What is SSL and how it works

-By hariharan.L

It is a protocal to secure application data when transmitted over a network.protocal means set of rules.TCP/IP model contain 5 layers.there are Application,Transport,Network,Data Link and Physical layers.SSL stands for Secure Socket Layer and TLS stands for Transport Layer Security.both term are used interchangeably.SSL contains many versions like SSLv3/TLS1.0/TLSv1.1/TLSv1.2/TLSv1.3.

Application data convert the secure data send to the Transport layer using SSL/TLS.transport layer contain two protocals.one is connection oriented protocal(TCP) and another one is connection less protocal(UDP).SSL/TLS should be supported only TCP.

popular SSL library
openssl(most popular)
LibreSSL(openBSD)
BoringSSL(google)
schannel(microsoft)
secure transport(apple)
GnuTLS
s2n(amazon)

How it works

Secure Message Transport

- ➢ confidentiality
  - cryptography
    - encryption/decryption using key concept.key produced by key generator.
    - encryption using some popular method like Modular Arithmetic.Modular Arithmetic contains Mod 2 addition.

- mod 2 addition speciality:
  probability of getting a zero and one is 50-50.hence it is good encryption function.mod 2 addition is also called XOR operation.easy to implement in hardware and software.
- p = 3 and k = 9(where p means message and k means key)

```
p -> 3 ->0011
k -> 9 ->1001
         ------
c = 10 <-1010
k -> 9 ->1001
         ------
p -> 3 <-0011
```

private/secret key cryptography(symmetric key cryptography)-both encryption and decryption using same key.

public key cryptography(asymmetric key cryptography)-encryption and decryption using different key.

Ciphers:

->symmentric cipher types:stream cipher,block cipher

stream cipher:

->encrypt one bit/byte/word at a time . it means cipher text nothing but adding plain text and key.key is random number generated by keystream generator.

->synchronous stream cipher.

->asynchronous stream cipher.

- cryptanalysis

  ->how to break encryption to find the plaintext or recovery key.

  ->crytanalysis working persons called cryptanalyst.

➢ integrity(hashing function)

➢ authenticity(MAC)

➢ non-repudiation

➢ no replay

SSL certificate ensure the data you send online are read by only the intended recipient and none else.In this process,the data traverse multiple computers before they reach the recipient .On the way,the data could be accessed by unauthorized third parties.However ,SSl makes some changes in the original data so that the data cannot be read by the third parties.