# UNDERSTANDING SSL

## SECURING YOUR WEBSITE TRAFFIC

**BONUS**
HOW TO SETUP A FREE SSL WITH LET'S ENCRYPT

NATHAN JAMES NEIL

# Understanding SSL

## *Securing Your Website Traffic With Bonus Steps to Setup An SSL Free With Let's Encrypt*

Nathan James Neil

**Copyright © 2016**

For more books by the author visit:

NeilPublishing.com

# Why I Wrote This Book

In 2014, I wrote one of number one bestselling business security books.  The objective of writing *Securing Business Data: Establishing a Core Value of Data Security* was to provide business owners an understanding of the questions that need asked and policies that need implemented to ensure the security of their business's information.

One of the topics that was mentioned in the first Chapter was implementing an SSL (Secure Socket Layer) into the business's web properties for an added layer of security. While, that book focused on the questions to ask and things to look for it did not go into detail on what an SSL is and how to implement one.

Following the popularity of that book, many people have approached me to develop a guide that focuses specifically on what an SSL is, where to get it, and how to implement it.

With that feedback, I decided to help business owners, bloggers, and others who wish to secure their site with an SSL by writing this book.

# Why You Should Read This Book

If you own or manage a website and do not have an understanding of what an SSL (Secure Socket Layer) is you NEED to read this book. With the strong threat of data breaches having an SSL is a must. There are additional benefits to having an SSL outside of just security. Google announced late last year that they were beginning to rank websites with SSL certificates higher than those who did not.

Every business wants to increase their search ranking and unfortunately, it may be a higher priority internally than security. By combining both the search ranking benefit and increased level of data security, my hope is a world that all websites are secured by this technology.

If you want to increase your search ranking you should read this book and along the way you will learn to secure your site as well.

Own an ecommerce site? Then you definitely need to read this book to ensure that you meet security requirements of payment processing companies.

This book will help you understand this technology and how to move forward with data integrity.

# Legal Disclaimer

The content of this book expresses the views and opinions of the author in understanding and establishing an additional security layer for your website.  It is designed to provide information and practices for understanding and implementing a Secure Socket Layer.

The author uses various service providers as examples in this book, but these mentions do not intend an endorsement or guarantee of services.

This book is not intended or should be taken as legal advice.  This book and its author only intend on providing self-help information understanding the usage, procedure, and implementation of a Secure Socket Layer.

This book is not a substitute from consulting with a security expert or a person who understands proper installation procedures when required.

This book does not come with any warranty or guarantee and the author cannot be held liable for any damages that may or may not result from negligence from any party.

# Table of Contents

# Part 1: Understanding SSL

## An Introduction

It does not matter if you are an individual, business, or organization, you have to approach online security in the same way that you would approach physical security. At your home you have locks, alarms, and other measures to prevent intruders from entering. At a business there are similar and likely stronger measures of physical security.

Understanding the need for physical security is easy. There is a threat that is visible. When it comes to online security and overall data security most people miss the target. There are many reasons for this. With a home intruder, you see the threat, but an online intruder can often go undetected. The treat of online theft is real, but rarely acknowledged. Technology also advances very quickly. Individuals and businesses who try to keep up with data and online security can easily be unaware of the latest security measures that are needed.

Most individuals and business owners think that it would never affect them. In February 2015, there was well over a billion stolen from a hundred different banks. The funds were stolen digitally and not by intruders taking hostages and demanding money. In my personal opinion the threat of online theft or intrusion is much more likely than the possible physical threat.

In this short book my objective is to explain one aspect of online security; the Secure Socket Layer. Technology can be confusing and almost magical in away. If this book helps just one detangle the confusion, then I am successful in my mission.

In this book we will use several terms, which should be outlined now. These will help you understand the context of my writing even if you are not familiar with technology or information systems. These terms can be defined further, but my goal is to explain them as non-technical as possible.

**Client:** An individual who is visiting a website

**Host:** The system or server that a website is housed on

**Encrypt:** To conceal and convert data into a cipher or code

**Decrypt:** Encrypted information being made readable

**Browser:** A program used to display websites

**SSL:** Secures data between a client and host

# What is a Secure Socket Layer

SSL, used frequently in this book, stands for Secure Socket Layer. An SSL provides an additional level of security to websites. Essentially what it does is creates a secure connection between the client and the host so that information sent between the two is encrypted and secured. The secure layer starts when a client enters a website into their browser and connects to the host.

For example, if I open up the website for M&T Bank, I can see that the traffic is secured. All information send from my computer (Client) to the M&T Bank site (Host) is encrypted as it moves through the web to each point. When the client or the host receives data it is then decrypted so it is readable.

While the information travels it is encrypted and if anyone would scrape the data, it would be in an unreadable format. This is because of the secure layer of communication, which is established by the SSL.

For there to be a secure connection established, the host must have a SSL Certificate installed. This certificate is a small piece of code that performs two functions.

The first function the certificate does is provides information about the identity of a business, website, or individual to verify the authenticity of the site. This information is displayed when you launch a website with a padlock symbol. If you click on that padlock it will provide you with details about the certificate issuer and holder. The highest trusted level of SSL authentication is the Extended Validation SSL. Those can be more costly and take more time to get established. For an organization or business like a bank or online store, it tells visitors that they when through an extended verification process.

The second function is processing data encryption. This function allows information and communication to be transferred over the internet between client and host, without being able to be intercepted by a malicious party. Only the intended recipient (client or host) of the information will be able to read it.

Think of this like going to the airport. If you are going to travel you need a passport, which is a metaphorical SSL Certificate. It is issued by a trusted authority, in this instance the government. There are strict rules on who can and cannot obtain one. When the traveler (host with a certificate) reaches security (client), the information is presented, verified, and passage permitted.

The encryption on the SSL works just like a physical lock. If you do not have the right key, the door will not open. An SSL uses two keys: public and private.

**Public Key:** encrypt information for transmission

**Private Key:** decrypt information and make it readable

Now that we have a grasp on some of the mechanical elements and terminology, we can go a little deeper into the process of how the SSL handshake between the client and host occurs.

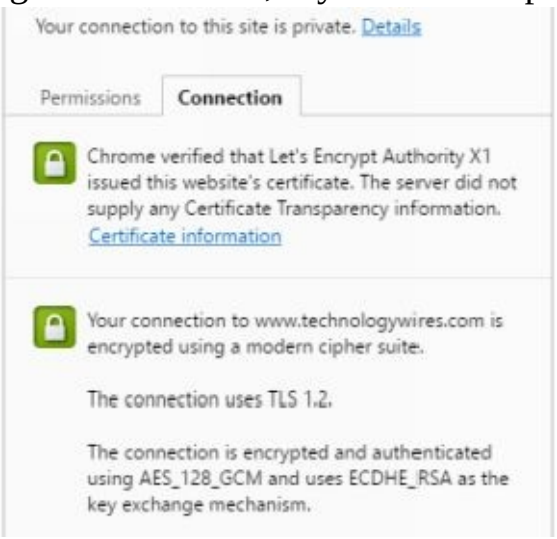
**SSL Handshake:** Greeting between the client's browser and the host.

Every SSL when it is issued, is for a specific website address. When the client enters the host's web address into their browser this handshake or greeting occurs. This handshake provides the following: information to create a secure link for the connection and a unique key for the session. After that process, secure communication begins.

# How Can I Tell if a Website Has an SSL

A normal website that is not secured with an SSL has *http://* before the web address, while sites secured with SSL use *http://*.

The second way that a client can tell that a website is secured with an SSL is a padlock symbol on the browser. Additionally, depending on the browser, if you click the padlock additional validation information is displayed.




Extended Validation SSL sites can be identified by turning the address bar in the browser green.  Again an Extended Validation SSL is the most trusted form of a certificate.

# Quick Recap

We went over a lot of information in a few short pages.  Let's recap what we have learned.

SSL Certificates provide a way for information to be sent securely from the client to the host and vice versa.  Websites that use an SSL are presented in the browser with *https://* before the domain name.  The SSL Certificate provides encryption so that the data cannot be intercepted and read.  Sending data without being connected to a host with an SSL is like mailing a postcard with all of your personal information.  As it travels everyone can see the information on the card.

SSLs can be used to secure website communications and other information that is sent and received by a host with a valid SSL.

# Search Engine Optimization Implications

Search Engine Optimization or SEO is the process of modifying your website to be more relevant in searches and in turn rank higher in popular search engines like Google. While I personally feel the security benefit is enough cause to get a SSL Certificate, some individuals and businesses might be given an extra incentive to purchase due to the SEO benefit it provides.

While it is still crucial to have high quality content on your site and optimized descriptions in your pages, Google announced in August of 2014 that websites with a SSL Certificate will be boosted in ranking. The ranking boost is logical. With all the spam sites out there a site that is verified by a third party to be trusted should be ranked higher. Google prefers these sites and ranks them higher because the user's information is encrypted with an extra layer of security.

Having an SSL adds security to your SEO goals in several ways. It prevents 3rd parties from tampering with the site, verifies the website is authentic, secures the traffic for clients who visit it, and encrypts all information.

According to Moz.com, only 1.9% of the top million sites use HTTPS with an SSL by default. Migrating to start using an SSL could give you that extra edge to rank higher than your competitors, but be aware that the number of sites using SSL is beginning to grow.

There are a few downsides as with everything that you should be aware of. First, mistakes can happen in moving the site to HTTPS if done improperly since it requires many moving parts. Consult with someone if you are unsure to make sure you implement it correctly.

Secured sites also have some potential to slow down your site if you do not have enough resources on your host (the server that houses the site) to process the handshakes we discussed.

The third factor is the added costs. On average webmasters spend between $100 to $200 on the average SSL certificate and the costs can go up significantly for even more detailed SSL certificates.

This third factor we will eliminate for many reading this. As we explore our various options, we will review some free solutions as well.

# Types of SSL Certificates

There are multiple validation types and packages for SSL Certificates. We will start by going over the different packages for SSL Certificates as offered by the top Certificate Authorities.

**Single Site SSL:** an SSL that Secures a Single Website

**Multiple Website SSL:** an SSL Certificate that can secure multiple different domains

**Wildcard SSL:** an SSL Certificate that secures a website and all of its subdomains

A single site SSL is a great option for a blogger or business that only uses one website. The multiple website SSL is great for businesses that own or manage multiple domains. It is a great value if you have a lot of domains that you need to secure. A wildcard SSL is best suited for domains that use multiple subdomains. Wildcard SSLs tend to be more expensive than the other two options.

There are also three main types of validation that are used for setting up an SSL.

**Domain Validation (DV):** Verifies that you are the owner of the domain

**Organization Validation (OV):** Verifies that you are the owner of the domain and that your organization is legitimate

**Extended Validation (EV):** A more expensive and lengthy issuance process, but an extended validation is the most secure as its holders have to go through a lengthy vetting process

The type of SSL you get depends on you or your organization’s needs and pricing varies. No matter which type of SSL you choose, you will get the latest encryption on the market, secure communications, and a boost in your site’s Google ranking.

# Part 2: Obtaining an SSL

## Where to Purchase an SSL

Below is a list of the top industry providers for paid SSL Certificates. If you already host your site with one of these providers, it may be a good option to select them as your source since most can automate installation or provide support.

**VeriSign:** Owned by Symantec, VeriSign is considered by many to be the most trusted and used by most of the big brands. It is reported that their Extended Validation certificate costs well over $1,000, but it does provide an outstanding $1.5 million dollar warranty.

**GeoTrust:** A good option for those who do not want to pay the VeriSign price. All of their options include a 256-bit encryption, warranty, and support. Many people do not know that this brand is now owned by Semantec as part of their acquisition of Verisign's security business in 2010.

**Comodo:** A solution with options for almost everyone with a great price on their Extended Validation package. ***It is important to note that a few years back there was an incident where fake Comodo certificates were used to spy on users in Iran.***

**DigiCert:** Trusted by large organizations such as AT&T, Microsoft, Yahoo, Facebook, NASA, and many others.

Thawte: A low cost SSL certificate provider with their cheapest single site plan selling for $149 a year.

**GoDaddy:** My personal favorite to use is GoDaddy. I have used them for multiple websites, single sites, and Extended Validation certificates. Easy to install with 24/7 support, and pricing starting as low as $69.99. The big edge here is that if you host your site with Godaddy most of the migration process can be automated. While I do not formally endorse a provider, in my experience, Godaddy has been a great to work with for multiple certificate purchases.

**Network Solutions:** Like GoDaddy many people host their site with Network Solutions as they have low priced products. They also have 24/7 support and is are a well-known and trusted brand.

## Free SSL From Let's Encrypt

One Certificate Authority that is new and not on this list is Let's Encrypt. Let's Encrypt is free, automated, and open source. There are many BIG players backing them including, but not limited to: Mozilla, Cisco, Facebook, Shopify, IdenTrust, Chrome, Sucuri, and many others.

Let's Encrypt was formed by the Internet Security Research Group, who is a tax-exempt organization with a mission to reduce financial, technological, and education barriers to secure communication over the Internet.

### *How it Works*

Let's Encrypt uses Domain Validation, which we discussed earlier. It identifies the server administrator and public key. When it is run for the first time it proves to the Let's Encrypt Certificate Authority that the server controls the domain.

Once the host has the authorized key pair it can then renew and revoke certificates easily, while also providing security and encryption to communication.

In the next section, we will walk through the steps of installing a free SSL using Let's Encrypt on an Ubuntu hosting environment. There are similar guides for other operating systems, but Ubuntu is among the most popular Linux distributions for hosting websites.

# Bonus Section

## Installing a Free SSL with Let's Encrypt

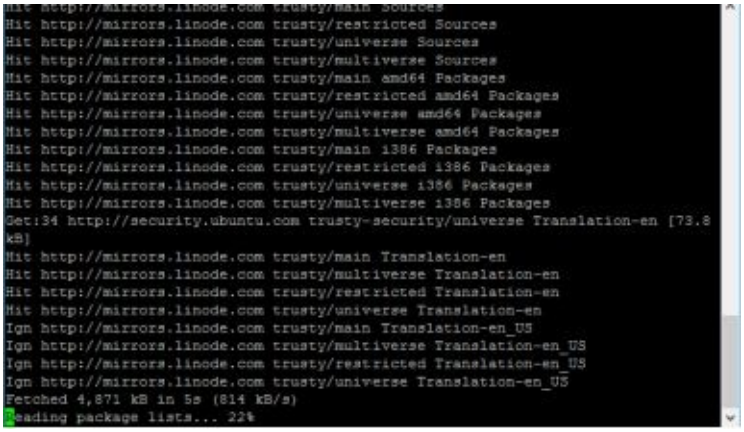
This bonus guide on installing a free SSL with using Let's Encrypt as the Certificate Authority walks you through the steps of installing and configuring an SSL on an Ubuntu 14.04 LTS server. Ubuntu is among the most popular solutions for a hosting solution. In this tutorial we will be using SSH and puTTY to install the certificate onto the system.

If you are unfamiliar with these technologies or unsure if you are using Ubuntu as a hosting environment, seek out the advice of your technology professional. In this tutorial, I will be installing an SSL onto my testing site technologywires.com.

To being we must launch puTTY and enter in the ip address of our host system. Once the terminal opens, enter your servers username and password. Please note that the user must have sudo privileges. For more information on what sudo is and how to understand the basics of Linux, please take a look at my book *Learning Ubuntu: A Beginners Guide to Using Linux.*

Once you are logged in, we must first update the package manager. We can do this by running: *sudo apt-get update*

This process may take a few moments and your screen may look like the example below.




Once that is completed we will need to install the git package to be able to download the Let's Encrypt client.

**Git** is a widely used source code management system for content development, which will allow us to pull the source code for Let's Encrypt.

To install git we must use the following command:

*sudo apt-get install git*

The system will ask you if you want to continue.  Press y and then the enter key to continue the install.

Now that git is loaded, we need to get the Let's Encrypt client.

We can do that by using the command below:

*sudo git clone https://github.com/letsencrypt/letsencrypt /opt/letsencrypt*

What that command does is creates a local copy of the Let's Encrypt repository under the /opt/letsencrypt directory.

To navigate to the directory where the repository is stored, we must navigate to the directory using the command below:

*cd /opt/letsencrypt*

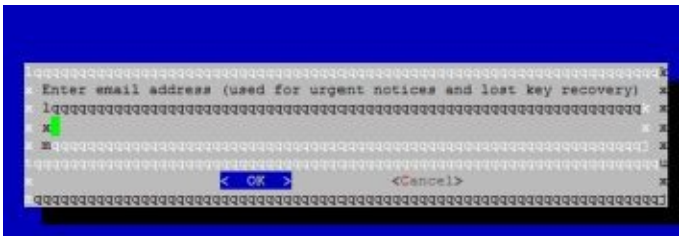
Now we can begin the process of running Let's Encrypt. In this instance, I want to establish an SSL for my site www.technologywires.com.  You would replace that with your domain name.

To create the certificate, I need to run the command below

*./letsencrypt-auto —apache -d www.technologywires.com*

Once that is entered, the system will begin to take the needed steps to take us into the next phase.

In the next phase, you will be prompted for an email address for notices and lost key recovery.




Upon completion of that field you will be asked to read the most recent terms of service and agree to them.


Then in the following prompt you will be asked if you want to use the easy method, which allows both HTTP and HTTPS or the secure method, which makes all requests redirect to secure HTTPS access.  I prefer the secure method.

Once you select your method, you will see a screen congratulating you. We have now installed an SSL Certificate for free!


Now if I load [www.technologywires.com](http://www.technologywires.com) in the browser, I will see the green padlock symbol in addition to HTTPS.


Please note that the one downside to using Let's Encrypt is that you must renew it every 90 days.

To renew your certificate you must navigate to the Let's Encrypt directory:

*cd /opt/letsencrypt*

Once you are in the directory, you can run the following command to renew:

*./letsencrypt-auto renew*

# Final Remarks

First, thank you for reading this book and for considering the use of an SSL on your website. If more people would implement this layer of security, our overall internet interactions would be much more secure.

For additional information on securing the data for your business, please read *Securing Business Data: Establishing a Core Value of Data Security*.

For more details on learning how to use Ubuntu 14.04 LTS and using it for a web server, read Learning Ubuntu: A Beginners Guide to Using Linux.

Thank you again for purchasing this book and feel free to share it with a friend. My main objective in writing these books is to increase awareness, while also providing solutions to common data security problems.