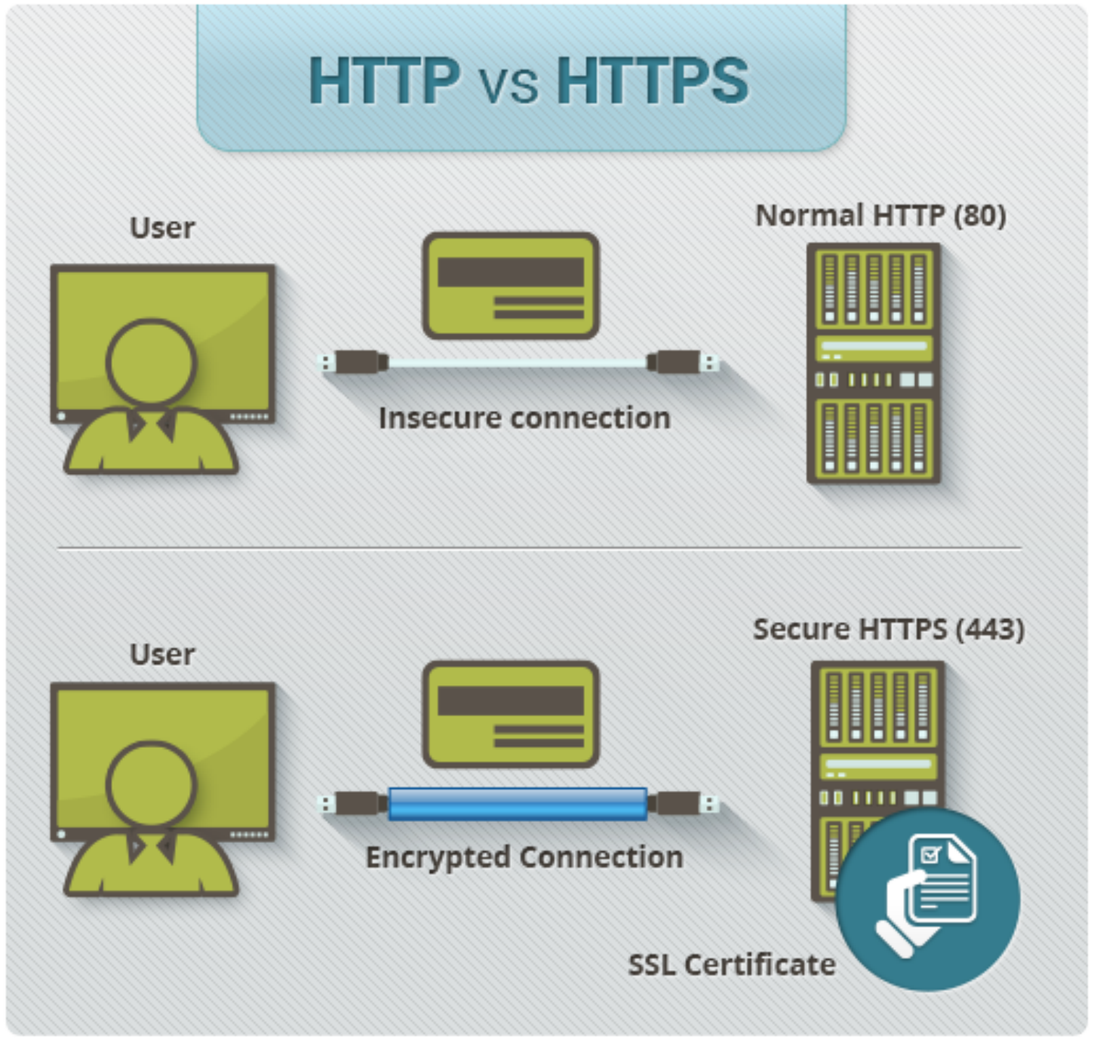
HTTPS

(the s stands for secure)



HTTPS is the secure version of http

Protocol

— SSL (Secure Socket Layer)
— TSL (Transport Security Layer)
— Public Key based system

How does it work?

Symmetric encryption and asymmetric encryption

— Symmetric Encryption: 1 key
— asymmetric Encryption: 2 keys, public and private

1. Browser sends a request to connect to secure site
2. Secure site sends response, including SSL certificate (this is called a handshake)
3. Browser does some checks to make sure the certificate is valid.
4. Some more complicated things go on, but basically the browser picks a random string to be used as an encryption key. It encrypts this with the public key on the certificate sent by the server.
5. The server gets the encrypted response and uses its

SSL is the equivalent of arranging an armored car to deliver credit card information from someone living in a cardboard box to someone living on a park bench

So why do we use it?

— any request I send bounces through hundreds of different places before it gets where it needs to go

— any person along the way can edit and change the contents of an unencrypted request

— using ssl, it is signed and secured

Man in the middle Attacks

— what if someone intercepts your key, switches it as theirs and passes it on?

— they can pretend to be you.

With HTTPS this is protected via certificates. There is a network of trust that you can verify a certificates accuracy against.

Other measures are
* DNSSEC Secure DNS extensions