SSL 3.0 and 2.0 Comparison and Analysis

Abstract

The SSL protocol is a digital signature, which is widely used for authenticating and establishing secure and encrypted connection between client and server. Although having some minor flaws, which can be easily solved through its superficial layer and without changing the whole base of protocol, SSL has proved to be a very efficient of safe client/server connection, that google itself has assigned it to its HTTP protocol.

This certificate is vastly exerted, due to its versatility and convenience. It is used almost in every browser and user doesn't need to enter a password nor and ID to have a secure connection. Here we describe at lengths the main aspects behind this technology.

Keywords: encrypted, data, authentication, server, certificate, web

1 Introduction

SSL[1] certificate in simple words keeps the connection between client (that can be you) and server secure and precludes criminals from reading and acquiring sensitive data like credit card numbers in payment gateways. For this reason enterprises and organizations add its certificate to their websites in order to keep these kind of information private.

Moreover having SSL connection in your website has the other benefits like the possibility of increase in rank in Google organic search and gaining the trust of visitors.[kasp]

Not only business websites, but also private websites use SSL to prevents attackers from copying the website and creating a fake version of it. Obviously for both domains encrypting their traffic is one of the most priorities.

HTTP[2] is an application protocol that determines how the information is transferred [1]through internet. The 'S' at the end of HTTP in websites indicates that the connection with that site is secure and date is safe. No matter the kind of browser without this

1. Secure Socket Layer
2. Hypertext Markup Language

certificate you will get an alert message when entering the website. This is a clear signal that the site is not safe.[kin]

In this paper, at segment 2, we take a look at a brief history of SSL, it's flaws and different types of SSL. After that in section 3 we'll discuss SSL layers. Then in segment 4 we talk about SSL's way of work and its ways of encryption. Next in segment 5 we evaluate different SSL attacks.

At the end, at section 6, we conclude that this version 3.0 of SSL is one of the most effective ways of secure and encrypted connection considered its strengths and weaknesses.

2 Background

SSL version 1.0 first developed during 1990s, however due to its flaws it was never released and used. Later on SSL 2.0 was introduced in 1995 but still had some security malfunctions, which lead to a totally redesign of SSL 3.0, that is used today.[kin]

Nowadays SSL is used with another name, TLS[3]. TLS came after SSL but it's more secure and up to date than SSL. In fact most of the websites that claim to have SSL certificate, actually have TLS, which is much more secure than SSL.

SSL has two layers, that each layer uses the services that are provided by lower services and itself provides functionality for upper layers, which is very like TCP protocol. The record layer provides classification and authentication for dependable transport protocol.

The layer above record layer is SSL handshake layer. It is a kind of key-exchange protocol that initialize and harmonize cryptographic at two endpoints. When its complete the confidential data of a n application can be sent via record layer.[wag]

2.1 Drawbacks of SSL 2.0

SSL 3.0's goal is to fix SSL 2.0 security weakness, which we'll mention briefly here. SSL 2.0 weaken the authentication keys to 40 bits, and it is very weak in MAC infrastructure, although it might seem to stop attacks.

In MAC SSL 2.0 makes the padding bytes into cipher blocks, however it leaves the padding length obvious, which can lead to detection of the bytes at the end of messages by attackers.[2]

[3]. Transport Layer Security

Also it has no protection for handshake protocol and the attacker in the middle attack can go undetected. It expects fixed domain certificate and mere single service and clashes with most of virtual hosting web servers.[wag]

2.2 Types of SSL certificate

There are different types of SSL certificate depending on the data and work context of the website, that are as follows:

1. Extended Validation certificates (EV SSL)
2. Organization Validated certificates (OV SSL)
3. Domain Validated certificates (DV SSL)
4. Wildcard SSL certificates
5. Multi-Domain SSL certificates (MDC)
6. Unified Communications Certificates (UCC)

2.2.1 Extended Validation certificates (EV SSL)

This is the highest-ranking and most expensive type of SSL certificate. It is used for websites which collect data and involve online payments or in other words E-commerce websites. When installed, this certificate displays the padlock, HTTPS, name of the business, and the country on the browser address bar. Depicting the website owner's information in the address bar at the top helps distinguish the site from fake ones. The EV SSL certificate, provides exclusive rights to the owners domain and must be executed by a standard identity verification.[kasp]

2.2.2 Organization Validated certificates (OV SSL)

This version of certificate is similar level to the EV SSL certificate. To obtain one; the website owner must complete some validation processes. This type of certificate also displays the website owner's information in the address bar to distinguish from malicious ones. OV SSL certificates is the second most expensive (after EV SSLs), and their main purpose is to encrypt the user's sensitive data during transactions. Commercial or websites must install an OV SSL certificate to make sure that any customer information shared, remains confidential.[kasp]

2.2.3 Domain Validated certificates (DV SSL)

The validation process to obtain this type of certificate is minimal, consequently, Domain Validation SSL certificates provide lower assurance and minimal encryption. They are used for blogs or informational websites, which do not involve data collection or online payments. This type of certificate is one of the least expensive and fastest ones to obtain. The process for validation merely requires website owners to prove that the domain is theirs only by sending an email or a phone call. The address bar only shows HTTPS and a padlock with no business name.[kasp]

2.2.4 Wildcard SSL certificates

Wildcard SSL certificate allows you to secure a base domain and unlimited sub-domains on a single certificate. Wildcard SSL certificates have an asterisk * as part of the common name, where the asterisk represents any valid sub-domains that have the same base domain.[kasp]

2.2.5 Multi-Domain SSL Certificate (MDC)

A Multi-Domain certificate can be used to secure many domains and/or sub-domain names. This entails the composition of totally unique domains and sub-domains with different TLDs (Top-Level Domains) apart from local/internal ones.

Multi-Domain certificates do not support sub-domains by default. If you need to secure both www.example.com and example.com with one Multi-Domain certificate, then both hostnames should be specified when obtaining the certificate.[kasp]

2.2.6 Unified Communications Certificate (UCC)

Unified Communications Certificates (UCC) are also types Multi-Domain SSL certificates. At the beginning they were designed maintain security for Microsoft Exchange and Live Communications servers. Nowadays, any website owner can use these certificates to secure multiple domains with single certificate. UCC are certified organizationally and are verified and exhibited a padlock on a browser. UCCs can be used as EV SSL certificates to give website visitors the highest assurance through the green address bar.[kasp]

2.3 Summary

In summary, after repairing most of it flaws, SSL has provided various ways of data protection in both aspects of security level and the expenses, which site owners are free to choose between.

3 The Layers

3.1 Record layer

This layer is at the bottom of the SSL protocol and assumes that key-exchange protocol has safely set up session state and key parameters. It sends blocks of data between client and server and if multiple messages are sent to quickly those messages will converted to a single SSL record, or alternatively be broken to smaller SSL records.[wag]

Each of these records are compressed and encrypted according to the encryption algorithm. For an instance in MAC they are calculated with this formula:

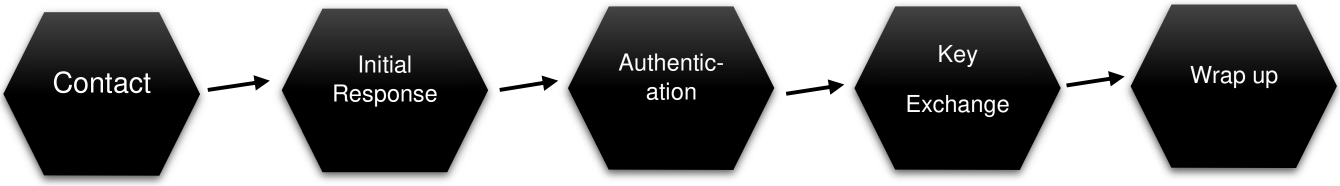
```
hash( MAC_write_secret + pad_2 +
     hash(MAC_write_secret + pad_1 + seq_num + length + content))
```

Where *MAC_write_secret* is a secret between server and client to ensure safe transmission.[ore]

3.2 Handshake layer

Handshake Protocol is used to establish sessions. This protocol allows the client and server to authenticate each other by sending a series of messages to each other. [intel]

The procedure for SSL handshake



- **Contact:** A client’s message is sent the server via the browser. The message contains sensitive information such as the client’s SSL version, encryption settings and session-specific information.
- **Initial Response:** As the first response, the server sends back security verification through some certificates, the server’s encryption settings, and session-specific data.
- **Authentication:** The browser validates the security certificate to confirm that it communicated with the correct authority.
- **Key Exchange:** The server and the browser of the client exchanges these keys. This exchange is confirmed with security.[intel]
- **Wrap up:** Both the sides, that are the browser and server will confirm that the exchange has taken place and the work is now complete.

4 How SSL works and Fundamental concepts

The main aim of SSL is ensuring that any data transferred between users and websites, or between two systems, remains impossible to read. It uses encryption algorithms to scramble data in transmission, which precludes attackers from reading it as it is sent over the connection.

The process works like this:

1. A client attempts to connect to a website (i.e., a web server) secured with SSL certificate.
2. The browser or server requests that the web server identifies itself for extra security.
3. The web server sends the browser or server responses with a copy of SSL certificate.
4. The browser or server checks to see whether the SSL certificate is verified. If it does, it sends a signal the webserver.
5. After that the web server returns a digital signed acknowledgment to initiate an SSL encrypted session.
6. Encrypted data is shared between the browser or server and the webserver.

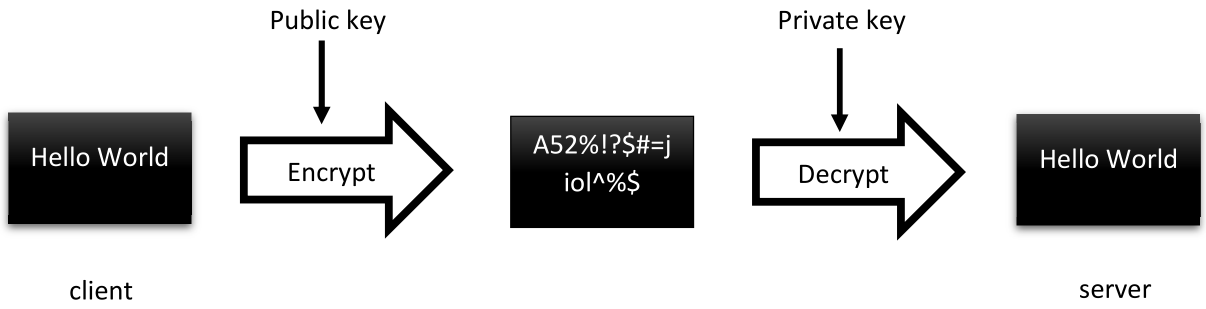
SSL certificate uses two kind of algorithms for encrypting and transmitting data, which are Asymmetric cryptography and Symmetric Cryptography.[tut]

4.1 Asymmetric cryptography

Asymmetric cryptography (also known as Asymmetric Encryption or Public Key Cryptography) uses a mathematical related key pair to encrypt and decrypt data. In a key pair, one key is shared with any server who is interested in a communication. This is called Public Key. The other key is kept secret and is called Private Key.

Public and private keys are mathematical related and were created using cryptographic algorithms which are based on mathematical problems termed one-way functions. These keys are mainly used to encrypt and decrypt the data.[tut]

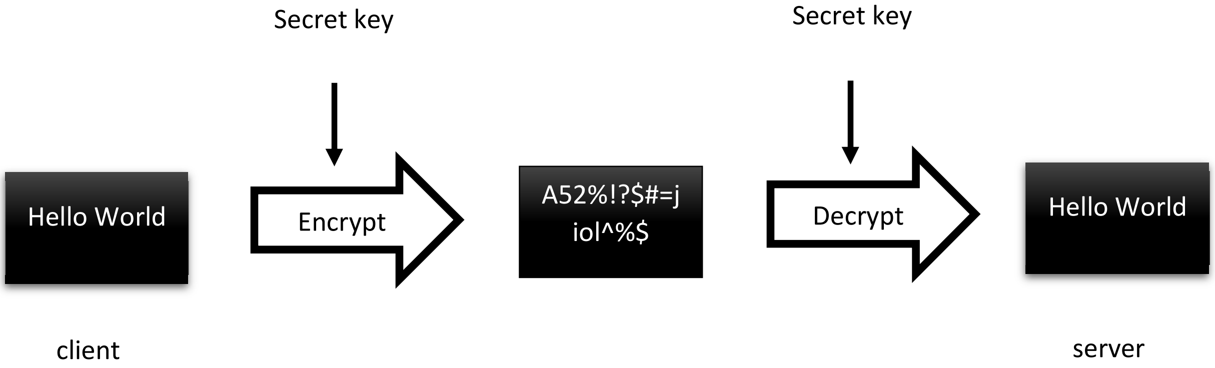
In the asymmetric cryptography, the sender encrypts the data with the receiver's public key and sends it to the receiver. The receiver decrypts it with the help of related private key.



4.2 Symmetric Cryptography

In the symmetric cryptography, there is only one key that encrypts and decrypts the data. Both sender and receiver must have this key, that is only defined to them.

SSL uses symmetric cryptography with session key after the first handshake is done. The symmetric algorithms, which are used widely are AES-128, AES-192 and AES-256.[tut]



5 SSL Attacks

It is true that SSL must and do perfectly protect confidential data against attacks, and it appears that underlying encryption is sufficient for information privacy. However recent studies by IETF have revealed that it is not enough on its own and perplexing attacks to record layer can breach system. Some of these attacks include: 1- Replay attacks 2- Exhaustion Attacks 3- Ciphersuite rollback attacks.

5.1 Replay attacks

These kinds of attacks are not much of concern as they are easy to preserve against. SSL protects data against these attacks by including a sequence number in MACed data. Re-ordered, deleted or delayed information are also protected via this mechanism.

These sequence numbers are 64 bit long so they shouldn’t be hard to wrap up and they are refreshed for each new key exchange so they roughly have no susceptibility.[wag]

5.2 Exhaustion attacks

This kind of SSL attack targets the SSL handshake protocol either by sending worthless data to the SSL server which will result in connection issues for legitimate users or by abusing the SSL handshake protocol itself.

There are many potential DDoS attacks that can exploit the SSL handshake to exhaust server resources. The Pushdo botnet accomplishes this pretty easily by sending rubbish data to a goaled SSL server. The SSL protocol is expensive and generates extra workload on the server to process garbage data as a legitimate handshake. Firewalls can’t help in this case because they are not usually capable of differentiating between valid and invalid SSL handshake parcels. Full DDoS protection could help against these kinds of attacks.[net]

Another SSL-based DDoS attack tool is the THC-SSL-DOS tool, that works by completing a normal SSL handshake but then immediately requests a renegotiation of the encryption method. As soon as the first renegotiation completion, it requests another renegotiation, and this continues. If the server SSL’s renegotiation is disabled, then it’s tool simply ends the SSL connection as soon as the negotiation completes and opens a new connection to start a new negotiation process. This is extremely computationally expensive and is effective at making services unavailable to legitimate users due to resource exhaustion.[net]

5.3 Ciphersuite rollback attacks

This kind of attack is mainly related to SSL 2.0, that an active attacker can silently user to use weakened encryption and it can be performed by editing cleartext list of ciphersuites send in messages.[wag]

SSL fixes this issue by authenticating all messages by *master_secret*, in which, the attacker can be determined at the end of handshake and session can be terminated.

5.4 Summary

As disscussed there are multiple ways to attack and breach SSL security, even though it has many built in features in order to prevent these threats and data exposures. However with help of TLS beside SSL most of these attacks are in vain.

6 Conclusion

This aim of this paper was to demonstrate the pros and cons of SSL protocol and the method of this mechanism, which is today, is used almost in every webpage and all the data in Internet go through its process.

In general by comparing SSL 3.0 and 2.0 it was indicated that SSL 3.0 has much more safer routes and features and we saw SSL 2.0 downsides and realized why it never released.

This paper revealed the different types of SSL protocols and their area of usage and how they can be obtained for one's website or how secure each certificate is.

This paper also revealed the different SSL algorithms and we saw how client and server interact with each other. Each process for data in either of these algorithms was also stated.

Different attacks that can threaten the SSL protocol was also discussed and we saw that SSL uses specific ways to deal with each attack which can prevent of data loss or revelation.

Overall it was proved that SSL protocol is today the most used and safest way of data transmission through the Internet.

7 Acknowledgements

It is hereby stated that this paper is compiled from different references and any credits will go those papers. Any mistakes, of course, is solely my responsibility.

References

[kin] https://kinsta.com/knowledgebase/how-ssl-works/

[kasp] https://www.kaspersky.com/resource-center/definitions/what-is-a-ssl-certificate

[ore] https://www.oreilly.com/library/view/web-security-and/1565922697/apcs02.html

[intel] https://intellipaat.com/blog/what-is-ssl-handshake/

[geek] https://www.geeksforgeeks.org/secure-socket-layer-ssl/

[tut] https://www.tutorialsteacher.com/https/how-ssl-works

[net] https://www.netscout.com/what-is-ddos/ssl-tls-exhaustion

[seek] https://www.seekahost.com/flaws-in-ssl-version-2/

[wag] https://www.usenix.org/legacy/publications/library/proceedings/ec96/full_papers/wagner/wagner.pdf

[bbl] https://bblfish.net/tmp/2009/05/spot2009_submission_15.pdf

[rfc] https://www.rfc-editor.org/rfc/rfc6101.html