

Differences Between SSL and TLS

Reading

40m

✓ Status

Incomplete

Introduction

Earlier, you were introduced to SSL and TLS. As a reminder, both cryptographic protocols provide security between the application and server information exchange. The difference is that TLS 1.0 was created as a successor to SSL 3.0 and is often used as a configuration for email programs.

Evolution of SSL and TLS:

- SSL V1 – 1994
- SSL V2 – 1995
- SSL V3 – 1996
- TLS 1.0 – 1999
- TLS 1.1 – 2006
- TLS 1.2 – 2008
- TLS 1.3 – 2015

TLS can work on different ports and uses more robust encryption algorithms like keyed-HMAC, while SSL-only uses MAC. TLS can also be used by an intermediate authority, not necessarily a Certificate Authority.

This reading will focus on the differences between SSL and TLS.

Which is More Secure?

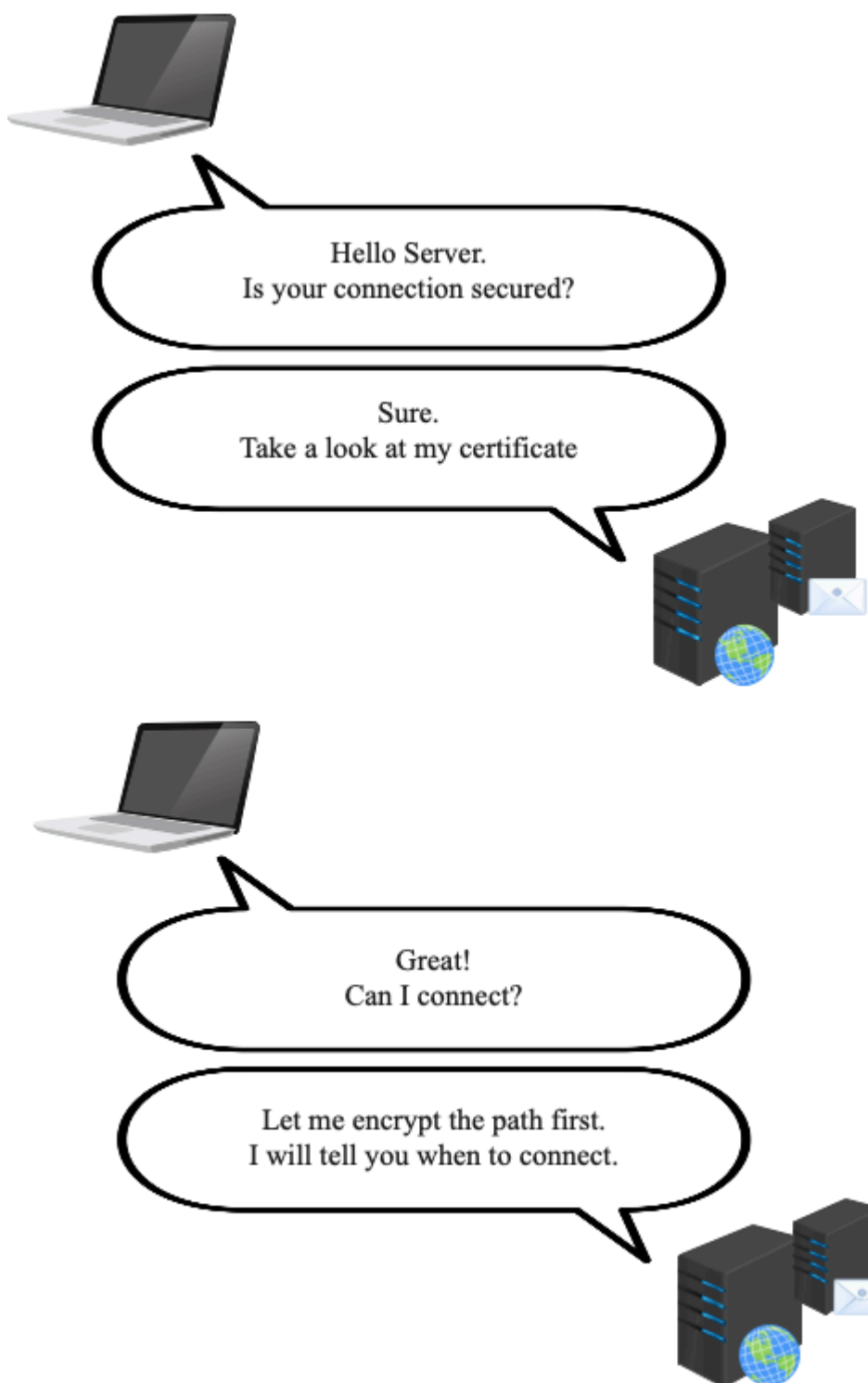
At first, the first version of the TLS protocol was slightly more secure than SSL, but in mid-2014, it was proven that the past generation of SSLs was wholly insecure and that it was possible to break their encryption.

This vulnerability became known as POODLE, and with it, other people could capture data transported by SSL, such as cookies and passwords. So any site that still uses SSL encryption is still at risk.

Long before these vulnerabilities were discovered, there were rumours of SSL falling into disuse. Since the POODLE vulnerability was disclosed, TLS has undergone updates and is currently at version 1.3. Several security flaws were fixed, and when compared to SSL, TLS became more secure.

How do SSL/TLS Certificates Work?

SSL/TLS certificates digitally attach a cryptographic key to a company's identifying information. This allows data to be transferred in a way that third parties cannot discover.



SSL/TLS works through each secure connection's public and private keys and session keys. The browser and server connect when the visitor puts an SSL-enabled URL in the browser and browses the secure page. During the initial connection, the public and private keys are used to create a session key, which is then used to encrypt and decrypt the transferred data. This session key will remain valid for a limited time and will only be used for that specific session.

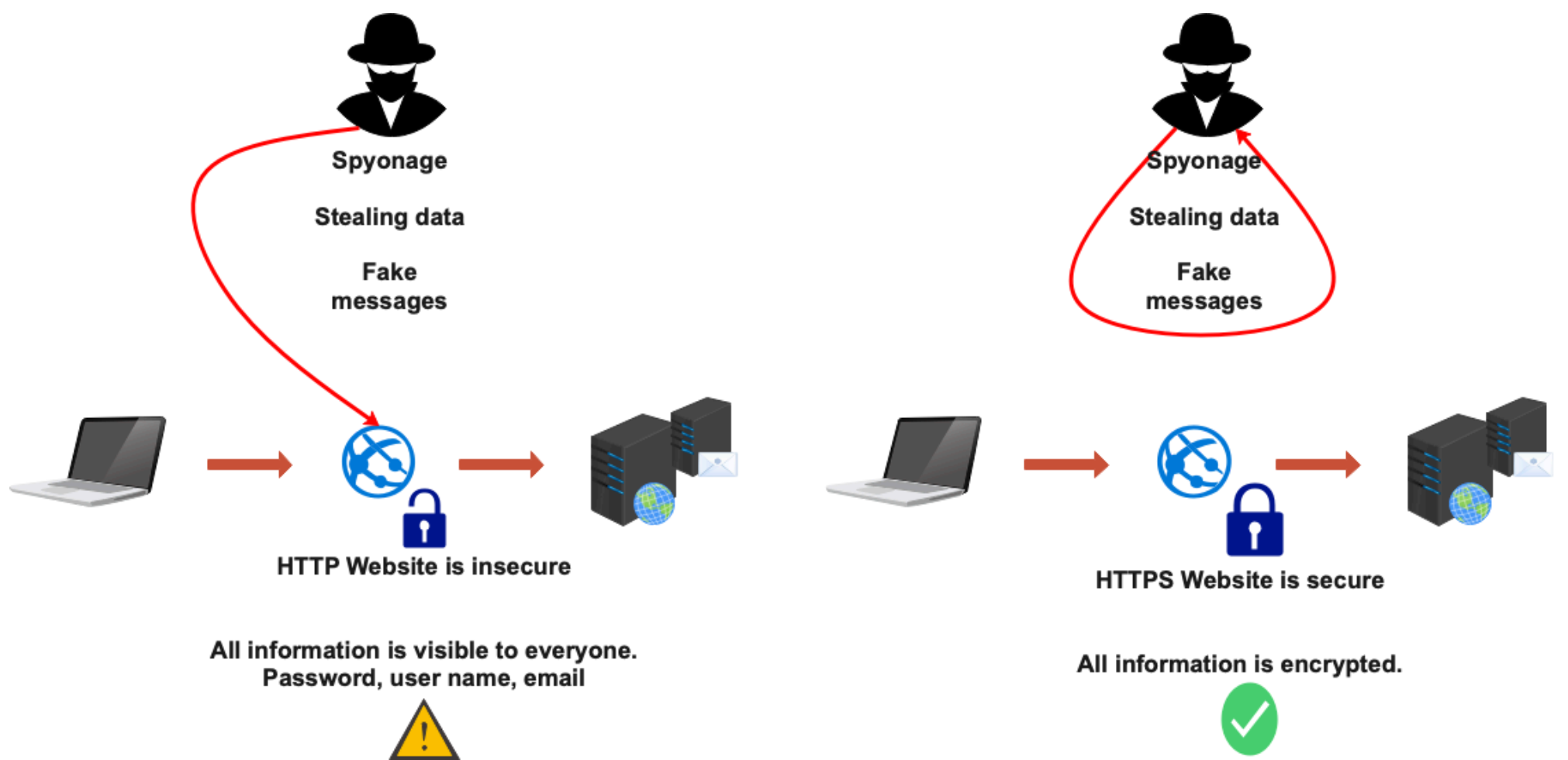
To find out if a website uses an SSL connection, just look for a padlock icon next to the URL in your browser. You should find information about the certificate and perform configurations by clicking on the padlock.

The purpose of SSL/TLS is to ensure that only one person (the person or organization to whom the data is being transmitted) can gain access to the information. This is particularly important when considering the number of devices and servers that information passes through before reaching its destination.

There are three cases where having an SSL/TLS is essential:

1. When authentication is needed: any server can impersonate your server by intercepting information transmitted along the way. SSL/TLS allows you to prove your server's identity, so visitors know it's authentic.
2. To ensure reliability: when owning a virtual store or any website that requests the use of personal information, it is essential to create a sense of security so that people feel comfortable in providing their data. An SSL/TLS certificate is a visible way to tell visitors that their data will be safe.
3. When you need to meet industry standards: in some industries, like finance, you must maintain a basic safety standard. There are also some Payment Card Industry (PCI) requirements for those who want to accept credit card payments on their website, and one of them is using an SSL/TLS certificate.

It is important to remember that the SSL/TLS certificate is valid for many devices, which makes it an even more versatile security option in the age of mobile devices.



What is the Relationship Between SSL/TLS and HTTPS?

When you install an SSL certificate, data transmission is configured to be done via HTTPS. Both technologies go hand in hand and only work with each other.

URLs are preceded by HTTP or HTTPS. This is what determines how any incoming or outgoing data is transmitted.

Why Has TLS Replaced SSL?

To protect online applications or data in transit from eavesdropping and alteration, TLS encryption is now routine. TLS has been vulnerable to breaches such as Crime and Heartbleed in 2012 and 2014. While it has demonstrated significant advances in efficiency and security, it is unrealistic to believe it is the most secure protocol.

Christopher Allen and Tim Dierks of Consensus Development created the TLS 1.0 protocol, an improvement over SSL 3.0. While the name change implies a substantial difference between the two, there were few. According to Dierks, Microsoft changed its name to avoid the impression that the Internet Engineering Task Force (IETF), which leads Internet standards, was endorsing Netscape's protocol and had to rebrand SSL 3.0 as part of the horse trade (for the same reason). And so, TLS 1.0 (which was SSL 3.1) was created. Following this way, TLS is replacing SSL, and virtually all SSL versions have been deprecated due to documented security flaws. An example is Google Chrome, which stopped using SSL 3.0 in 2014. Most contemporary online browsers do not support SSL at all.

Why Replace SSL Certificates with TLS Certificates?

The main reason to replace SSL certificates with new TLS certificates is that they are incompatible with each other; they use different protocols and algorithms. Any browser or client application using one protocol will be unable to securely connect to a server using the other protocol without making explicit configuration changes on both sides of the connection.

What's Next?

In addition to HTTPS, the HTTP protocol has also evolved into what is defined as HTTP/2. This is what experts consider an evolution in technology regarding security benefits. HTTP/2 arrived in 2015, about 15 years after HTTP/1 as an upgrade to reduce some of the problems of the first version of the protocol.

Thus, the new version allows for more simplicity and, therefore, faster data transfer, strengthening the security of web applications. In this way, it contributes to improving the user experience. This transition in the protocol is also a reflection of technological developments. But it also meets user expectations, improving web communications, etc.

Main Advantages of HTTP/2

This evolution in the HTTP was decisive in keeping up with the new times of the Internet, where more speed is expected, but mobile access also benefits more. The advantages of HTTP/2 are also broader.

Therefore, here are the most significant ones:

- Improvements in web performance.
- Optimizes the web experience for mobile users.
- Reduces operating expenses for telecom providers.
- Resource-saving reduces worldwide bandwidth congestion.
- Facilitates multimedia communication with images and videos.
- Better use of technology.
- Strengthens data protection.

What is HTTP/3

The next generation of this technology is already here. This means HTTP3, developed by three technological giants: Cloudflare, Google, and Mozilla.

This is a significant new change from HTTP and builds on the QUIC (pronounced "quick"). However, its name was initially proposed as the acronym for "Quick UDP Internet Connections" that Google created. Thus, until recently, the latest version of the protocol was known as HTTP-over-QUIC. The old HTTP used the TCP as one of the layers for transporting data from the original HTTP. In the case of HTTP/3, TCP is replaced by QUIC, which, in turn, is based on UDP.

The change allows HTTP/3 to improve the loading speed of websites, as well as the security of connections. However, HTTP/3 still needs to be applied on a large scale, at least for now. Only about 10% of sites will support it already. But Chrome and Firefox browsers already support it in stable versions.

Main Advantages of HTTP/3

HTTP/3 has several benefits over HTTP/2, as you would expect. But, in summary, it can improve the Internet for everyone, improving the performance of websites and the user experience.

The main advantages of HTTP/3 are below:


- Faster website loading speed.
- Better website performance.
- Reduction of poor or leaky Internet connections.
- Strengthens protection against various types of computer attacks.

However, it is essential to underline that this HTTP protocol is still being improved, as several aspects need to be improved and considered.

At this stage, there may be some compatibility issues. Especially because HTTP/1 can be upgraded to HTTP/2, but the same cannot happen with HTTP/3, as it uses the UDP protocol instead of TCP. Therefore, some experts predict that most sites will not even implement the new version of the protocol. This way, it would only be used in content distribution networks or service providers to access other websites.

NIST Recommendations

NIST lists and identifies its recommendations for TLS server configurations in [section 3: NIST SP 800-52 TLS Server Recommendations](#).



Review Section 3 of the document above in detail. * Optional: you may visit [NIST SP 800-52 TLS Server Recommendations](#) to explore further.

✓ Mark Completed

←

Previous

Common Encryption Methods Quiz

Next

Unpacking Linux Commands Using AI Tools

→

How well did this activity help you to understand the content?

Let us know how we're doing



W07D2

Tue Aug 6

> Outline & Notes (1)

> Lectures (1)

✓ Work (6)

5 hrs

 [Case Studies: Encyption & Data Breach](#)

 [Cryptography Recap](#)

 [Cryptographics Algorithms](#)

? [Common Encryption Methods Quiz](#)

 [Differences Between SSL and TLS](#)

</> [Unpacking Linux Commands Using AI Tools](#)

W07D2 Schedule »