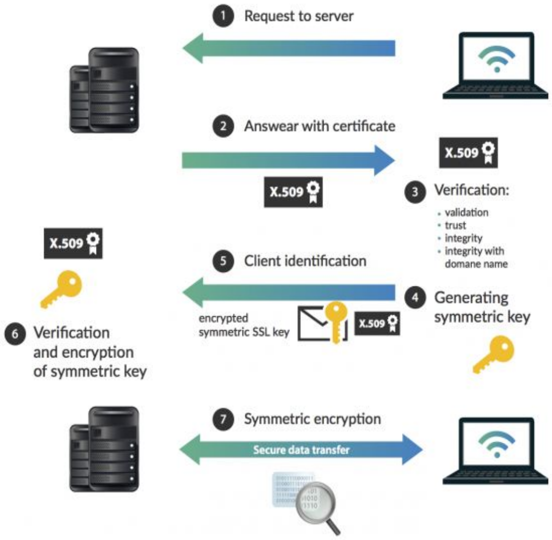

1 Request to server
2 Answear with certificate
X.509
X.509
3 Verification:
validation
trust
integrity
integrity with domane name
X.509
5 Client identification
4 Generating symmetric key
6 Verification and encryption of symmetric key
encrypted symmetric SSL key
X.509
7 Symmetric encryption
Secure data transfer

Figure 3: Working

III. METHODOLOGY

Prerequisites -

1) Apache web server
2) Root Access to VPN

Step 1) Activation of SSL Module

sudo a2enmod ssl

sudo service apache2 restart

Step 2) Creation of new directory for SSL certificate

sudo mkdir /etc/apache2/ssl

Step 3) Creation of Self-Signed SSL certificate

sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/apache2/ssl/apache.key -out /etc/apache2/ssl/apache.crt

openssl: This is the basic command line tool for creating and managing OpenSSL certificates, keys, and other files.

req: This subcommand specifies that we want to use X.509 certificate signing request (CSR) management. The "X.509" is a public key infrastructure standard that SSL and TLS adheres to for its key and certificate management.

-newkey rsa:2048: This specifies that we want to generate a new certificate and a new key at the same time. The rsa:2048 portion tells it to make an RSA key that is 2048 bits long.

Step 4) Setting up the certificate

nano /etc/apache2/sites-available/default-ssl

Step 5) Activation of new Virtual Host

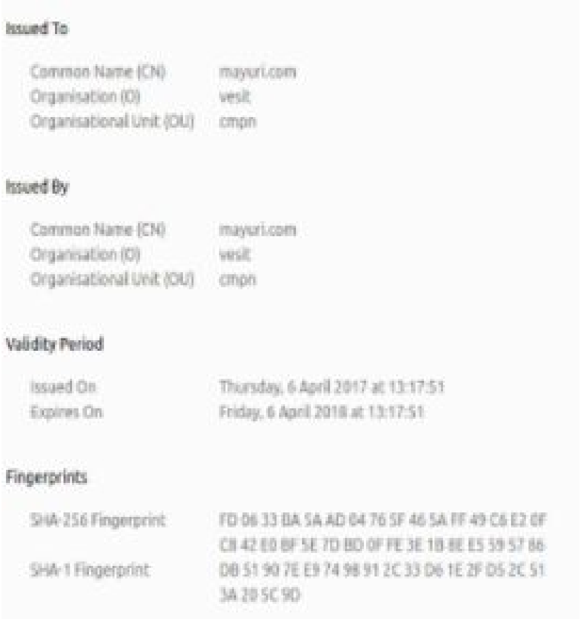
sudo a2ensite default-ssl

Step 6) Restart the apache service

Step 7) Go to the Web browser and type :

https://example.com

IV. EXPERIMENTAL RESULTS



Issued To

Common Name (CN) mayuri.com
Organisation (O) vesit
Organisational Unit (OU) cmpn

Issued By

Common Name (CN) mayuri.com
Organisation (O) vesit
Organisational Unit (OU) cmpn

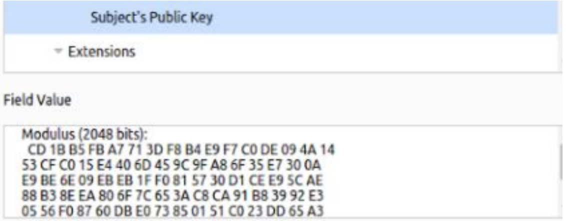
Validity Period

Issued On Thursday, 6 April 2017 at 13:17:51
Expires On Friday, 6 April 2018 at 13:17:51

Fingerprints

```
SHA-256 Fingerprint    FD 06 33 DA 5A AD 04 76 5F 46 5A FF 49 C6 E2 0F
                       C8 42 E0 BF 5E 7D BD 0F FE 3E 1B 8E E5 59 57 86
SHA-1 Fingerprint      DB 51 90 7E E9 74 98 91 2C 33 D6 1E 2F D5 2C 51
                       3A 20 5C 9D
```

Figure 4: SSL Certificate Generated



```
Modulus (2048 bits):
 CD 1B B5 FB A7 71 3D F8 B4 E9 F7 C0 DE 09 4A 14
53 CF C0 15 E4 40 6D 45 9C 9F A8 6F 35 E7 30 0A
E9 BE 6E 09 EB EB 1F F0 81 57 30 D1 CE E9 5C AE
88 B3 8E EA 80 6F 7C 65 3A C8 CA 91 B8 39 92 E3
05 56 F0 87 60 DB E0 73 85 01 51 C0 23 DD 65 A3
```

Figure 5: Public Key Generated

V. CONCLUSION

An SSL Certificate is a special file on your web server that enables encrypted security for online communications. SSL creates an encrypted connection between your web server and your visitor’s web browser allowing for private information to be transmitted without the problems of eavesdropping, data tampering, or message forgery.

VI. REFERENCES

[1] https://www.exabytes.my/web-security/ssl

[2] https://blog.webnames.ca/what-is-ssl/

[3]https://www.digitalocean.com/community/tutorials/how-to-create-a-self-signed-ssl-certificate-for-apache-in-ubuntu-16-04