CS 105 TA Lecture Notes
December 1, 2014

SSL and TLS: a summary

SSL and TLS are terms for the technologies the secure Internet communications that allows you to send personal and private information without it being seen by anyone but who it's being sent to.

...websites that start with "https://" uses SSL/TLS.

TLS works with very, VERY large numbers (usually at least 2048 bits). Instead of working with numbers to understand how TLS works, we'll examine how it works using colors of paint.

Before we begin the algorithm, there are three numbers (colors of paint) that we'll define:

- The shared certificate, a number that is shared between everyone on the Internet. Everyone has this number, including you, your friend, and the more people who have it, the better!
- Your secret, a secret number that only you know. This should be kept secret.
- The server's secret, a secret number that only the server you're connecting to knows. This should be kept secret.

In lecture, we assigned a color of paint to each of those three numbers:

- The shared certificate is assigned the color yellow
- Your secret is assigned the color orange
- The server's secret is assigned the color blue

Suppose you now want to connect to Amazon. The algorithm is as follows:

STEP 1:

At the same time, on your own computers:

(a): You combine the yellow (certificate) and orange (your secret) to make a new color of paint.

...this creates a yellow-orange color.

(b): Amazon combines the yellow (certificate) and blue (their secret) to make a new color of paint.

...this creates a yellow-blue color.

This algorithm only works if paint cannot be subtracted. If you are able to reverse the mixing of the paint (e.g.: find out what the blue is from the yellow-blue), then this algorithm breaks and the Internet is not secure.

...luckily, lots of smart people have looked at this for a LONG time. So far, we are good!

STEP 2:

You and Amazon send your newly created color to each other.

...you get the yellow-blue from Amazon.

...Amazon gets the yellow-orange from you.

STEP 3:

Each party (you and Amazon) takes the color you received and adds your secret color to it.

...you take the yellow-blue and add your orange to get a yellow-blue-orange.

...Amazon takes the yellow-orange and adds its blue to get a yellow-orange-blue.

Since the order that the colors are added to the mix doesn't matter in generating new colors, both you and Amazon have the same color! This new colors is called a shared secret because the number is shared between both of you, but is secret to everyone else

STEP 4:

Now that you and Amazon both have the same color, this means you both have the same really, REALLY large number. Now you and Amazon can exchange information by encrypting that information before sending it.

One simple way to encrypt data is to use the **XOR** ("Exclusive OR") operation. This operation takes two binary numbers and returns a new binary number. Specifically:

- If the input numbers are the same, XOR returns 0. (0 XOR 0 == 0, 1 XOR 1 == 0)
- If the input numbers are different, XOR returns 1. (0 XOR 1 == 1, 1 XOR 0 == 1)

Ex: 111000 XOR 010101 == 101101

This algorithm described is called **Diffie–Hellman** key exchange. Diffie-Hellman is a real algorithm used as part of TLS; we made a few simplifications, but the basis of what is going on it exactly how your transactions on the Internet are secured!

SSL and TLS: in more detail (for those interested)

How do we securely transfer information on the web, and what does the "https://" thing actually mean?

What is SSL?

SSL (Secure Sockets Layer) is the standard security technology for establishing an encrypted link between a web server and a browser. This link ensures that all data passed between the web server and browsers remain private and integral. SSL is an industry standard and is used by millions of websites in the protection of their online transactions with their customers.

What is TLS?

Transport Layer Security (TLS) is a protocol that ensures privacy between communicating applications and their users on the Internet. When a server and client communicate, TLS ensures that no third party may eavesdrop or tamper with any message. TLS is the successor to the Secure Sockets Layer (SSL).

So what does it do?

TLS is composed of two layers: the TLS Record Protocol and the TLS Handshake Protocol. The TLS Record Protocol provides connection security with some encryption method (the TLS Record Protocol can also be used without encryption).

The TLS Handshake Protocol allows the server and client to authenticate each other and to negotiate an encryption algorithm and cryptographic keys before data is exchanged.

What is encryption?

Encryption is the conversion of electronic data into another form, called ciphertext, which cannot be easily understood by anyone except authorized parties, thus preventing any third party members from intercepting your secure data.

CS 105 TA Lecture Notes
December 1, 2014

What is a 'Hash Algorithm'?

A hash function is simply an algorithm that takes a string of any length and reduces it to a unique fixed length string.

What are hash algorithms used for?

Hashes are used to ensure data and message integrity, password validity as well as the basis of many other cryptographic systems. Important properties: Each hash is unique but always repeatable. That means that the word 'cat' will hash to something that no other word hashes too, but it will always hash to the same thing. The function is 'one way'. Meaning that if you are given the value of what 'cat' hashes too but you didn't know what made it, you would never be able to find out that 'cat' was the original word.

So hashing algorithms will yield a unique way to represent any block of information that is very specific to a key/secret chosen by a user.

Hashing algorithms prevent third party users from discovering the information being transmitted by uniquely encoding information based on a key that is constructed by the two users.