Using TLS and SSL

Reading

10m - 25m

✓ Status Incomplete

Introduction

This reading introduces you to Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL). TLS and SSL are protocols designed to provide secure communications over the internet, ensuring that data transmitted between parties remains confidential and cannot be modified by attackers.

As a new cyber security professional, it is essential to understand how these protocols work, their strengths and limitations, and their applications in modern network security. With the automation of numerous operations, the flow of data in the digital environment has increased, and, as a result, system vulnerabilities are quickly discovered by people. Hence the importance of TLS or SSL protocols.

TLS and SSL

TLS and SSL were created to ensure that information can be transmitted, received, or stored between server and clients. Both cryptographic protocols protect the flow of data that travels between computer networks because it is common to cause confusion between them.

TLS and SSL are encrypted protocols that guarantee communication security to the user as soon as they access the virtual environment, such as browsing pages (HTTP), e-mail (SMTP), and other means for transferring data. TLS certificates are a more up-to-date and secure version of SSL, typically used as a setting in e-mail programs. However, no less important than the SSL certificate, it has its role in any transaction between server and client. The terms SSL and TLS are commonly used together and are referred to as one another.

As for SSL certificates, they guarantee security to the user as soon as they access a website. This means the data sent is encrypted to prevent others from misusing the information.

Generally speaking, there are no significant technical differences between the TLS and SSL protocols, but the two have specific rules.

SSL uses only the MAC algorithm. At the same time, TLS can operate on different ports and uses more robust encryption algorithms, such as Hashing for Message Authentication Code (HMAC).

Benefits of SSL and TLS

To ensure the security of Internet communication protocols (TCP/IP), the endings "HTTPS" and "HTTP" are commonly found in the navigation bars. In HTTP, data travels freely, while HTTPS is encrypted with SSL/TLS.

Certificates for SSL/TLS are the digital ones that end up offering users the guarantee of privacy, authenticity, and integrity of the information of a portal on the network, which assures the visitor that they are accessing a safe and original website and not a copy made by attackers or malicious people.

When a developer configures a server safely and correctly, they guarantee their clients that they can verify through the certificate that the website is working with safe protocols.

Benefits of Using SSL/TLS Digital Certificates

One of the benefits of having digital certificates brings reliability and credibility to the site because when issuing the certificate, the certifying authority will verify and attest that the person who wants to acquire a certificate is the site's owner. In addition, it analyzes whether the domain owner is legally constituted and has an address and telephone number. Using the SSL/TLS protocol, all data is encrypted, preventing information falsification and improper access.

> ℹ **TIP:** it is good to remember that for a virtual store or e-commerce, it is essential to use a digital certificate.

The following are highlights of some models of SSL certificates that are on the market:

- Domain validated: validation, in this case, is done automatically by the Certification Authority, which will confirm the existence of the domain. For verification, the data registered with the organization responsible for registering the domain are taken into account.
- Self-signed: the organization will generate its certificate. Generally, they are for internal use, not having interoperability with Internet browsers.
- Fully authenticated (organization validation): the Certification Authority, in this case, will validate whether the person who requested the SSL certificate owns the website, whether it is legally constituted, and whether it is in a position to request the certificate.
- Fully authenticated certificates for those who operate in e-commerce are the most recommended, as they provide greater security for users, companies, and customers.

Conclusion

With so many certificate options on the market, the Cyber Security analyst must know which types to choose and check. Regarding protection for a virtual store, the most used today are SSL EV and standard SSL. You can find MDC SSL (capable of validating numerous domains), WildCard SSL (which can validate all website subdomains), and others.

✓ Mark Completed

← Previous
Symmetric, Asymmetric Key and Hash Quiz

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

Let us know how we're doing

☆ ☆ ☆ ☆ ☆

W07D1

Mon Aug 5

› Lectures (1)

⌄ Work (4)

3 hrs

- The Minimum Security Strength of Cryptography
- </> Decrypting and Sending a File
- ? Symmetric, Asymmetric Key and Hash Quiz
- Using TLS and SSL

W07D1 Schedule »

Powered by Lighthouse Labs.