TME4- WSM- SSL/TL

SSL/TLS

What is meant by SSL and TLS? Explain the working of SSL and TLS.

One of the most important thing in doing online business is that the connection should be secure and trusted. The SSL also known as Secure Sockets layer uses public-key encryption meaning that it helps in delivering the sensitive information under the pre-defined prototypes. Without the use of SSL, anyone can easily eavesdrop and also can easily steal information. It helps to provide reliability, efficiency and privacy. SSL is the predecessor of TLS(Transport Layer Security), they both belong to the family of certificates used in web browsers and web applications for data transfer.

To set up a secure SSL/TLS certificate or connection one has to go through various steps in order to do so. Our web browsers address these days are Https which means that SSL layer is applied to it. This is done once the secure page is requested by the browser. After receiving the request it check series of things in order such as: is the certificate comes from a trusted party, is the certificate still or currently valid and the relationship between the site and certificate.

If one has to use the certificate on the website, one has to go these checks. likely pass along securely. After this is passed, the browser uses a public key to encrypt a random key. When two computers are ready to make a connection, then a secure session is made under which symmetric key is sent from one computer to another. After the key is exchanged the session begins and the machines starts interacting with each other. After the session is finished, each machine throws the key in the recycle bin so that it is not used again.

To get a certificate on your server one has to create a private and public key on the server. The CSR data sends to the SSL certificate issuer called a certificate authority contains a public key. The machine uses the data file and create a data structure to match your private key. If it matches the connection is made successful. After this one will receive a certificate which can be installed on the server. The installation and testing of the certificates will be different depending on the server and the requirements of the server. This is also known as handshake in technical terms when the keys are exchanged and a secure connection is made. SSL latest version is 3.0 which is used worldwide.

Please find the following steps in order to make a Client-Server Connection:

- Imagine, we want to send our client ?Hello? in a message which will be encrypted and we will set it up with the preferences of the client. The message will contain a public key and random bytes as well so that the right compression methods are supported by our client.

- Ther SSL or TLS server will then respond saying ?Hello? from the list provided by the client. It will then have a session ID and random byte strings. Also an certificate would be send which will be a digital certificate. If the authentication is required the server sends another request to the client for the authentication. The server will then send list of the types of certificates supported by the client.

- Verification takes place while this happens. If the verification is successful then the connection will be made and random bytes would be sent to the client to check the certificates and the working but all of this happens once the public key is passed.

-

If SSL server sends a request to the client certificate request, if the connection is success, it will give a prompt that it is successful or it will give an alert saying that handshake failed due to the error.

- The SSL or TLS server verifies the client's certificate for the secure and private connection

- The SSL client sends a finish message to the server saying that the handskake was successful.

Also now a days, during a SSL and TLS session, the server and client can now deliver symmetrically encrypted messages with shared secret key.

References:

https://www.digicert.com/ssl/

https://tools.ietf.org/html/rfc6101

https://www.ibm.com/support/knowledgecenter/en/SSFKSJ_7.1.0/com.ibm.mq.doc/sy10660_.htm

https://www.hostingadvice.com/how-to/tls-vs-ssl/