North Asian International Research Journal of Sciences, Engineering & I.T.

ISSN: 2454-7514 Vol. 7, Issue-1 January -2021

IRJIF. I.F. : 3.821

Index Copernicus Value: 52.88 Citation Index

A Peer Reviewed Refereed Journal

UTILIZATION OF CRYPTOGRAPHY FOR HTTPS PROTOCOL

MALIK BILAL*

****Software Engineer at HOSTGATE.IN India's Best Web Hosting Company***

ABSTRACT

For this project, I will be choosing the protocol HTTPS. During the course of this project, I will be provided detailed information in regards to the utilization of cryptography. I will also be providing insight on the cryptographic algorithms that are utilized with this protocol. I will also examine the algorithm that is utilized and provide insight on the steps that are utilized with this protocol. I will also be providing information in regards to the aspects of the algorithm and how it appealed to the committee/decision-makers. I will also provide insight on the different types of software and systems which utilize this protocol as well.

***KEY-WORDS**: Utilization, Cryptography, Https, Protocol, SSL, TSL, Hostgate.in*

Cryptographic Algorithms

HTTPS does not have one specific type of algorithm that it utilizes when it is transmitting data through its protocol. HTTPS has an embedded type of algorithm in its code. In 1994, Netscape Communications created HTTPS, which means Hypertext Transfer Protocol over Secure Socket Layer (Hoffman, 2018). They created this algorithm to provide a secure method from transmitting data over the Internet. HTTP was created to transfer information through the Internet, but unfortunately all of the data transmitted was in clear text. A standard needed to be created to rectify this and HTTPS was the standard created to fix this problem.

HTTPS works by encrypting all information, whether it is secret, sensitive or is not sensitive information, traveling from a user's web browser to the server of whatever website they are browsing to and utilizing (Rose, 2017). This algorithm provides additional layers of security for the information being transmitted because it obscures the data in a manner that is not easily read by those who should not be accessing the information. When HTTPS was implemented it utilized SSL for its encryption protocol, now SSL has been updated. The newer version of SSL that is being utilized in HTTPS is TLS, which stands for Transport Layer Security (Admin, 2018). TLS and SSL provides the same functionalities, TLS provides stronger encryption algorithms and it has the ability to work on different ports.

Utilizing SSL and TLS for HTTPS is a match made in heaven because of the encryption algorithms utilized for this protocol. The algorithm used for this protocol is both symmetric and asymmetric algorithm. SSLTLS utilizes asymmetric and symmetric encryption by encrypting the server certificate with an asymmetric public and private key pair (DigiCert, 2019). This allows for a more secure connection and transmission of data through this session. The next step of the process the session key create by the server and the browser forms the symmetric portion of the SSL handshake (DigiCert, 2019). Because the server and the browser both know what the session key is they are able to encrypt the data through this session without any issues.

A simpler way of explaining the process is the server pushes out a copy of the asymmetric public key that it is storing (DigiCert, 2019). During the next step of the process whatever web browser a person is utilizing creates a symmetric session key that is combined and encrypted with the server's asymmetric public key. Then the product of the previous steps is sent to the server. The server will decrypt the product of the previous step using the asymmetric key stored on the server and then it will be able to discover the symmetric key that came from the browser (DigiCert, 2019). The final step of the process the server and the web browser can now encrypt and decrypt all data sent through a connection with the symmetric session key because they have taken all of the necessary steps and precautions to validate the security measures of the session.

Appeal of HTTPS

There are many aspects and features within SSL/TLS which made it an ideal choice for the developers of HTTPS to choose this type of algorithm. Several of those features are the ability for SSL/TLS to be able to set up cipher suites (Symantec, 2019). This is a great feature because it can be utilized with different web browsers and server operating systems. Different browsers and different server operating systems require certain modifications and configurations to make their products work and secure. Because of these factors it could have been extremely hard to find the right product to use for encrypting web traffic. SSL/TLS makes this choice easy because this algorithm it provides the ability for clients and servers to share their capabilities. With this step the devices can figure out the cryptographic features they both can support.

Another feature which made SSL/TLS the encryption algorithm choice for HTTPS is the ability for authentication to happen from the server and client. During this process the client verifies to make sure the certificate provided by the server is an authentic one (GlobalSign, 2018). This feature is important because for a connection to be truly secure not only does the data have to be encrypted. Verification needs to happen to determine that the data is being sent to the right website or company. SSL/TLS provides the verification steps needed to authenticate that the data is being encrypted and transmitted to the right website or company.

Install and Maintain

Transforming HTTP to HTTPS there is a process that must be followed for this to be done efficiently and correctly. A verified certificate must be installed on the web hosting server for an organization to enable secure web browsing for their users. There are several options for obtaining a secure certificate. An organization can acquire a HTTPS certificate from a certificate authority (CA), utilized a cloud-based HTTPS certificate or

implement a free HTTPS certificate (Heinig, 2018). Obtaining a certificate from a CA comes at a cost but with the cost it provides support from the organization with getting the certificate properly installed on the web server.

An organization must create a private key file and a certificate signing request (CSR) from their web server (DigiCert, 2019). Once this step is completed they must provide the contents of their CSR to a CA or take the necessary steps to generate a self-signed certificate which is not verified by a CA. After providing the contents of their CSR to a CA, the CA will validate the certificate request. After the validation is completed, the CA will email the requester their SSL certificate. To properly maintain their certificates organizations must follow the process to request their certificates each time that they certificates expire. Depending on the length the certificates may last for a year or multiple years.

References

1. Admin. (2018, August 2). What is HTTPS | Difference between HTTP and HTTPS | How its Work? Retrieved June 30, 2019, from https://www.webinspector.com/blog/website-security-check/what-is-https-and-why-switching-to-https/
2. DigiCert. (2019). SSL Certificate Installation Instructions & Tutorials. Retrieved July 9, 2019, from https://www.digicert.com/ssl-certificate-installation.htm
3. GlobalSign. (2018, May 22). What's the difference between HTTP and HTTPS? Retrieved June 30, 2019, from https://www.globalsign.com/en/blog/the-difference-between-http-and-https/
4. Heinig, I. (2018, May 21). How to Obtain an HTTPS Certificate for Your Website. Retrieved July 13, 2019, from https://themanifest.com/web-design/how-obtain-https-certificate-your-website
5. Hoffman, C. (2018, October 15). What Is HTTPS, and Why Should I Care? Retrieved June 30, 2019, from https://www.howtogeek.com/181767/htg-explains-what-is-https-and-why-should-i-care/
6. Rose, A. (2017, November 10). How HTTPS Works: The Basics of Internet Security and Privacy. Retrieved June 30, 2019, from https://strongarm.io/blog/how-https-works/
7. Symantec. (2019). What is SSL, TLS and HTTPS? Retrieved June 30, 2019, from https://www.websecurity.symantec.com/security-topics/what-is-ssl-tls-http
8. https://hostgate.in/