Marco CAVANI ID: 10570027

TLS 1.3 Overview

20/05/2022

Contents

[Introduction 2](#_Toc104526561)

[HTTP & HTTPS 2](#_Toc104526562)

[Symmetric and Asymmetric encryption 2](#_Toc104526563)

[TLS v1.3 3](#_Toc104526564)

[TLS v1.3 Components 3](#_Toc104526565)

[Handshake 3](#_Toc104526566)

[Record Protocol 5](#_Toc104526567)

[Security Overview 5](#_Toc104526568)

[TLS v1.3 Security 5](#_Toc104526569)

[Main Differences from TLS 1.2 6](#_Toc104526570)

[Summary 6](#_Toc104526571)

[References 7](#_Toc104526572)

# Introduction

TLS stand for Transport Layer Security, and it is the upgrade of the deprecated Secure Sacket Layer or SSL (Wikipedia Contributors, 2019). It has been designed for network security and is taking advantage of symmetric and asymmetric cryptography to encrypt the communications (J. Lake, 2019). In fact, it can be used for email messaging and voice encryption or more generically, for securing the connections between the user and the server by providing confidentiality, integrity, and authentication.(Wikipedia Contributors, 2019). For instance, TLS is now day extensively used as layer on top of the network communication and is responsible for preventing information corruption and promoting non-repudiation and confidentiality between two or more entities(E. Rescorla, 2018). Furthermore, TLS provide Authentication of both the server and the client via digital signature, along with Confidentiality as it makes the information visible to the endpoint only, and message integrity by preventing the disclosure of information against threats such as men in the middle attack(E. Rescorla, 2018). Even though other previous versions are still used, this report will focus on TLS latest version 1.3.

# HTTP & HTTPS

The Hypertext Transfer Protocol (HTTP) is used on top of Transmission Control Protocol(TCP) to establish a connection between the client and the server(E. Rescorla, 2018). However, the connection does not provide security such as encryption is not provided. different from HTTPS which provides symmetric and asymmetric encryption through TLS certificate(J. Lake, 2019).HTTPS stand for Hypertext Transfer Protocol Secure, and it comes with security futures that allows the user to exchange information in a safe way(J. Lake, 2019).

# Symmetric and Asymmetric encryption

There are two types of encryptions Symmetric and asymmetric. The symmetric encryption is made by one share key which is used for both encryption and decryption, reason way the key exchange is often a problem in symmetric cryptography as a third figure could intercept the key on the fly and decrypt the communication. In saying that, symmetric encryption is fast and computably easy. On the other hand, the asymmetric encryption is made by using a private and a public key, where the public key is accessible and the private key stays private. This method takes advantage of large primes and their exponentiation to keep information secure through an algorithm which hides the plaintext making difficult for a hacker to break the cipher even if the public key and the cipher text are available. Least but not last, Asymmetric cryptography can provide authentication (e.g., digital signature).

# TLS v1.3

TLS 1.3 provides authentication, confidentiality, and integrity over internet communication combining symmetric and asymmetric crypto systems(Rescorla, 2018).

Diagram

Description automatically generated

Figure 1

As it can be seen in figure 1, in the initial phase of the communication, the client requests a connection to the server followed by TLS version and a list of cipher suit supported. The Server responds with the chosen cipher suit along with the server certificate and the request for client certificate which is optional. After that, the client sends the secret key information encrypted with the server public key using asymmetric method, along with the client certificate(if required).once the connection is established the two parties can exchange information using the shared key using a symmetric method (IBM, 2022).

## TLS v1.3 Components

TLS consist in two main components : the handshake and the record protocols(R. Heaton, 2014).

### Handshake

The handshake can be divided in three sub-protocol(R. Heaton, 2014):

1. The “Hello” message, where the client sends information about TLS version and a list of cipher suit supported followed by the server responds in the “ServerHello” message that contains the appropriated cipher suit and TLS version which can be supported by the client(R. Heaton, 2014)
2. The certificate exchange phase is where the server identify itself to the client through the SSL certificate. The SSL certificate contains information such the name of company who owns the certification, the public key, the digital signature, and the expiring date of the certificate. The client is also demanded to send its certificated in some instances especially in application that requires a certain degree of protections.
3. The key exchange step defines the key in which the plaintext is encrypted and decrypted. In this stage the share secret key previously generated is defined to be used in the symmetric encryption.

More precisely, the client creates a random key to be used in the symmetric algorithm which is then encrypted using the predefined algorithm selected in the “Hello” message and the server’s public key combined. After that, the encrypted key is sent to the server which decrypt it using its private key(R. Heaton, 2014). TLS v1.3 supports 5 cipher suites:

In the handshake the following security criteria are defined

* Authentication which is provided through asymmetric cryptography:

|  |  |  |
| --- | --- | --- |
| RSA (PKCS#1 variants) | Elliptic Curve Digital Signature Algorithm (ECDSA) | Edwards-Curve Digital Signature Algorithm (EdDSA) |
| PKCS stand for Public-key Cryptographic Standards, it provides mathematical standards for encryption and digital signature (*PKCS 1*, 2021). | It offers an alternative method to Digital Signature Algorithm (DSA) using elliptic curve cryptography (*Elliptic Curve Digital Signature Algorithm*, 2022). | It’s a digital signature scheme based on twisted Edwards curves (*EdDSA*, 2022). |

And symmetric cryptography:

|  |
| --- |
| pre-shared key (PSK) |
| PSK is a symmetric key sharing method that can be used to establish a secure TLS connection between two parties based on pre-shared key (*PKCS 1*, 2021). |

* Confidentiality can be ensured by asymmetric key exchange (e.g., DHE & ECDHE) and symmetric encryption data exchange method based on the share secret, as the data can be visible to the endpoint only.

|  |  |
| --- | --- |
| DHE | ECDHE |
| DHE stand for Diffie-Hellman key exchange, and in a protocol that can be used to generate public and private key, public key distribution and create a share secret. The share secret is often used as the key for symmetric encryption(Wikipedia Contributors, 2019c). | ECDHE is similar to DHE, but it uses elliptic curve to generate public and private keys(Wikipedia Contributors, 2019b). |

* Integrity is guaranteed as the transmitted data cannot be modified without been detected.

|  |  |
| --- | --- |
| Authenticated encryption with associated data (AEAD) | Hashed-Key Derivation Function (HKDF) |
| AEAD is often used to tie associated data in a way that user can be linked to some data related to an ID(GOOGLE, 2021). | It can use both block cipher and hash function to digest the plaintext(Wikipedia Contributors, 2019**c**)**.** |

### Record Protocol

The second component is called record protocol and uses the parameters defined in the handshake to protect the traffic. Moreover, it divides the traffic in an array of records where each record is protected independently(E. Rescorla, 2018).

## Security Overview

The security provided from TLC is considerably dependant on Diffie-Hellman key exchange and the bilateral authentication method where both parties can be identified using the SSL certificate(E. Rescorla, 2018).

In the handshake the following parameters are defined:

In the record protocol:

Traffic is divided and encrypted separately to prevent traffic analysis attacks. (E. Rescorla, 2018)

# TLS v1.3 Security

The TLS protocol provides Confidentiality, Data Integrity, Peer Entity authentication, non-Repudiation(E. Rescorla, 2018). TLS 1.3 version has come with security futures that are aimed to prevent eavesdropping tempering, and message forgery(E. Rescorla, 2018). However, eavesdropping attacks are divided in two type active and passive. In the eavesdropping attack a third figure intercept the connection between the parties. A classic example of active type is Men-in-the-middle attack which can altered the data causing the disruption of the communication. Unlike the passive attacks where the hackers are inclined to listen without interfering directly to the information flow. In saying that, TLS 1.3 has been designed to mitigate the consequences of active and active and passive network attack. In fact, it is possible to mitigate eavesdropping attacks like man-in-the-middle as only one side authentication is sufficient to mitigate the attack(E. Rescorla, 2018). Additionally, the handshake prevents data tempering by using AEAD Cipher suite and Message forgery providing non-repudiation system such as digital signature algorithms (PKCS, ECDSA and EdDSA). This new version of TLS has removed some unsafe futures which were linked to vulnerability exploited in the past. The following methods are no longer used in version 1.3 (E. Rescorla, 2018):

* the RSA for the key exchange
* RC4, 3DES and camelia for the encryption
* MD5, SHA-1 for the hash system
* Cipher Modes AES-CBC
* DSA Signatures (ECDSA ≥ 224 bit) for the session renegotiation

The following table outlines the common attacks related to the algorithms on the left column

|  |  |
| --- | --- |
| method | Common attack |
| RSA-PKCS#1 v1.5 Encryption | * Bleichenbacher 1998 * Jager 2015 * DROWN 2016 |
| RC4 | * Roos’s Bias 1995 * Fluhrer, Martin & Shamir 2001 * Klein 2005 * Combinatorial Problem 2001 * Royal Holloway 2013 * Bar-mitzvah 2015 * NOMORE 2015 |
| MD5, SHA-1 | * SLOTH 2016 * SHAttered 2017 |
| Cipher Modes AES-CBC | * Vaudenay 2002 * Boneh/Brumley 2003 * BEAST 2011 * Lucky13 2013 * POODLE 2014 * Lucky Microseconds 2015 |

# Main Differences from TLS 1.2

The number of Symmetric algorithms has dropped from twenty-seven to five, and they all are Authenticated Encryption with Associated data(AEAD) algorithms. The cipher suite model has been changed to split the authentication and key exchange processes from the record protection algorithm and a hash Hashed-Key Derivation Function (HKDF) that can be utilized with both the Message Authentication(MAC) and the key derivation function. Additionally, the cipher suit now provides secrecy through the shared secret. Moreover, a shorten application data exchange was added to decrees the connection in the and handshake which resulted in faster communications and less points of attack. In my opinion, the cryptosystem is surprisingly a simplified version but, at the same time it offers more advanced futures(E. Rescorla, 2018).

# Summary

During my research I was curious about the criteria in which the latest version has been made at the same time surprised to see how many attacks can be dropped by catting down the vulnerable algorithms seen in version 1.2. I was also able to learn about attacks related to the web and the risks that can occur while using internet, I was also surprised to see how easily can be for a target to be a victim of cybercrime without even realizing it. My recommendation for the readers is to visit secure websites only to maximize the security over the navigation and stay updated about possible threats and countermeasures.

# References

1. *An overview of the SSL or TLS handshake*. (2022, April 28). Www.ibm.com. <https://www.ibm.com/docs/en/ibm-mq/7.5?topic=ssl-overview-tls-handshake>
2. Brodie, A. (n.d.). Overview of TLS v1.3 What’s new, what’s removed and what’s changed? https://owasp.org/www-chapter-[london/assets/slides/OWASPLondon20180125\_TLSv1.3\_Andy\_Brodie.pdf](https://edithcowanuni-my.sharepoint.com/personal/mcavani_our_ecu_edu_au/Documents/Brodie,%20A.%20(n.d.).%20Overview%20of%20TLS%20v1.3%20What’s%20new,%20what’s%20removed%20and%20what’s%20changed?%20https://owasp.org/www-chapter-london/assets/slides/OWASPLondon20180125_TLSv1.3_Andy_Brodie.pdf)
3. EdDSA. (2022, March 6). Wikipedia. [https://en.wikipedia.org/wiki/EdDSA#:~:text=In%20public%2Dkey%20cryptography%2C%20Edwards](https://en.wikipedia.org/wiki/EdDSA%23:~:text=In%20public%2Dkey%20cryptography%2C%20Edwards)
4. Elliptic Curve Digital Signature Algorithm. (2022, February 13). Wikipedia. <https://en.wikipedia.org/wiki/Elliptic_Curve_Digital_Signature_Algorithm>
5. GOOGLE. (2021). Authenticated Encryption with Associated Data (AEAD)  |  Tink  |  Google Developers. Google Developers. <https://developers.google.com/tink/aead>
6. Heaton, R. (2014, March 27). How does HTTPS actually work? | Robert Heaton. Robert Heaton. <https://robertheaton.com/2014/03/27/how-does-https-actually-work/>
7. *HTTP vs HTTPS - javatpoint*. (n.d.). [Www.javatpoint.com. https://www.javatpoint.com/http-vs-https](https://edithcowanuni-my.sharepoint.com/personal/mcavani_our_ecu_edu_au/Documents/Www.javatpoint.com.%20https:/www.javatpoint.com/http-vs-https)
8. IBM. (2022, April 28). An overview of the SSL or TLS handshake. Www.ibm.com. <https://www.ibm.com/docs/en/ibm-mq/7.5?topic=ssl-overview-tls-handshake>
9. Lake, J. (2019, February 25). What is TLS encryption and how does it work? Comparitech. <https://www.comparitech.com/blog/information-security/tls-encryption/>
10. PKCS 1. (2021, November 20). Wikipedia. <https://en.wikipedia.org/wiki/PKCS_1>
11. Rescorla, E. (2018, August 22). *The Transport Layer Security (TLS) Protocol Version 1.3*. Datatracker.ietf.org. <https://datatracker.ietf.org/doc/html/rfc8446>
12. Wikipedia Contributors. (2019, March 26). Transport Layer Security. Wikipedia; Wikimedia Foundation. <https://en.wikipedia.org/wiki/Transport_Layer_Security>
13. Wikipedia Contributors. (2019b, December 12). Elliptic-curve Diffie–Hellman. Wikipedia; Wikimedia Foundation. <https://en.wikipedia.org/wiki/Elliptic-curve_Diffie%E2%80%93Hellman>
14. Wikipedia Contributors. (2019c, December 12). Elliptic-curve Diffie–Hellman. Wikipedia; Wikimedia Foundation. <https://en.wikipedia.org/wiki/Elliptic-curve_Diffie%E2%80%93Hellman>