HTTP and SSL

How SSL Works

Why SSL?

Encryption: Hiding what is sent from one computer to another.

Identification: Making sure the computer you are sending messages to is one you can trust.

Encryption

Without some form on encryption, sensitive data (passwords, credit cards, social security numbers) can be intercepted by any computer on any network that the request travels through on its way to the server.

SSL makes it to where those interception computers would just see nonsense data that it cannot unencrypt.

Encryption Handshake

1. Computer and server agree on how to encrypt.
2. Server sends certificate and encryption key to computer.
3. Computer says "start encrypting".
4. Server says "start encrypting".
5. Messages between computer and server are now encrypted.

How to Encrypt

Computer sends a hello message to the server containing the key exchange method, the cipher, the hash, the version of SSL the computer is using, and the random number that is used as the base of the encryption.

The server responds to the hello method validating the key exchange method, cipher and hash.

Server's Certificate

The certificate contains information about who the server belongs to, when the certificate expires and the server's public key.

Agree to Encrypt

Computer sends three messages: both computers calculate the master secret code agreed upon in the hello message, computer asks server to start encrypting, server validates the request to start encrypting.

Messages are Encrypted

The login password info or banking information sent by the computer to the server is now encrypted and looks like junk to anyone who doesn't have the decryption keys the computer and the server made together.

Identification

Just because a server has an SSL certificate doesn't necessarily mean that it's one you can trust, just that it will encrypt messages going back and forth with it to a computer.

How to Identify

1. Company asks a certificate authority for a certificate.
2. Certificate authority creates the certificate and signs it cryptographically.
3. Company installs the certificate on their server.
4. Browser issued with root certificates.
5. Browser trusts correctly signed certificates.

Company Asks for Certificate

The company has to provide information about themselves as a company, what they do, where they are located, and information about the web server.

The certificate authority validates the data and the authenticity of the company via public records and other sorts of checking up.

Creating the Certificate

The certificate contains, among other things, the version number of the certificate, its serial number, the algorithm used, the issuer of the certificate, the details of the company, the company's public key information, the signature algorithm, the signature itself.

The signature is created by condensing all of the details of the certificate into a number via a hash function, and then the number if encrypted via a private key.

Certificate on the Server

The company who requested the certificate then installs it on their server, which is configured to use the certificate in the handshake process.

Browser Issued Root Cert

Browsers come with root certificates of various certificate authorities in order to be able to check the authenticity of any certificate it examines.

These root certificates contain the certificate authorities' public keys.

Browsers Validate Certificates

When the browser received a certificate from a server, it is able to verify that the certificate is valid using the root certificates.

Self-Signed Certificates

Where the same party plays both the role of the company asking for a certificate and the certificate authority authenticating the certificate.

Useful in development environments test code against, but not trusted in production environments.

How to Use SSL

SSL and Information

- User Authentication (logins and passwords)
- Financial Information (credit cards, bank accounts, online orders)
- Sensitive Data (social security number, birth dates, license numbers)
- Medical Information
- Proprietary and Confidential Information (business contracts, client lists, legal documents)

When to Use SSL

An SSL certificate is required to use HTTP connections.

Encryption and decryption takes time and uses computer and network resources, making the connection slower and and put more burden on both the computer and the server, so you have to balance speed and security.