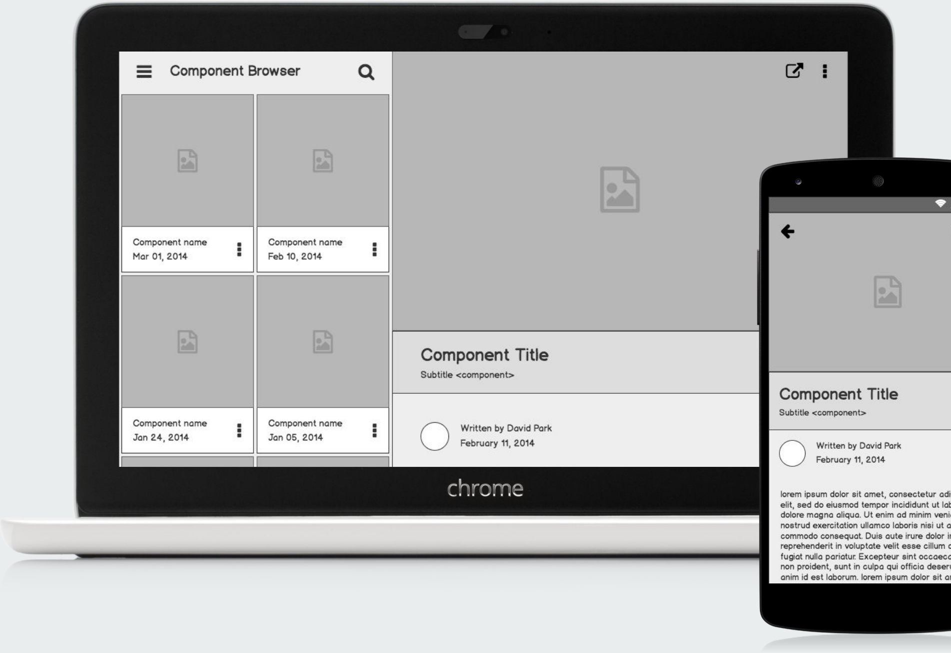
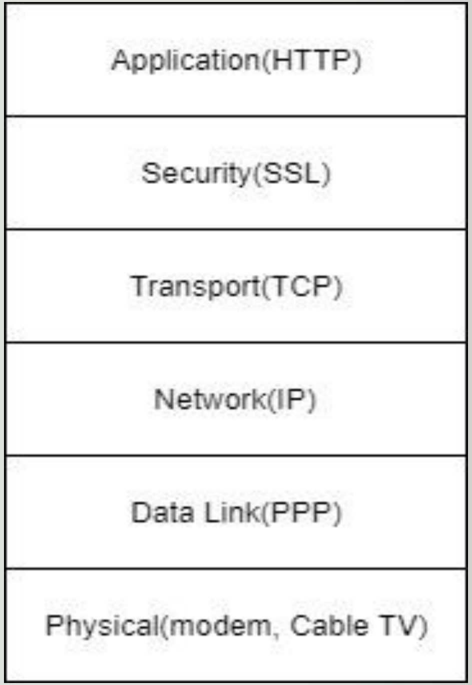
HTTPS & Certificates

AAYUSH - 00151203116
CHITRESH - 00651203116
SHIVAM - 02951203116
DEVANG - 40651203116
VARUN - 41351203116



What is HTTPS ?



Application(HTTP)

Security(SSL)

Transport(TCP)

Network(IP)

Data Link(PPP)

Physical(modem, Cable TV)

- It stands for hypertext Transfer Protocol over Secure Socket Layer, or HTTP over SSL.

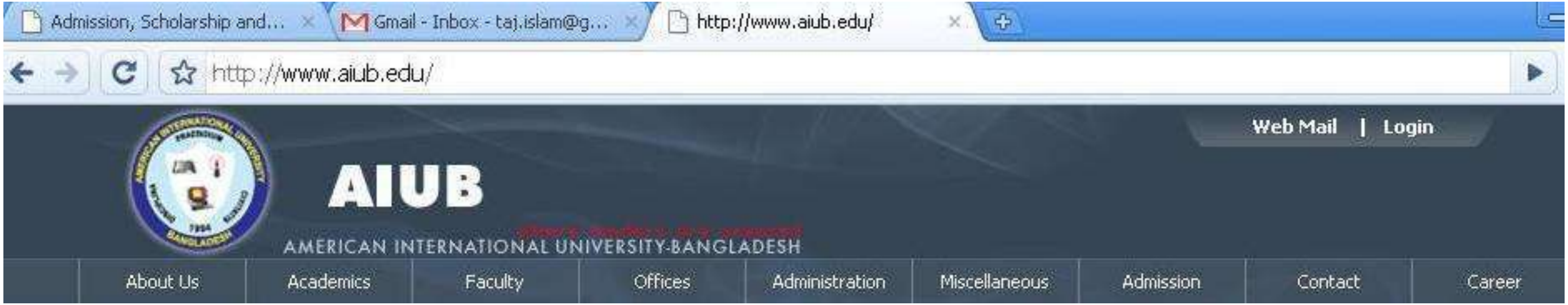
HTTP VS HTTPS

- On the basis of uses ?
- Security ?
- Works in Model’s which layer ?
- Certificate ?
- Encryption ?
- Transfering of data ?

Limitation of HTTPS

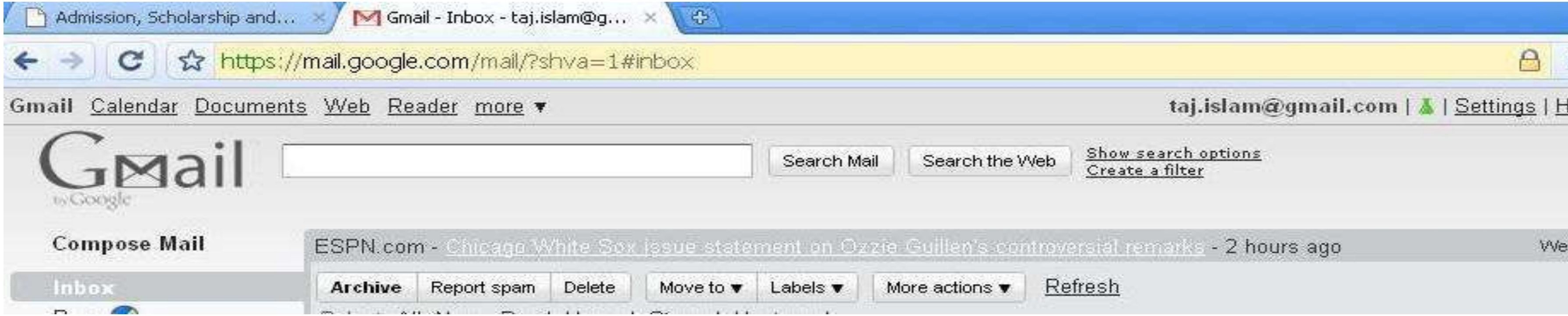
- An HTTPS server can only provide one “virtual host” behind a single socket, as opposed to multiple ones behind an http socket.
- HTTPS cannot prevent stealing confidential information from the pages cached on the browser.
- HTTPS is slightly slower than HTTP.

HOW IT WORKS IN BROWSER: HTTP



http://www.aiub.edu/

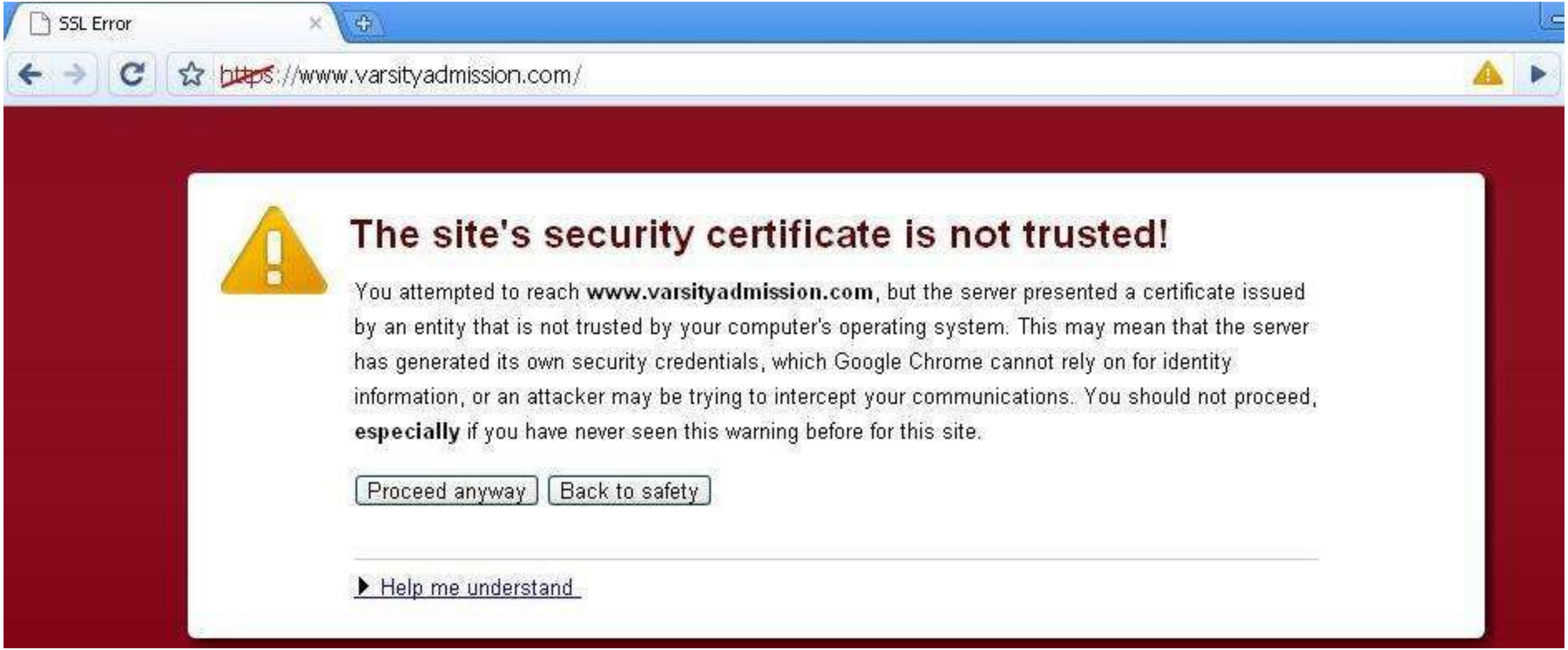
HOW IT WORKS IN BROWSER: HTTPS



https://mail.google.com/mail/?shva=1#inbox

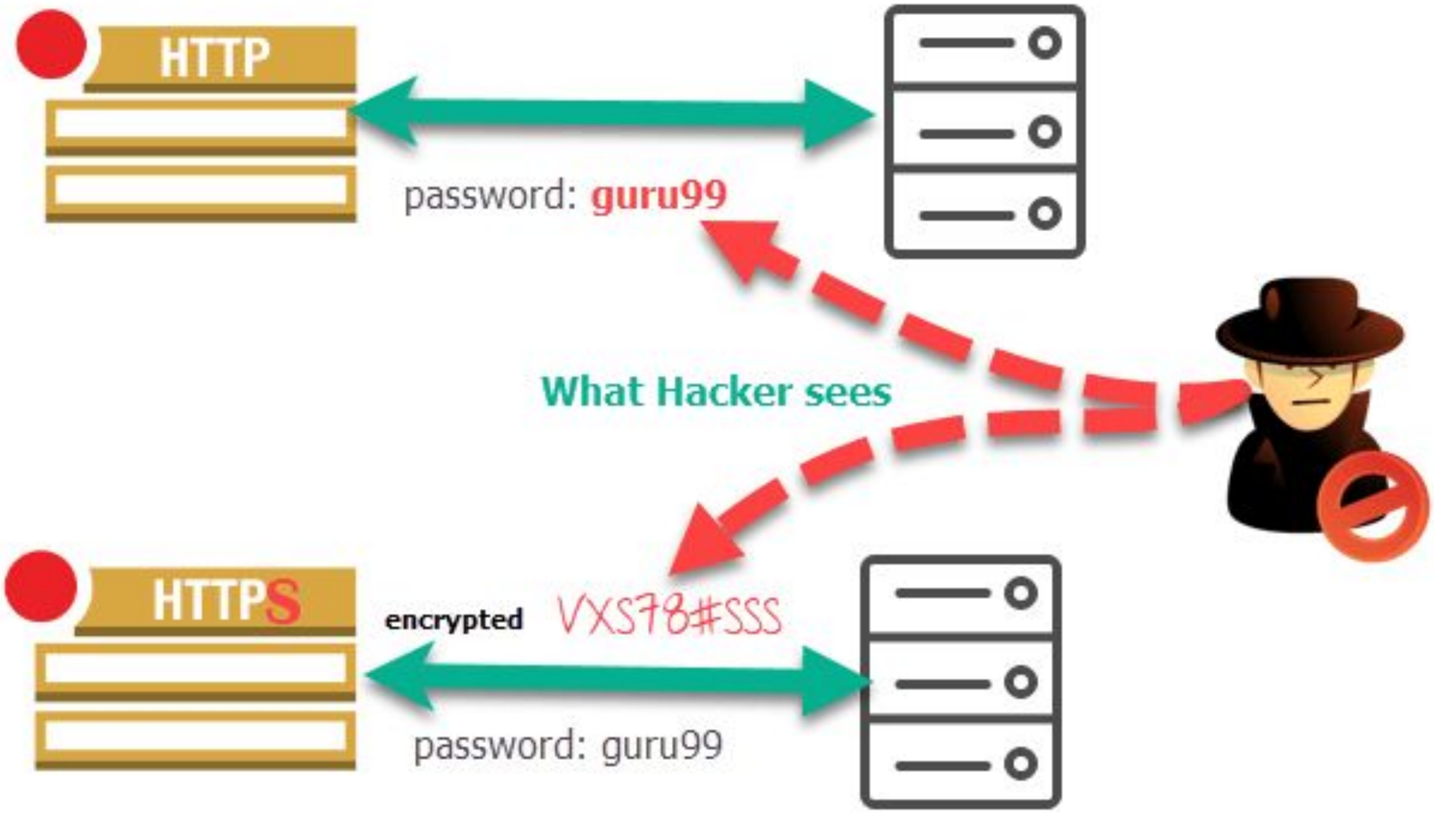
ESPN.com - Chicago White Sox issue statement on Ozzie Guillen's controversial remarks - 2 hours ago

HOW IT WORKS IN BROWSER:
HTTPS WITHOUT CERTIFICATION



The site's security certificate is not trusted!

You attempted to reach **www.varsityadmission.com**, but the server presented a certificate issued by an entity that is not trusted by your computer's operating system. This may mean that the server has generated its own security credentials, which Google Chrome cannot rely on for identity information, or an attacker may be trying to intercept your communications. You should not proceed, **especially** if you have never seen this warning before for this site.


HTTP
password: guru99
What Hacker sees
HTTPS
encrypted
VXS78#SSS
password: guru99

WHY SSL ??

SSL Certificates are small data files that digitally bind a cryptographic key to an organization’s details. When installed on a web server, it activates the padlock and the https protocol and allows secure connections from a web server to a browser.

Finally It is safe.
:)

What does SSL concern ?

- SSL includes two sub protocols:

1. Record Protocol - defines the format used to transmit data
2. Handshake Protocol - using the Record protocol to exchange messages between an SSL-enable server and SSL enable client.

Useful Terms

Digital Signature - A message digest derived from the original one, has following important properties:

- ➔ The digest is difficult to reverse
- ➔ It is hard to find a different message that computed to the same digest value

Useful Terms

A certificate has following content :

- ➔ The certificate issuer’s name
- ➔ The entity for whom the certificate is being issued (aka the subject)
- ➔ The public key of the subject
- ➔ Some time stamps

TYPES OF CERTIFICATES.

Domain Validated Certificate

Domain Validated certificates are certificates that are checked against domain registry. There is no identifying organizational information for these certificates and thus should never be used for commercial purposes. It is the cheapest type of certificate to get, but this is a high risk certificate use on a public website.

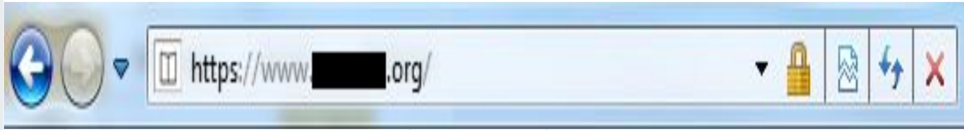
Organization Validated Certificate

Organizational certificates are Trusted. Organizations are strictly authenticated by real agents against business registry databases hosted by governments. Documents may exchange and personnel may be contacted during validation to prove the right of use.

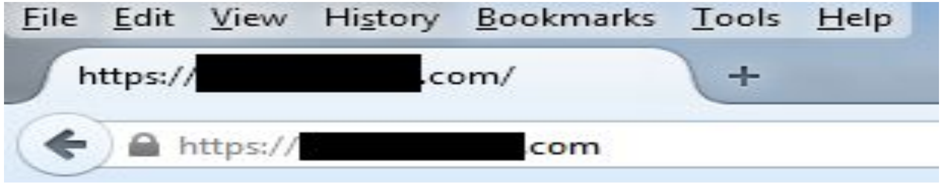
Extended Validation Certificate

Nothing provides more trust and security than Symantec Extended Validation Certificates. It is used by most of the world’s leading organizations. They have found that switching from OV to EV certificates increases online transactions and improve customer confidence. It is no longer a luxury but a necessity.

HOW TO VISUALISE BETWEEN DIFFERENT TYPES OF CERTIFICATES ???


https://www.[redacted].org/

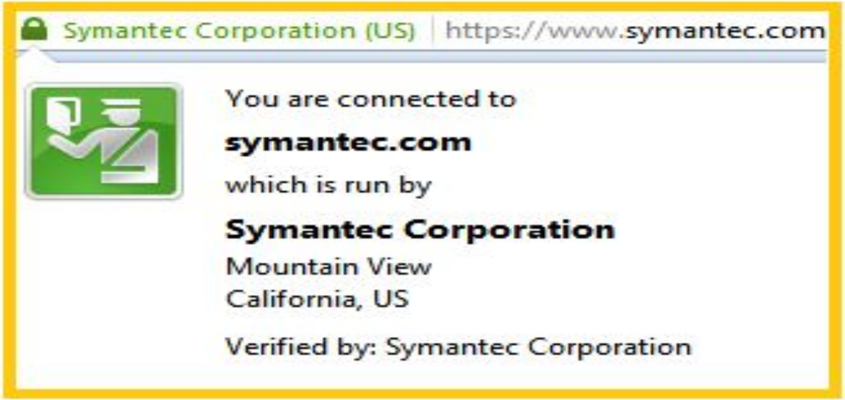
DOMAIN VALIDATED CERTIFICATE.



https://[redacted].com/

https://[redacted]com

ORGANISATION VALIDATED CERTIFICATE


Symantec Corporation (US) | https://www.symantec.com

You are connected to

symantec.com

which is run by

Symantec Corporation

Mountain View

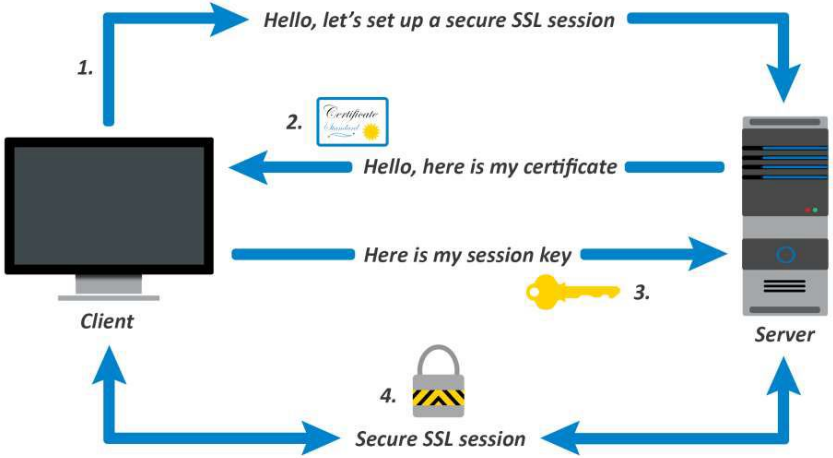
California, US

Verified by: Symantec Corporation

EXTENDED VALIDATION CERTIFICATE

Server Authentication

- Server Authentication is a means of authenticating and identifying the server to the client using a Server Certificate.
- A Server Certificate is a required part of any SSL communication. The server certificate contains basic information and a digital signature that properly identifies the server it is associated with.



Mutual or “Two-Way” Authentication

➔ Mutual Authentication, also commonly referred to as Two-Way Authentication, refers to the combination of both Server and Client Authentication.

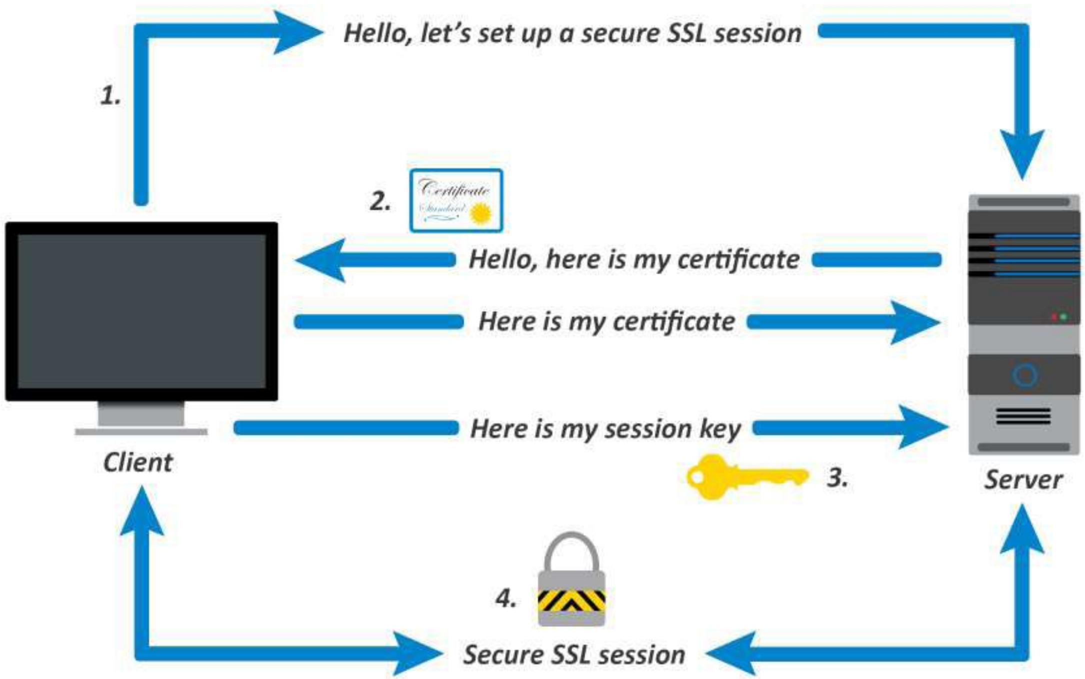
➔ The authentication is mutual, or two-way, because the server is authenticating itself to the client, and the client is authenticating itself to the server.

Client Authentication

- Client Authentication, similar to server authentication, is a means of authenticating and identifying the client to the server using a Client Certificate.

- A Client Certificate contains basic information about the client's identity, and the digital signature on this certificate verifies that this information is authentic.

Mutual Authentication Diagram

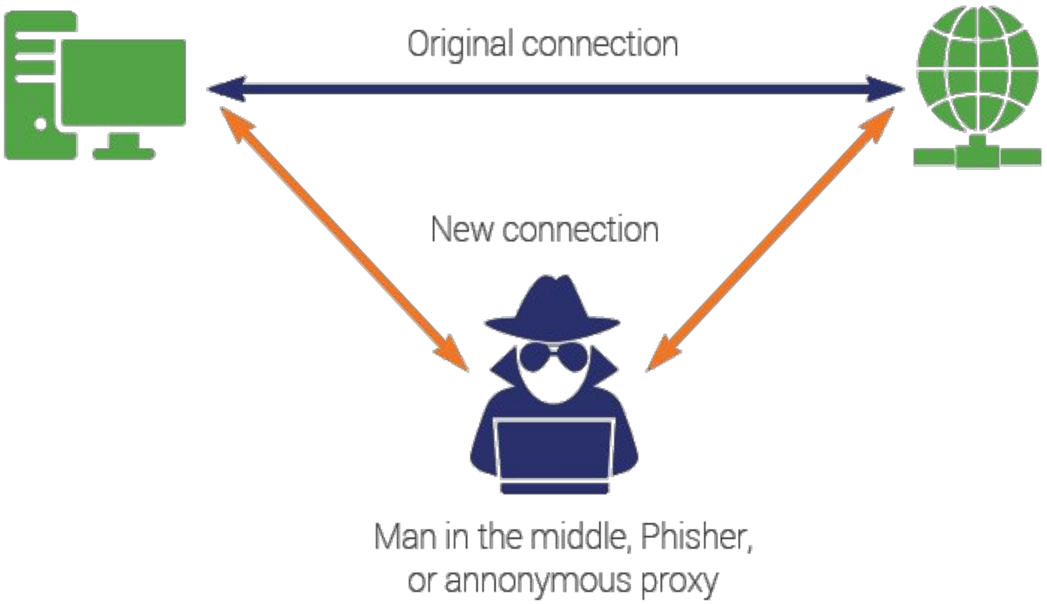


IS IT SAFE ???

Common Attacks

- HEARTBLEED BUG
- Heartbleed is a serious vulnerability in the SSL based encryption.
- Occasionally, one of the computers will send an encrypted piece of data, called a *heartbeat request,* to the other. The second computer will reply back with the exact same encrypted piece of data, proving that the connection is still in place. Crucially, the heartbeat request includes information about its own length.

Man
in
the
Middle
Attack



THANKYOU !!