International Journal of Interdisciplinary Innovative Research & Development (IJIIRD)

ISSN: 2456-236X

Vol. 03 Issue 01 | 2018

Authentication Certificate

[1]Shajal A. Tiwari , [2]Roshan M. Jaiswal

[1,2] *Department of Computer Science Mumbai Educational Trust College, Mumbai, India*

ABSTRACT

Most server authenticate user by the means of username and password technique. If one augments with another method that will make more difficult for imposters to break in. For servers whose users connect through web browsers, one option would be client certificate authentication. Authentication certificate points out most information security is currently based on secured socket layer, which are designed to encrypt messages from being violated during transmission. Most of the information security is currently based on SSL (secured socket layer).

General Terms: ***SSL (secured socket layer), TLS (Transport layer security)***

Keywords: ***Certification authority (CA), extended validation (EV) certificate, Web Host Manager (WHM), Certificate Signing Request (CSR).***

1. INTRODUCTION

Most information security is currently based on SSL (secured socket layer) which are designed to encrypt messages send from the browser before sending it to the server to prevent messages from being violated during transmission.

At the server level, the SSL decrypts the message and verifies that it came from the correct sender in am authentication process that compares encoded cipher keys that are contained in a certificate. The software should identify the damage to the information during transmission, before it actually arrives at the server.

A digital certificate is quiet similar to credit card that establishes credentials of member doing business or other transactions on the internet. It contains their name, serial number, expiration date, a copy of their certificate holder’s public key (used for encryption messages and digital signature), and the digital signature of the certificate issuing authority.

The actual information included on the certificate itself is not complex and is sometimes little more than the email address of the certificate administrator (CA).Certificate administrators (CAs) are usually large, well established organizations, successful in digital encryption technology, including AT&T,GTE and VeriSign.

SSL system currently offers both 40-bit and 128-bit encryption technology for certification, with the 128-bit system as the more difficult encryption technique for an intruder to break since it permits 3.4*1038 possible keys.

A more recently developed SSL system available for deployment only within United States has 168-bit encryption. Since the internet is functionally a global network, communications outside of the United States are constrained to operate at the lowest common global denominator of the 40-bit encryption system. This significantly heightens the risk of intrusion at all levels of e-commerce.

1.1 SSL (Secure socket layer) Certificate

SSL (Secured socket Layer) is a standard security protocol for establishing encrypted links between server and client, typically (a web server and a web browser) or a mail server and mail client (example outlook) in an online communication. The usage of SSL ensures that all data transmitted between the web server and browser remains encrypted.

SSL allows sensitive information like credit card numbers, social security numbers and login credentials to be transmitted securely. Normally, data sent between browser and web server is sent in plain text, living user vulnerable to eavesdropping. If an attacker is able to intercept all data sent between a browser and a web browser, they can see and use that information.

More specially, SSL is a secured protocol. Protocols describe how algorithm should be used. The SSL protocol determines variables of the encryption for both the links and the data being transmitted.
All browsers have the capability to interact with the secured web servers using SSL protocol. However, the browser and server need what is called an SSL certificate to be able to establish a secure connection.

Internet users have come to associate their online security with the lock icon that comes with an SSL – secured website or green address bar that comes with an extended validation SSL – secured website. SSL – secured websites also begins with https rather than http.

A SSL certificate comprises of your domain name, the company name and other things which can be your address, your city, your state and your country. It will also show the expiration date of the SSL plus details of the issuing CA. Whenever a browser initiates the connection with a SSL secured website, it will first retrieve the site's SSL certificate to check if it's still valid. It's also verified that the CA is one that browser trusts , and also that the certificate is being used by the website for which it has been used. If any of these checks fails, a warning will be displayed to the user, indicating that the website is not secured by a valid SSL certificate.

1.2 What is SSL/TLS certificate?

SSL or TLS (Transport layer security) certificates are data files that bind the cryptographic key to the details of the respective organization. On the installation of the SSL/TLS certificate on the web server a secure connection is created between the web server and the browser that connects to it. The padlock is showed on the address bar and the website's URL is prefixed with "https" instead of "http". A green address bar is shown by the browser if the website uses the extended validation (EV) certificate.

2. WHY WEBSITES' NEED SSL CERTIFICATE?

The internet has proved to be a great platform of new global business opportunities for business organizations conducting e-commerce. With this improvement of internet a gateway for opportunist is also created for fraudsters and cyber criminals who steal the customer's bank information and card details.
SSL has the capability to secure millions of users' data on internet. It is more cautious especially when comes to online transactions or when transfer of confidential information takes place.

2.1 work Process of SSL Certificate?

SSL Certificate works on "SSL Handshake mechanism".
A standard SSL handshake is as follows when RSA algorithm is used. RSA follows asymmetric cryptography algorithm. Asymmetric works on two different keys i.e public key and private key. An example of asymmetric cryptography.

1. A browser sends its public key to the server and requests for required data.
2. The server encrypts the data using browsers public key and sends the encrypted data.
3. The browser later decrypts the data on receiving it.

How SSL certificate works on a website:

1. A end user asks their browser to make the secure connection to a website. (for e.g. https://www.abc.com)
2. The browser then obtains the IP address of the website from DNS server and then requests a secure connection to the website.
3. To initiate this secure connection, the browser requests that the server identifies itself by sending a copy of its SSL certificate to the browser.
4. The browser checks the certificate to ensure the following:
   a) If it is signed by a trusted CA.
   b) Valid: If it is not expired or been revoked.
   c) If it's meeting the required standard on key lengths and other items.
   d) If the listed domains on the certificate matches the domain requested by the user.

5. When the browser ensures that the browser can be trusted, it creates the symmetric session key which it encrypts with the public key in the website's certificate. The session key is later sent to the web server.
6. The web server then uses its private key to decrypt the symmetric session key.
7. An acknowledgement is sent by the server that it is encrypted with the session key.
8. Here on, all the data transmitted between the server and browser is ensured to be encrypted and secure.

The following diagrammatic representation states how SSL works and how it appears to different web browsers.

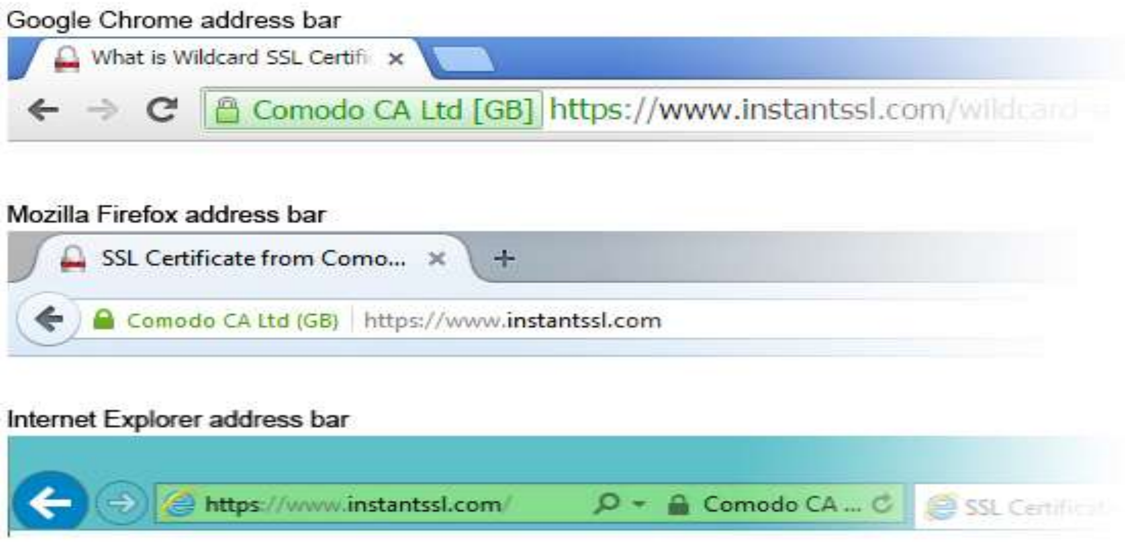
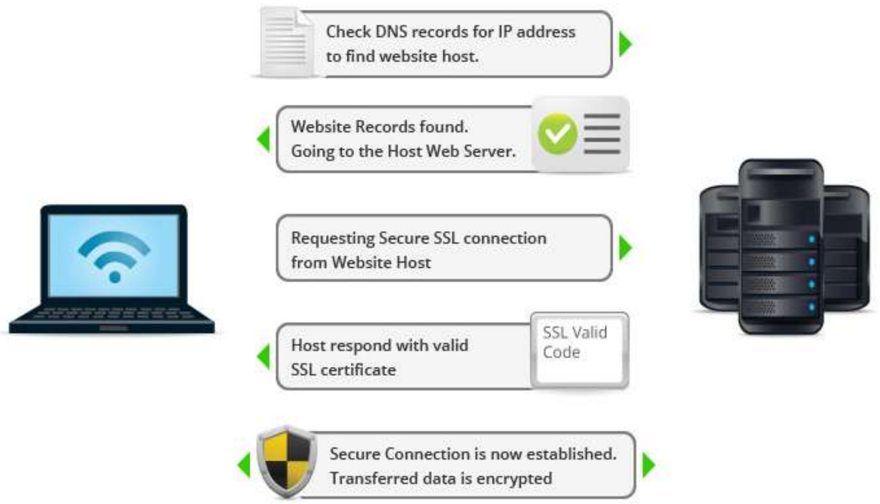

Google Chrome address bar
What is Wildcard SSL Certifi
Comodo CA Ltd [GB]
https://www.instantssl.com/wildcard
Mozilla Firefox address bar
SSL Certificate from Como...
Comodo CA Ltd (GB)
https://www.instantssl.com
Internet Explorer address bar
https://www.instantssl.com/
Comodo CA ...
SSL Certificat

Fig 1: SSL Certificate at different browsers


Check DNS records for IP address to find website host.

Website Records found. Going to the Host Web Server.

Requesting Secure SSL connection from Website Host

Host respond with valid SSL certificate

SSL Valid Code

Secure Connection is now established. Transferred data is encrypted

Fig 2: SSL Certificate process

2.2 Implementation of SSL

Implementing SSL on website is just an installation ahead. The steps involved in installation are as follows:

Step1. Acquiring the SSL Certificate.

From trusted CA one needs to get and install a certificate to implement SSL/TLS security on website. A trusted CA will have its roots in all major root store programs, that states certificate which is purchased will be trusted by internet browsers and mobile devices used by particular website visitor. It is also important to understand which kind of certificate is required. The types of certificate are as follows.

1. **Single domain certificates**: It allows securing one fully qualified domain name (FQDN).
2. **Wildcard certificates:** It secures a single domain and end number of sub domains of that domain. For example, a wildcard certificate for “abc.com” could also be used to secure “payments.abc.com”, “login.abc.com”.

3. **Multi-domain certificates:** This domain allows website owners to secure multiple, distinct domains on a one certificate. For example, a single MDC can be used to secure domain-1.com, domain-2.com, domain-3.co.in and etc.
4. **Extended validation certificates:** This kind of certificate provides the highest level of security, trust and customer conversion for online business. Due to this kind of certificates, EV certificates contain a unique differentiator designed to clearly communicate the trust level of the website to the visitors. Into this type of certificate whenever somebody visits a website which uses EV SSL, the address bar will turn into green for major browsers such as chrome, Firefox and internet explorer.

Step2. Activating and Installing the SSL Certificate.

The web host takes care of the activation when the SSL certificate is purchased from the web host. The administrator of the website has the rights to activate the SSL through Web Host Manager (WHM) or cPanel.

In WHM dashboard select the SSL/TLS option and choose “Generate SSL certificate and signing request”. Now, generate your private key by filling form for Certificate Signing Request (CSR).The domain name must be properly entered asked in the box for host to make cert for. Next, the CSR is send to respective CA to purchase certificate.

Step3. Updating the website from HTTP to HTTPS.

The website is now capable of https. The website is configured so that visitors can directly redirect to https whenever site is accessed.

3. ISSUE OF SSL CERTIFICATE

The certification authority (CA) issues SSL certificates. On receiving application, the CA verifies and checks for two factors. It confirms the legal identity of the company seeking the certificate and if the applicant controls the domain mentioned in the certificate.

The issued SSL certificates are linked to the “trusted root” certificate owned by the CA. Popular internet browsers like Firefox, chrome, Microsoft edge have these root certificate embedded in their “Certificate Store”. If the website certificate chains to the root in the certificate store then the browser allows the trusted and secure https connection. If the website certificate does not chain to a root then the web browser displays the warning that the connection is not secured.

3.1 Details Included In SSL Certificate

The details included in SSL certificate are as follows.
1. Details of whom the certificate is issued.
2. This includes the domain name/common name, serial number, the details of the issuer, period of validity (date of issue and expiry),SHA finger prints, subject public key algorithm, subject’s public key, certificate signature value, certificate signature algorithm.
3. The other details which are important as well are SSL/TLS version, type of certificate, certificate signature algorithm, perfect forward security status and cipher suite.
4. The organization having validation and extended validation certificate includes checked identity information regarding the owner of website, organization name, address, city, state and country.

4. CONCLUSION

With SSL certificate the websites’ security is ensured well. No of the offenders can offend into the website of the organization. All technicalities related to the SSL certificate gives the website and its domain the power and capability to keep it out from the cybercrimes and keeps it confidential.

The each step involved in process, implementation and issuing the certificate assures the website security.

5. REFERENCES

[1] https://www.digicert.com/ssl/
[2]https://www.instantssl.com/ssl-certificate.html
[3] https://www.geeksforgeeks.org/rsa-algorithm-cryptograph