Computer Network Security

TE - IT

Lecture -18
06/09/2022

Session: 11:00 - 12:00 PM

Prof. Stella J
Department of Information Technology
Xavier Institute of Engineering

Module-4

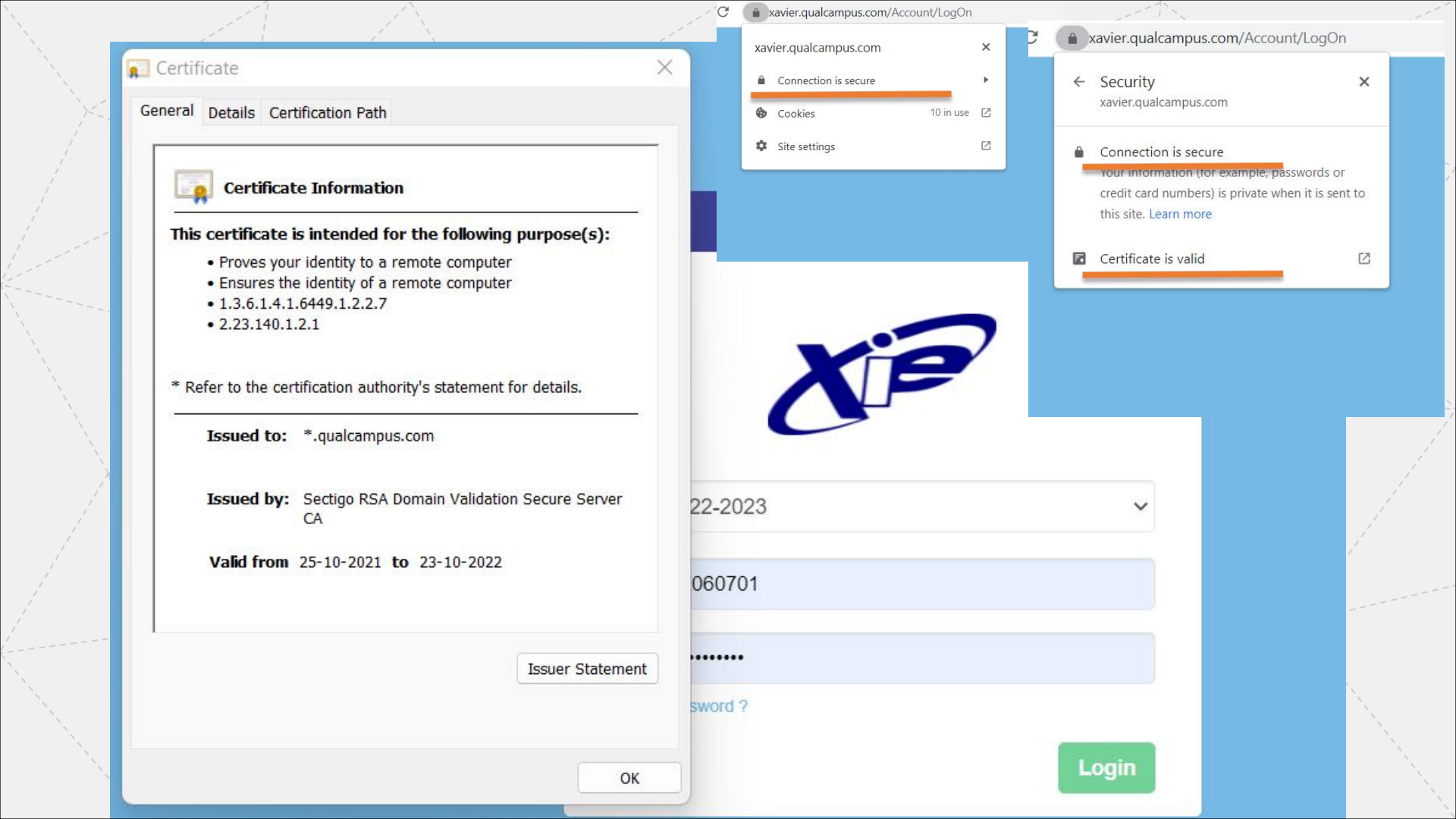
Web Security Consideration

1. Secure Socket Layer Architecture / Transport Layer Security
2. HTTPS
3. Secure Shell Protocol Stack

Web Security

World wide web or just web is a collection of web servers that runs several websites that hold the desired information.

Mostly used Browsers: Internet Explorer, Chrome, Firefox,Safari etc

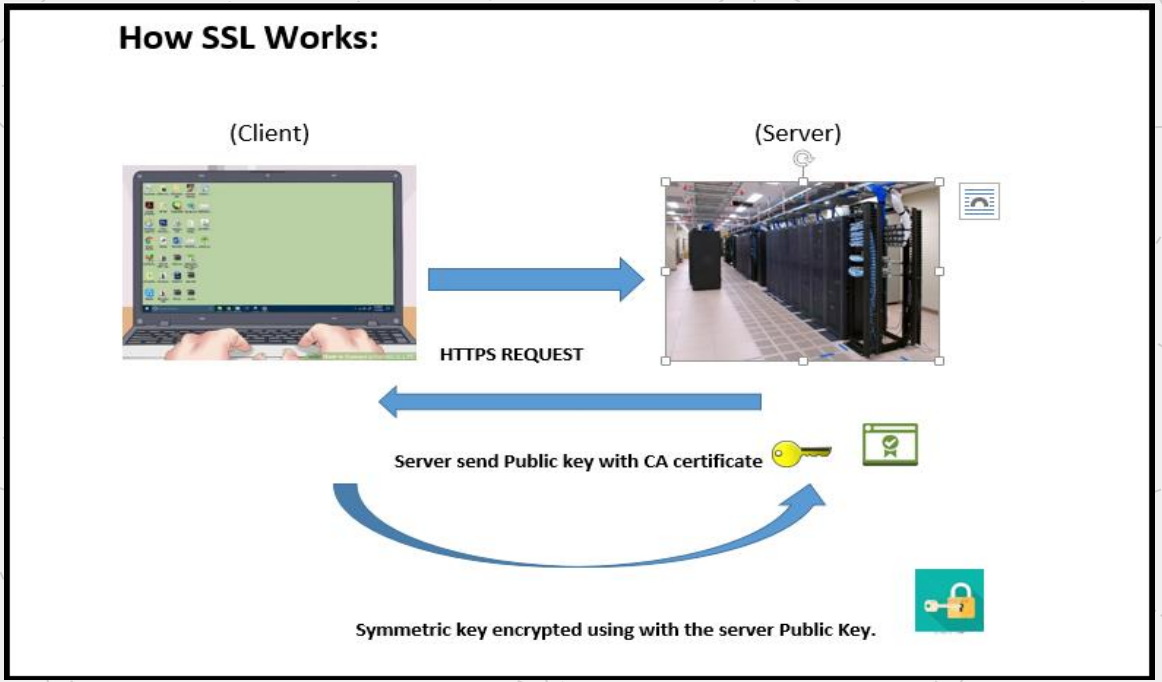

xavier.qualcampus.com/Account/LogOn
xavier.qualcampus.com
Connection is secure
Cookies
10 in use
Site settings
xavier.qualcampus.com/Account/LogOn
Security
xavier.qualcampus.com
Connection is secure
Your information (for example, passwords or credit card numbers) is private when it is sent to this site. Learn more
Certificate is valid
Certificate
General
Details
Certification Path
Certificate Information
This certificate is intended for the following purpose(s):
• Proves your identity to a remote computer
• Ensures the identity of a remote computer
• 1.3.6.1.4.1.6449.1.2.2.7
• 2.23.140.1.2.1
* Refer to the certification authority's statement for details.
Issued to: *.qualcampus.com
Issued by: Sectigo RSA Domain Validation Secure Server CA
Valid from 25-10-2021 to 23-10-2022
Issuer Statement
OK
22-2023
060701
sword ?
Login

Secure Socket Layer

The Secure Socket Layer and Transport Layer Security are the most widely use web security protocol. It is essentially a protocol that provides a secure channel between two machines operating over the internet

Secure Socket Layer

Def: SSL is a cryptographic protocol designed to protect communication between two entities



Connection: Transport to provide the service

Connection state Parameters:

1. server and client random
2. server write MAC secret
3. client write MAC secret
4. server write key - Shared key by server
5. Intialization vector
6. Sequence number - Based on BW the data is fragmented and sent with sequence number

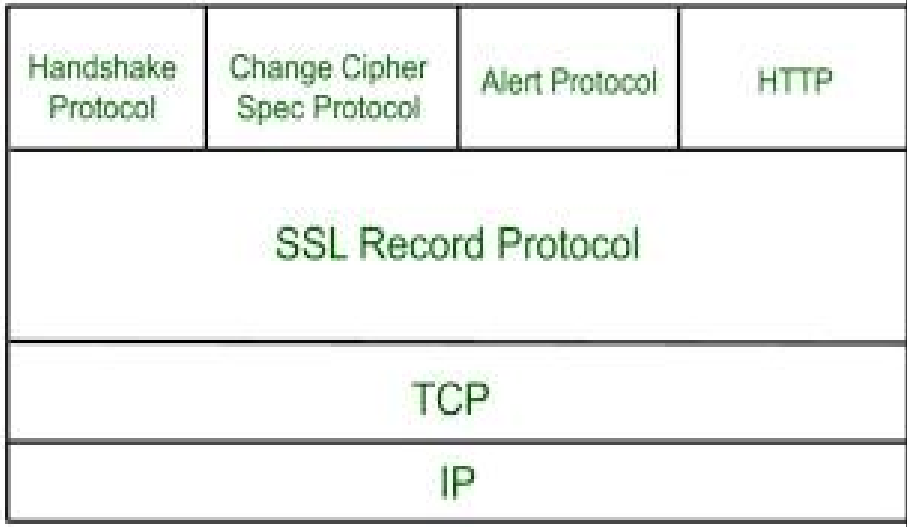
Session: Association between client and server

Session state Parameters:

1. Session identifier
2. Peer certificate - X.509 Certificate provided by CA
3. Compression method
4. Cipher spec - Encryption & Authentication Algorithm
5. Master Secret - Secret key shared among the client & server
6. IS Resumble - Flag

SSL Protocols

SSL uses different protocols for secure transmission of data. This works in Layers. At each layer messages may include fields for length, description, and content.



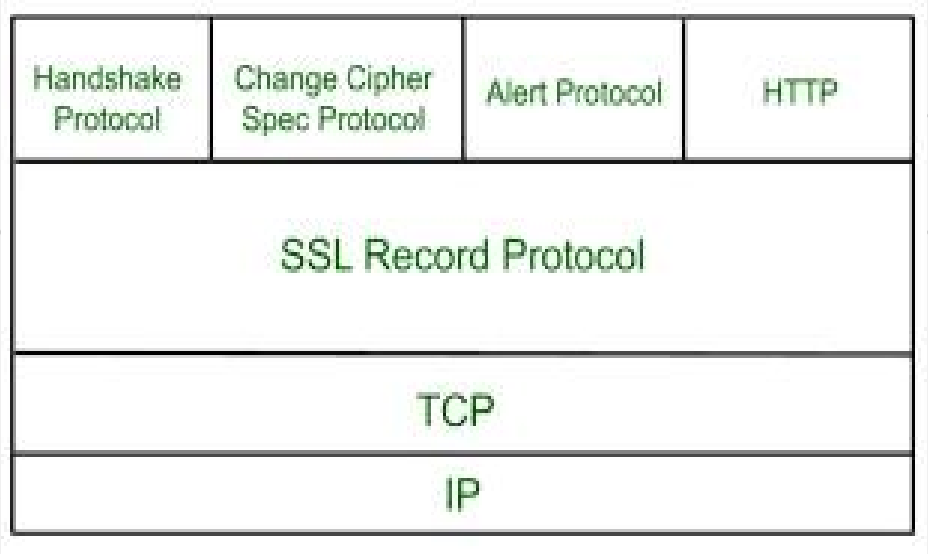
SSL takes messages to be transmitted, fragments, compress and applied MAC, encrypts and transmit.

On the Rx side, It decrypt, verify, decompress and reassembled and then delivered to higher level clients

SSL Protocols

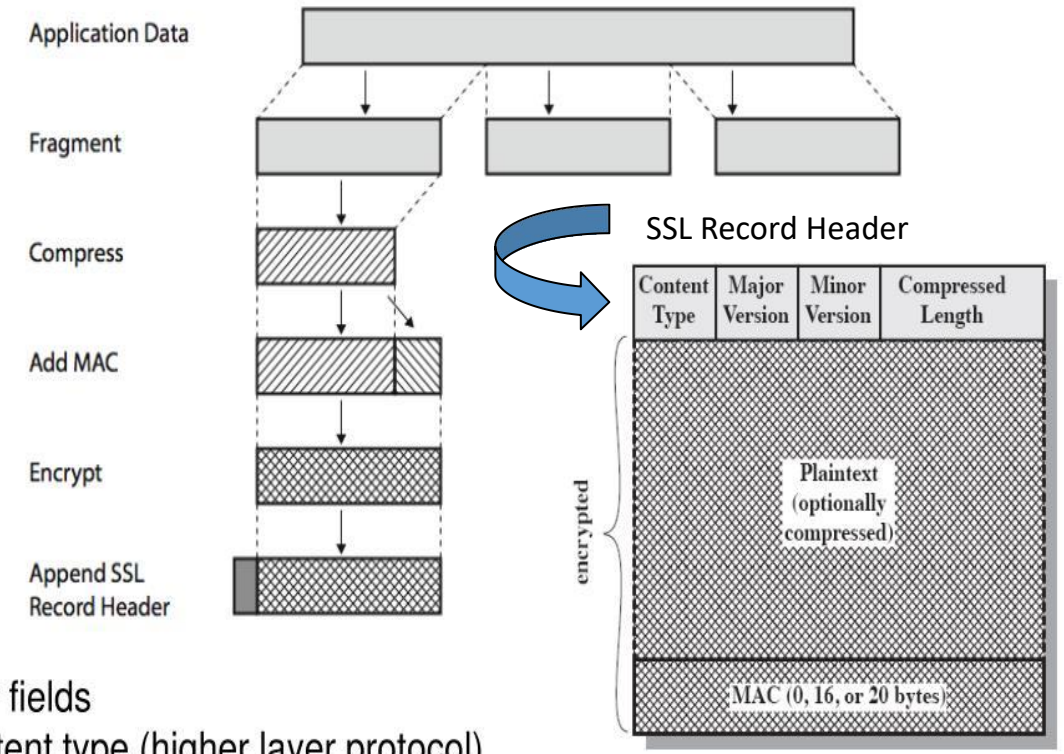
SSL uses different protocols for secure transmission of data

1. SSL Record Protocol
2. Handshake Protocol
3. Change Cipher Spec Protocol
4. Alert Protocol



SSL Record Protocol:

The SSL Record Layer is the last protocol that receives the raw data from the higher application layers and other SSL protocols such as handshake



header fields

- content type (higher layer protocol)
  - change_cipher_spec, alert, handshake, application data
- version
- compressed length (or plaintext length if no compression) of the fragment

Generating MAC:

Hash(MAC_write_secret || Pad-2 || Hash(MAC_write_secret || Pad-1 || Seq_num || SSL Compressed Length || SSL Compressed Type || SSL Compressed Fragment))

Pad-2 = 0101 0110
Pad-1 = 0011 0110

48 times repeated for MD5
40 times repeated for SHA-1

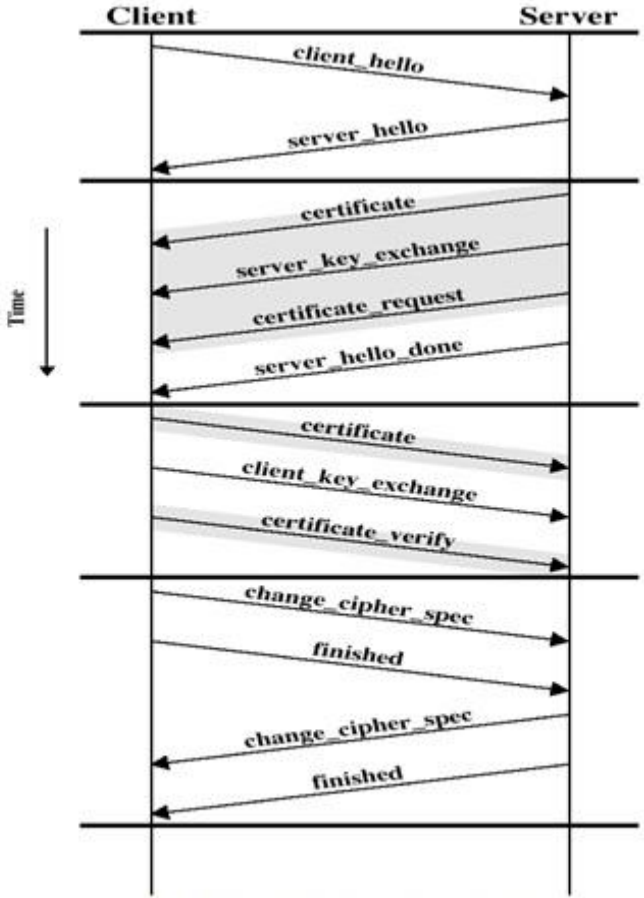
SSL Handshake Protocol:

SSL Handshake protocol allows following between client and Server. The handshake is done before any data is transmitted

- 1. to authenticate each other
- 2. to negotiate encryption and MAC algorithms
- 3. to create cryptographic keys to be used
- 4. to establish a session and then a connection

There are four phases in SSL handshake protocol. Following series of messages are used in these 4 phases.

- Phase-1: Establish Security Capabilities
- Phase-2: Server Authentication and Key Exchange
- Phase-3: Client Authentication and Key Exchange



SSL Handshake Protocol

SSL Handshake Protocol:

Message Type	Parameters
•Hello_request	•Null
•Client_hello	•version random •session Id •cipher suite •compression method
•Server_hello	•version random •session Id •cipher suite •compression method
•Certificate	•Chain of X.509-v3 certificates
•Server_key_exchange	•Parameters •signature,
•Certificate_request	•type •authorities
•Server_done	•NULL
•Certificate_Verify	•Signature
•Client_Key_exchange	•parameters •signature
•Finished	•Hash Value

SSL Handshake Protocol:

Phase#1: Establish security capabilities, including protocol version, session ID, cipher suite, compression method, and initial random numbers.

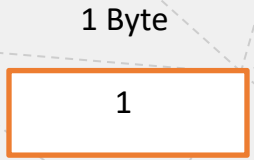
Phase#2: Server may send certificate, key exchange, and request certificate. At this stage, server signals end of the hello message phase.

Phase#3: Client transmits certificate if needed. Client transmits key exchange. Client may transmit certificate verification.

Phase#4: Change cipher suite and finish handshake protocol.

Change Cipher Spec Protocol:

- The change cipher spec protocol notifies about the changes in cipher parameters.
- It is used to change the encryption being used by the client and server.
- It is a 1 Byte data tells the server about the changes need to be done in the keys



Change Cipher Spec Protocol

Alert Protocol:

Conveys SSL-related alerts to peer entity

Two byte message: Level-Alert, level=warning or fatal,
fatal⇒Immediate termination

0 Close notify (warning or fatal)

10 Unexpected message (fatal)

20 Bad record MAC (fatal)

21 Decryption failed (fatal, TLS only)

22 Record overflow (fatal, TLS only)

41 No certificate (SSL v3 only) (warning or fatal)

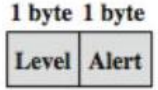
42 Bad certificate (warning or fatal)

43 Unsupported certificate (warning or fatal)

44 Certificate revoked (warning or fatal)

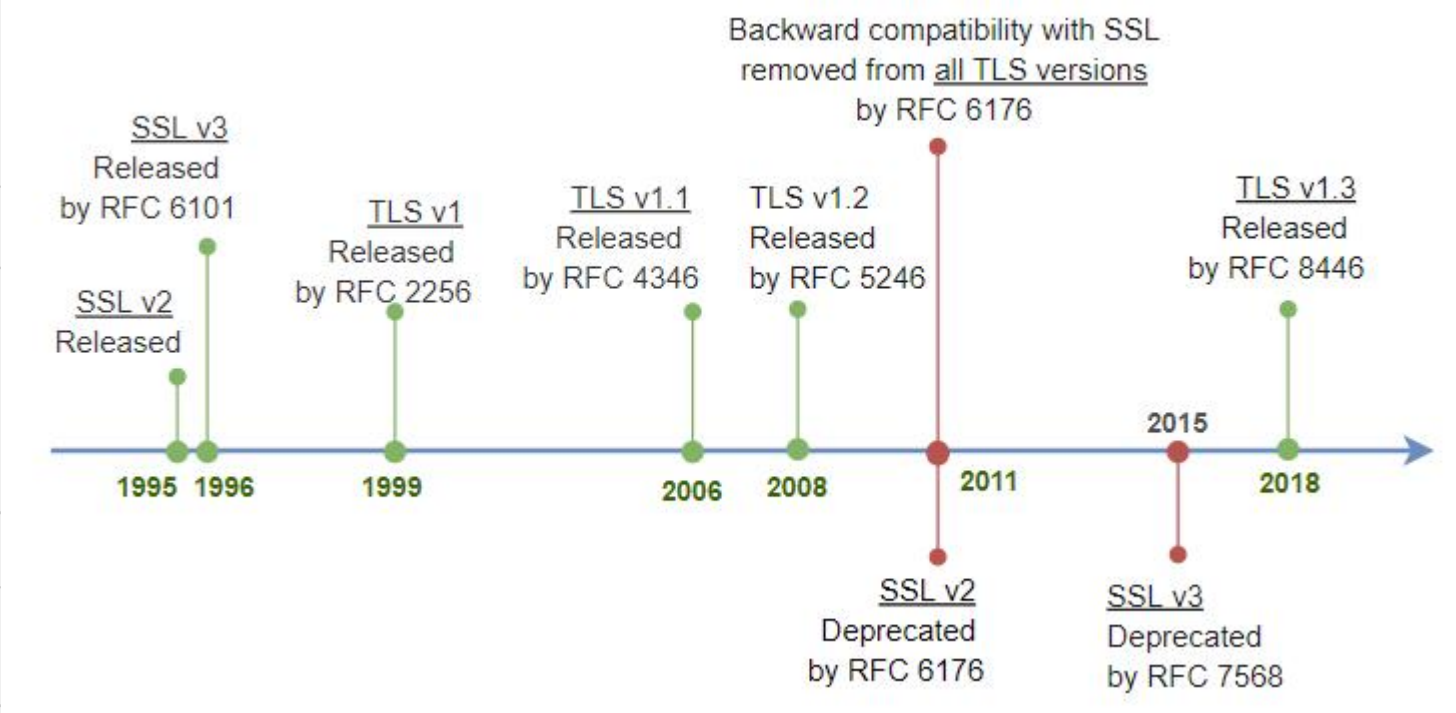
45 Certificate expired (warning or fatal)

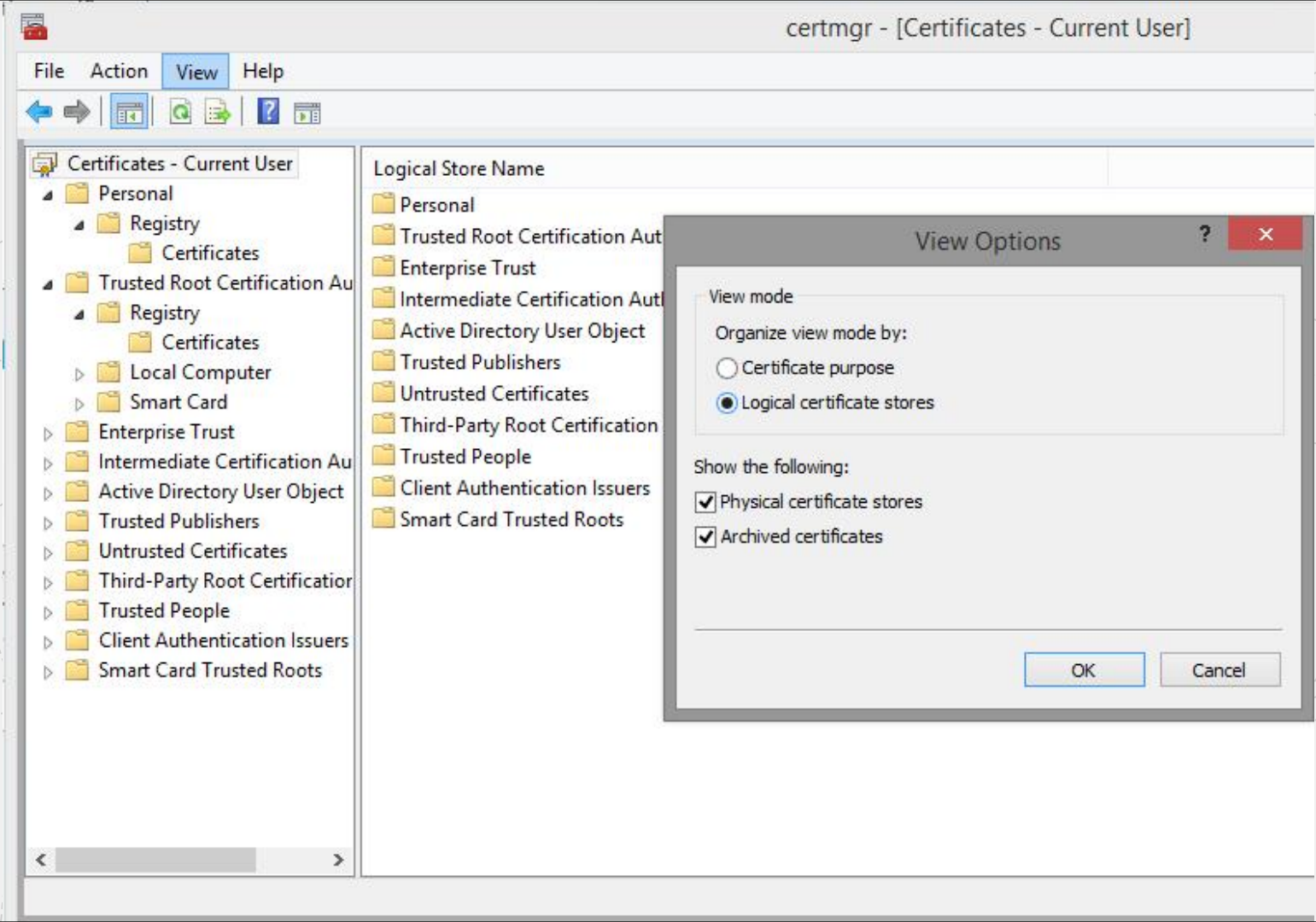
....



(b) Alert Protocol

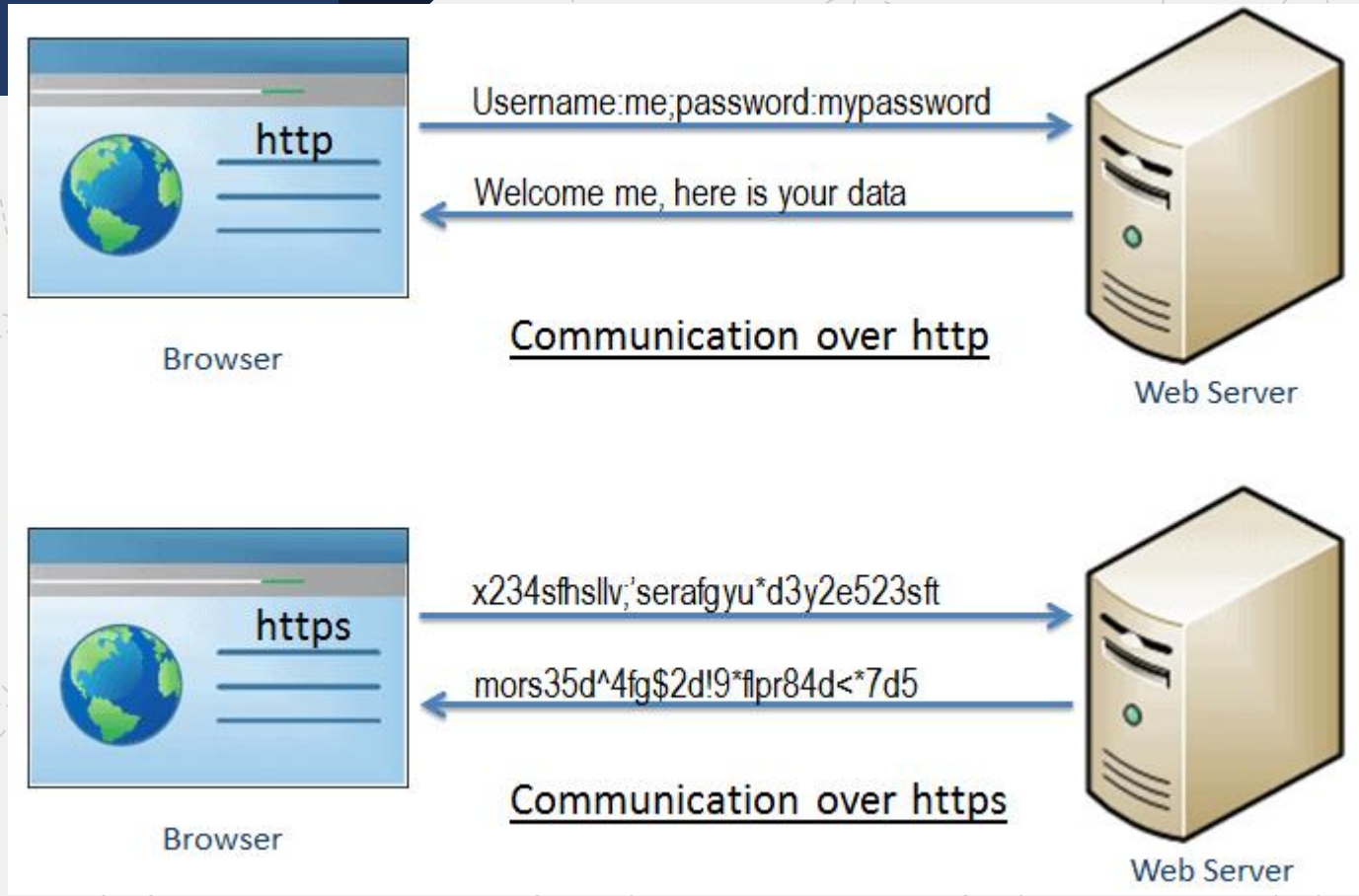
SSL Version


Backward compatibility with SSL removed from all TLS versions by RFC 6176
SSL v3 Released by RFC 6101
SSL v2 Released
TLS v1 Released by RFC 2256
TLS v1.1 Released by RFC 4346
TLS v1.2 Released by RFC 5246
TLS v1.3 Released by RFC 8446
1995
1996
1999
2006
2008
2011
2015
2018
SSL v2 Deprecated by RFC 6176
SSL v3 Deprecated by RFC 7568


certmgr - [Certificates - Current User]
File
Action
View
Help
Certificates - Current User
Personal
Registry
Certificates
Trusted Root Certification Au
Registry
Certificates
Local Computer
Smart Card
Enterprise Trust
Intermediate Certification Au
Active Directory User Object
Trusted Publishers
Untrusted Certificates
Third-Party Root Certificatior
Trusted People
Client Authentication Issuers
Smart Card Trusted Roots
Logical Store Name
Personal
Trusted Root Certification Aut
Enterprise Trust
Intermediate Certification Autl
Active Directory User Object
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification
Trusted People
Client Authentication Issuers
Smart Card Trusted Roots
View Options
View mode
Organize view mode by:
Certificate purpose
Logical certificate stores
Show the following:
Physical certificate stores
Archived certificates
OK
Cancel

HTTPS:

HTTPS:


http
Username:me;password:mypassword
Welcome me, here is your data
Browser
Communication over http
Web Server
https
x234sfhsllv;'serafgyu*d3y2e523sft
mors35d^4fg$2d!9*flpr84d<*7d5
Browser
Communication over https
Web Server

HTTP VS HTTPS:

HTTP	HTTPS
URL begins with http://	URL begins with http://
The request is processed through port 80 by default	The request is processed through port 443 by default
Fast transfer of unencrypted data over a simpler protocol	Longer data transfer, as there are additional steps to provide encryption (handshake, certificate verification)
Not safe, vulnerable to MITM attacks and traffic interception	Safe- maximizes the complexity of traffic and information interception
Main purpose - data exchange on the Internet	Main purpose - confidential data exchange, including the exchange through unsafe networks.
Does not improve search ranking	Improves search ranking
Does not save data about the referring website and displays referral traffic as direct	Stores data about the referring websites and significantly increases the accuracy of analytic services
Does not support AMP	Is required for AMP
Is less trustworthy	Is more trustworthy
Perfect fit for blogs, forums, educational and entertainment websites	Perfect fit for commercial and financial websites, and services that require confidentiality of data

THANK YOU