International Journal of Sciences: Basic and Applied Research (IJSBAR)

ISSN 2307-4531
(Print & Online)

http://gssrr.org/index.php?journal=JournalOfBasicAndApplied

A Discussion of Internal Communication Procedure of Transport Layer Security Protocol on Telecommunication Networks

Ahmed Faraz*

Senior Assistant Professor, Department of Computer Engineering, Bahria University Karachi Campus,
13-National Stadium Road, Karachi 75260, Pakistan
Email: ahmedfaraz.bukc@bahria.edu.pk
Email: ahmed.faraz2004@gmail.com

Abstract

The research paper written by us discusses the review of internal communication procedure of Transport Layer Security protocol on telecommunication networks. In this research paper we discuss the security measures and security techniques employed by Transport Layer Security protocol for the provision of data privacy, confidentiality and authentication on telecommunication networks to the network users. The telecommunication networks include both the wired and wireless communication networks mostly including computer communication networks. The connection establishment for connecting client side and server side used by Transport Layer Security protocol is discussed in this research paper in order to facilitate the understanding of internal connection establishment and internal connection management procedure between client side and server side of telecommunication network. We have focused on Cipher Suit and Security Services provided by Transport Layer Security protocol in detail in order to high light key features of connection establishment in Transport Layer Security protocol. The discussion in the research paper will be useful for extension of Transport Layer Security protocol's usability and implementations by researchers.

Keywords: Cipher Suit; Finished Message; Security Services; Handshake; Cipher Spec Messages.

----

* Corresponding author.

1. Introduction

In this research paper we will discuss the Transport Layer Security in detail for the purpose of providing the readers and the researchers a detailed description of the security and protection provided by the Transport Layer Security (TLS) protocol of communication networks. As we know that the information transmitted over insecure computer communication networks or over wireless communication networks also contain sensitive data which is to be transmitted over communication network. The two protocols Secure Socket Layer (SSL) protocol and Transport Layer Security (TLS) protocol provide secure transmission of sensitive data over insecure communication networks, but TLS replaced SSL as referred in [13,14,15]. In order to understand TLS protocol, Internet's Client Server model and design principles of computer communication protocols should be understood by the reader of the paper. There are many online transactions in which TLS protocol is used. Financial transactions, medical transactions, social networking transactions use TLS protocol for transmitting sensitive information over communication networks. The examples of financial transactions incorporate credit card/ debit card transactions, transmission of sensitive financial data, transactions through online financial apps. The examples of medical transactions include sensitive medical reports data through communication networks. The social networking transactions include the data from email transfer and passwords transfer through communication networks. All these transactions utilize TLS protocol for secure transmission of sensitive data as discussed in [11,12,13]. In order to understand the underlying working of Transport Layer Security (TLS) protocol, the engineer should have an in depth understanding of the protocol architecture, data transmission unit of the discussed layer "Transport Layer", the security provision in data transmission unit, client server communication, operating systems configurations on client side and server side, operating systems adaptability and hardware compatibility issues. In this review paper, we will try to address all of these study and analysis points of TLS protocol.

2. Previous Work

From the beginning of computer networks and networking, the scientists and researchers had been thinking about the security of data transmitted over networks connections. The scientists and engineers started their work on designing and implementing protocols which can provide security to the data transmission at renowned computing based companies for example Netscape, Microsoft, and IBM etc.The figure 1 elaborates in an expressive way the evolution of Secure Socket Layer protocol which was designed and developed at Netscape Communications. The time line begins in November 1993 with the release of Mosaic 1.0 by National Centre for Super Computing Applications NCSA. Mosaic was the first popular web browser. Netscape Communications designed and developed the first version of SSL after eight months. Then five months later, Netscape Communications launched its web browser with the support of second version of SSL i.e. SSL2.0 with the name Netscape Navigator. Microsoft published Private Communication Technology PCT specification and invented its first version of Private Communication Technology PCT as an extension of SSL version 2.0. PCT addressed many weaknesses of SSL version 2.0 and later on a new version of SSL which is SSL version 3.0 was launched and many of its ideas were incorporated in it. The figure 1 describes the time line for the invention of SSL and its new versions. The milestone achievement of Netscape is the US patent for SSL and Netscape developed all three versions of SSL from the feedback of web community. The development of SSL was kept open. The

Internet Engineering Task Force developed many standards for internetworking and to avoid any bias for any company IETF renamed SSL as TLS. The SSL used for many years and it is very popular but the difference between SSL and TLS should be discussed in the future research papers.

The Transport Layer Security (TLS) protocol was proposed in 1999 by Internet Engineering Tasks Force (IETF) and this protocol was invented for providing security measures and cryptographic facilities in the protocols running on application layer of OSI model. The TLS protocol versions range from 1.0 to 1.3 and this protocol runs on application layer. The current version of running protocol is TLS 1.3. The TLS protocol has the provision of security by using certificates shared and used between both sides of communicating network. The weaknesses of Secure Socket Layer (SSL) protocol were removed by Transport Layer Security (TLS) protocol in its different versions. The Secure Socket Layer (SSL) protocol was invented by Netscape Company for providing security to HTTP and turn HTTP into HTTPS. Both protocols run over application layer of OSI model.

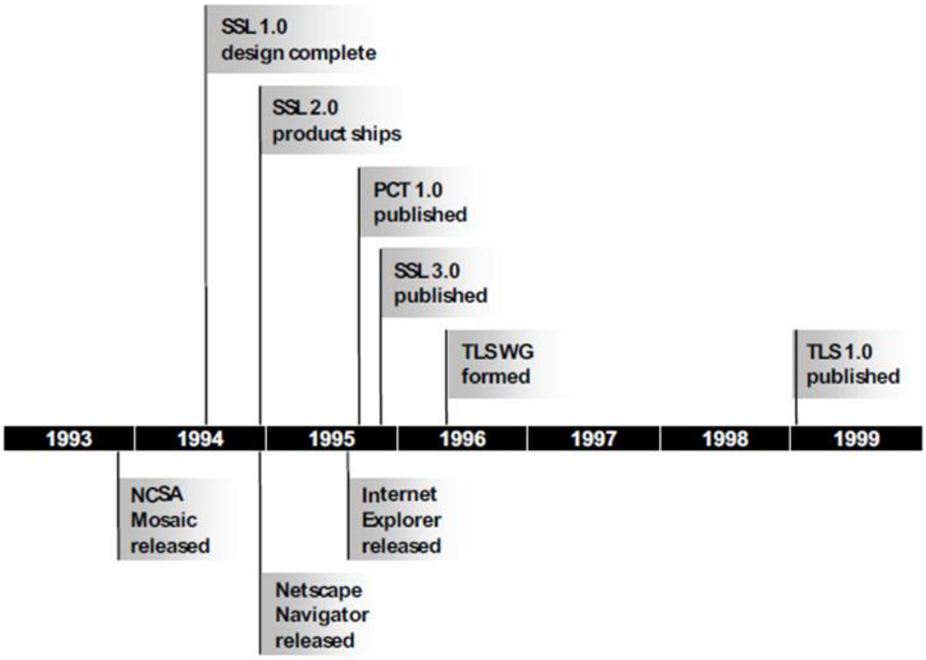

Figure 1: Time Line of Invention of Secure Socket Layer and Transport Layer Security Protocol.

All of the discussion of previous work is referred from [21,22].

3. Superseding SSL by TLS

The Transport Layer Security (TLS) protocol is successor of Secure Socket Layer (SSL) protocol. The Secure Socket Layer (SSL) protocol started its evolution from SSL version 1.0. Whenever the protocols were designed, the protocols evolved and the designers need to consider all of the issues raised during the evolution of protocols design from origin. The issues raised during the evolution of protocols are hardware compatibility, operating systems adaptation, and layers acceptance from the client side to the server side. The shortcomings of SSL protocol insists scientists to work on a new protocol to overcome the shortcomings of SSL and they work towards invention of TLS. The discussion of the comparison of SSL and TLS is a big work and many researchers worked on this topic as discussed in [14,15,16]. But there is a space on further work.

The security requirements of information systems raise day by day because of the perimeter growth of internet work and an increase in the social networking sites as referred in [17]. All of the layers of internetwork need specific levels of security, but in this review paper we will discuss the security related with transport layer specifically. As we know that the transport layer works through “segments” data unit which is usually referred by the engineers and scientists as Transmission Control Protocol (TCP) segments, we will also address the security issues provided in TCP segments. The TLS protocol has interoperability capability by using a client server model which is more adaptable and acceptable to TLS protocol. The public key certificates are provided for the authentication and Cipher Suits is provided for the purpose of secure transmission of Transport Layer segments. The data transmission unit in Transport Layer Security (TLS) protocol is TLS record as discussed in [11,12,13, 14,15].

Architecture and Communication Mechanism of TLS Protocol

In this section of our review paper we will discuss the architecture of Transport Layer Security (TLS) protocol in detail. The Transport Layer Protocol (TLS) works on the basis of TLS records. The TLS protocol exchange records with in communication between sender side and the receiver side of the communication network. In order to maintain the data records integrity, authenticity and confidentiality, TLS protocol runs cryptographic algorithms on its layer selected from a specific suit of cryptographic algorithms dedicated for TLS protocol. In order to gain an understanding of any protocol, the network engineer should have an understanding of the data transmission unit and its function. The data transmission unit of TLS protocol is record. The record consists of the following fields as shown in figure 1:

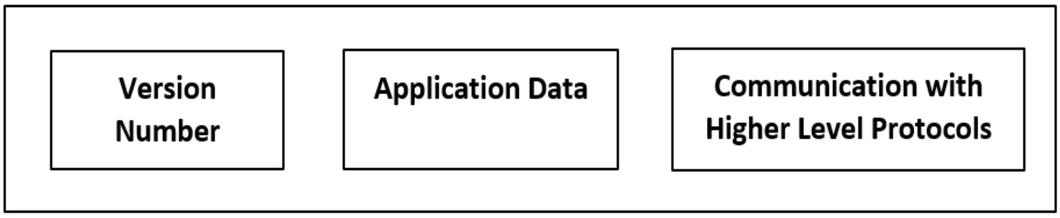

Figure 2: Transport Layer Security Protocol Record Field.

The Transport Layer Security protocol’s data transmission unit consists of the following fields:

- Version Number
- Application Data
- Communication with Higher Level Protocols

3.1. Security Parameters and Security Measures in relation with TLS record

As we know that the TLS protocol works on the “records” which is the data transmission unit of TLS protocol, the TLS protocol runs many protocol for the management of connection established between sender side and the receiver side of communication network. Each protocol with in the super set of TLS protocol has its own record and TLS protocol uses the sub record field for the purpose of managing connection between sender side and receiver side of the communication network as referred in [12]. The protocols which are active in the field of communication systems are analyzed and measured in terms of two parameters, the first one is security parameters and the second one is security measures as referred in [13]. The TLS protocol establishes and manages the connection between the client side and the server side of the communication network when security parameters are considered. And the TLS protocol issues the errors and warnings to the client side from the server side or vice versa when the security measures are considered but there is an access to TLS record through malicious user or an attacker.

The fundamental data unit for transmission of data through TLS protocol is “record” as discussed in [3,6,7]. The TLS protocol exchanges record between client and server sides for the purpose of secure data transmission. The record of the TLS protocol contains the version information, application data and the higher level protocol fields. The version information of TLS record states the current version or release of TLS protocol. The application data field of the TLS record states the data exchanged between client and server side of the communication network. The higher level protocol field states the higher level protocols on the top of the record to which application data of TLS record communicates. The block diagram of the TLS record (see figure 1) will be more explanative in understanding the fields and the working of fields in relevance with TLS protocol and the protocols in the layers of protocol stack. The TLS protocol secure the TLS record exchange through implementation of cryptographic algorithms. The data integrity, authenticity and confidentiality is provided in TLS protocol through efficient use of key management and cryptography as described in the paper [12,13].

The Transport Layer Security (TLS) protocol works on the fundamental principles of computer communication networks: data integrity, authenticity and confidentiality. These three principles are implemented in Transport Layer Security (TLS) protocol in its every sub layer and data transmission unit as referred in [13].

3.2. Sub Protocols of TLS Protocol

There are three sub protocols working in Transport Layer Security (TLS) protocols:

- Handshake Protocol
- Change Cipher Spec Protocol
- Alert Protocol

3.3. Purpose of Sub Protocols of TLS Protocol

We will describe the purpose of three sub protocols of TLS. The handshake protocol establishes the session between client and the server machine, and after the establishment of session, the handshake protocol manages the negotiated session between the two sides. The second sub protocol is Change Cipher Spec protocol, which changes the cryptographic parameters in order to secure the confidentiality of transferred data unit which is TLS record. The third sub protocol is Alert protocol which notifies the error condition to the client side and the server side when something wrong occurs during transmission of application data. The sub protocols are discussed in detail in [14,15].

3.4. TLS Handshake Protocol

The Handshake protocol works to initialize the client side and the server side of the communication network by negotiating the security services provided for the application data. The Handshake protocol exchanges series of messages between the client side and the server side for initialization of the communication session. The Cipher Suit of TLS protocol contains the algorithms for Key Establishment, Digital Signatures, Data Integrity algorithms and Confidentiality algorithms as mentioned in [16,17]. In the further review work and analysis of TLS Handshake protocol we will study and discuss how TLS Handshake protocol provides security measures using key establishment, digital signatures, data integrity and confidentiality algorithms. The papers [17,18,19]are more useful. We can visualize the stack of cipher suit of TLS Handshake protocol in order to understand the basic working of it in figure 2.

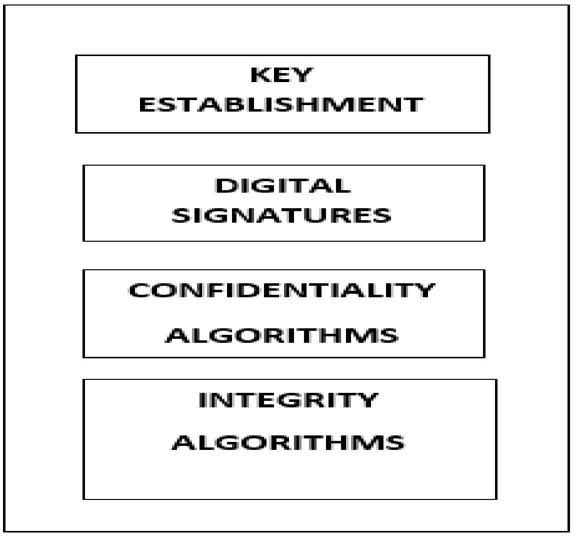

Figure 3: Cipher Suit of TLS Handshake Protocol.

3.5. Cipher Suit and Security Services of TLS Protocol

The TLS Handshake protocol exchanges messages between the client side and the server side for providing security services to the machines on network. The security services provided by TLS Handshake are Confidentiality, Integrity, Authentication and Replay protection. The TLS Handshake protocol's main purpose is to start the client side and the server side by the transmission of messages. A sequence of messages is transmitted between the client side and the server side for establishment of session between the communicating machines. The cryptographic capability in message transmission is optional at the start of the session establishment. The Cipher Suit algorithms are used in establishment of the session between the client side and the server side. As we know that the Cipher Suit of algorithms contains key establishment, digital signature, confidentiality and integrity, on or more than one services of Cipher Suit can be used by TLS Handshake protocol in order to secure transmission of records on network. After initialization of the machines, the client side and the server side are configured using one or more than one security services of TLS Handshake protocol as discussed in [20,12].

The TLS Handshake protocol provide the following security services to the client side and the server side on computer communication network:

Confidentiality of data ensures the secure transmission of data on the network by TLS Handshake protocol. The confidentiality of data prevents eavesdropping attack. The confidentiality of data is made practicable by using cryptographic algorithms in TLS record and message exchange as discussed in [20].

Integrity of data ensures the complete TLS record transmission between client side and the server side. Using integrity feature of TLS Handshake protocol's Cipher Suit, data addition, data deletion and data modification by the attacker can be prevented.

Authentication service of Cipher Suit of TLS Handshake protocol prevents forgery of data. The authentication service prevents IP spoofing attack and ensures the legalized authentic user's data transmission through computer communication network. Authentication is discussed in detail in [2].

Replay service of Cipher Suit of TLS Handshake protocol prevents malicious user's access to TLS record and messages and stop replay attack.

The security services of TLS Handshake protocol can be visualized in the following diagram labelled as figure 3:

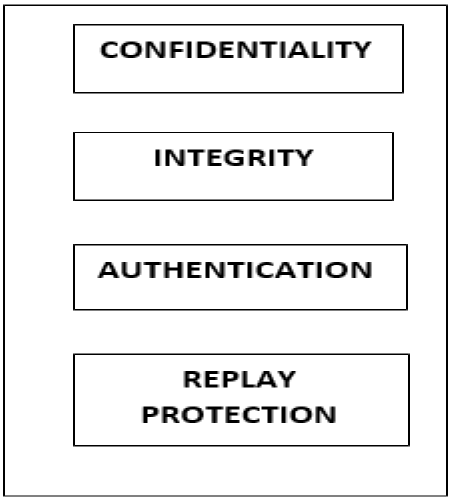

Figure 4: Security Services of TLS Protocol.

The TLS Handshake protocol provides security in order to stop the replay attack by malicious unauthenticated user. As we know that in replay attack, an unauthenticated user get access of the data transmission unit or message or packet to launch the replay attack. The Transport Layer Security TLS protocol provides implicit anti-replay which is activated when there is an increase in sequence number during transmission of TLS records. The security services are discussed in [20].

4. Authentication of Users in TLS Protocol

The Transport Layer Security (TLS) Handshake protocol provides authentication of users on the client side and the server side using X.509 public key certificates. The point to be considered most important is that all of these security services of TLS Handshake protocol which are data confidentiality, data authentication, data integrity and replay protection are made active during the configuration process on the client side and the server side of the TLS Handshake protocol. This is referred in detail in [10, 20].

5. TLS Handshake and Connection Establishment

Now we will discuss how Transport Layer Security (TLS) protocol works. First of all the Transport Layer Security (TLS) Handshake protocol is initiated, TLS Handshake establishes the session between the client side and the server side of computer communication network. Fundamentally, the session establishment and session management is done by TLS Handshake protocol in the first stage. Then cipher suit of TLS Handshake protocol is activated during which data confidentiality, data integrity and authentication services are selected between the client side and the server side by running the TLS negotiation algorithm, also the other security parameters are established during selection of services in negotiation. Also the symmetric keys are derived. In other words, after the initialization of TLS Handshake protocol, the client side and the server side runs the negotiation algorithm which negotiates on the security services which are data confidentiality, data integrity and authentication between the two sides of computer communication network. The negotiated set of security services is called “cipher suit” as referred in [13,14, 15,19].

In summarized words, we can say that in the first step TLS Handshake protocol establishes the session between the client side and the server side, then the negotiated security services including the symmetric key derivation is performed in the second step. In the third step of the TLS Handshake protocol, the ChangeCipherSpec message is transmitted by one side to the other side. The purpose of the ChangeCipherSpec message is to inform both sides of computer communication network that TLS Handshake protocol has defined services negotiated between two sides, also the symmetric keys have been defined, now the communication in the form of messages can be done. After the transmission of ChangeCipherSpec message, the message transfer starts and the messages are encrypted using derived symmetric keys and protection of messages is provided through cryptography and data integrity. The steps taken by Transport Layer Security (TLS) protocol for establishment of handshake and communication can be depicted through flowchart / block diagram in the figure 4 and discussed in detail in [12,13].

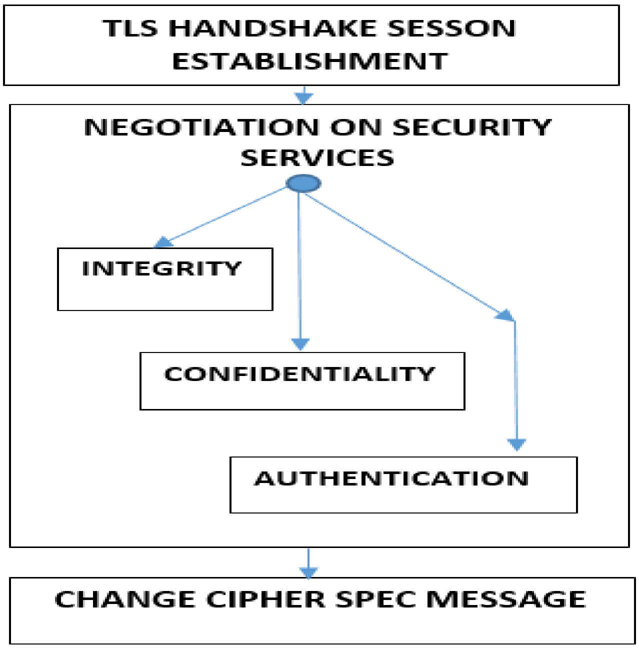
TLS HANDSHAKE SESSON ESTABLISHMENT
NEGOTIATION ON SECURITY SERVICES
INTEGRITY
CONFIDENTIALITY
AUTHENTICATION
CHANGE CIPHER SPEC MESSAGE

Figure 5: Transport Layer Security (TLS) Handshake protocol steps in handshaking between the client side and the server side.

The mechanism in TLS Handshake protocol connection establishment is of deep interest and can be used as a paradigm for design of new more sophisticated and more secure transmission layer protocols in the future. The TLS Handshake protocol establishes session by making decision on session parameters on the client side and the server side of the communication network. Session parameters are also referred as security parameters or security measures in literature as referred in articles [25,26]. After definition of security parameters, the ChangeCipherSpec message is transmitted between client side and the server side of the communication network. After the successful transmission of the ChangeCipherSpec message, the sequence of messages starts transmission. The purpose of ChangeCipherSpec message is to send the informative message from the client to the server or vice versa that negotiated services are agreed by both sides and a set of confidentiality, integrity, authentication services are agreed by both sides, now transmission of messages can be started. We think that TLS protocol is over secure in such a manner that after transmission of ChangeCipherSpec message, the handshake messages are assessed for integrity check. Also the transmission of ChangeCipherSpec message is protected using negotiated cipher suit and derived symmetric keys. The messages transferred after transmission of ChangeCipherSpec message, are referred as “Finished Messages”. Again Finished messages are protected using negotiated cipher suit algorithms and derived symmetric keys. As we know that cipher suit contains the sets of algorithms for integrity, confidentiality and authentication algorithms. All of these details can be referred from [17,18].

6. Constraints or Limitations of TLS Protocol

We have discussed internal communication procedure of Transport Layer Security (TLS) protocol in this review paper and the constraints proposed and implemented for TLS protocol is of utmost significance. The constraints or limitations of TLS protocol are discussed in more detail in RFC of TLS 1.3 [21]. The session resumption mechanism of TLS protocol has a vulnerability that whenever there is a connection established between the sender side and the receiver side, the identifiers are defined for connection establishment and when the connection is disconnected the identifiers which were used for connection establishment should not be reused for disconnection between sender side and the receiver side. If the same id is used for connection establishment and disestablishment the attacker can take the advantage of gaining the access of communication network through accessing identifier for connection establishment.

7. Results and Discussion of Review

As far as results are concerned, this paper elaborates the internal communication procedure of Transport Layer Security (TLS) protocol and the TLS handshake protocol’s connection establishment mechanism and cipher suit of TLS protocol. From the detailed discussion of internal communication procedure of Transport Layer Security (TLS) protocol, we got the results that the cryptographic algorithm for providing secure data transmission between the sender side and the receiver side of telecommunication network are of utmost importance, the more robust cryptographic algorithm employed in connection establishment mechanism, the more secure data transmission done in communication of data on telecommunication network. The study of typical parameters of cryptographic algorithms and comparison of cryptographic algorithms for implementation in Transport Layer Security TLS protocol is the future work of the given research. Secondly the key establishment during communication mechanism is of extreme significance, the privacy of keys to the client side and the server side can be enhanced using security based algorithms in future.

8. Conclusions

We have discussed internal communication procedure of Transport Layer Security (TLS) protocol in this review paper. The purpose of writing the review paper is to make the design and working TLS protocol more understandable for engineers, software developers and computer scientists using the diagrammatic representation of TLS protocol’s main entities and parameters. The TLS protocol is an extension of SSL 3.0 protocol and provides more strength on securing transfer of application data between the client side and the server side of communication network. When we discuss the protocol design we have to include many facets of communication protocol in the review procedure. We have tried our best to discuss the TLS protocol thoroughly, but it is impossible to cover all features of TLS protocol in a single review paper. This paper will be helpful for graduate students, PhD students and scientists who are doing their work in protocol design and network security.

Acknowledgements

We are thankful to higher management of Bahria University Karachi Campus for motivating us to work on our research interests and move toward prolific research publications.

References

[1]. Li, P., Su, J., & Wang, X. (2020). ITLS: lightweight transport-layer security protocol for IOT with minimal latency and perfect forward secrecy. *IEEE Internet of Things Journal*, *7*(8), 6828-6841.

[2]. Kumar, P. M., & Gandhi, U. D. (2020). Enhanced DTLS with CoAP-based authentication scheme for the internet of things in healthcare application. The Journal of Supercomputing, 76(6), 3963-3983.

[3]. Platzer, F., Schäfer, M., & Steinebach, M. Critical traffic analysis on the tor network. In Proceedings of the 15th International Conference on Availability, Reliability and Security (pp. 1-10). (2020, August)

[4]. Zhang, F., Maram, D., Malvai, H., Goldfeder, S., & Juels, A. Deco: Liberating web data using decentralized oracles for tls. In Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security. (2020, October). (pp. 1919-1938).

[5]. Chalkiadakis, N., Deyannis, D., Karnikis, D., Vasiliadis, G., & Ioannidis, S. The million dollar handshake: secure and attested communications in the cloud. In 2020 IEEE 13th International Conference on Cloud Computing (CLOUD) IEEE. (2020, October). (pp. 63-70).

[6]. Levillain, O. Implementation flaws in TLS stacks: lessons learned and study of TLS 1.3 benefits. In International Conference on Risks and Security of Internet and Systems Springer, Cham. (2020, November). (pp. 87-104).

[7]. Sidna, J., Amine, B., Abdallah, N., & El Alami, H. Analysis and evaluation of communication Protocols for IoT Applications. In Proceedings of the 13th international conference on intelligent systems: theories and applications (2020, September). (pp. 1-6).

[8]. Bhattacharjya, A., Zhong, X., Wang, J., & Li, X. (2020). CoAP—application layer connection-less lightweight protocol for the Internet of Things (IoT) and CoAP-IPSEC Security with DTLS Supporting CoAP. In Digital twin technologies and smart cities (pp. 151-175). Springer, Cham.

[9]. Iashvili, G., Iavich, M., Gagnidze, A., & Gnatyuk, S. (2020). Increasing Usability of TLS Certificate Generation Process Using Secure Design. In IVUS (pp. 35-41).

[10]. Quan, L., Guo, Q., Chen, H., Xie, X., Li, X., Liu, Y., & Hu, J. SADT: syntax-aware differential testing of certificate validation in SSL/TLS implementations. In2020 35th IEEE/ACM International Conference on Automated Software Engineering (ASE)IEEE. (2020, September). (pp. 524-535).

[11]. Alemu, S. B. (2020). The transformation of TLS from version 1.2 to 1.3.

[12]. Dierks, T., & Rescorla, E. (2008). The transport layer security (TLS) protocol version 1.2 (No. rfc5246).

[13]. Polk, T., McKay, K., & Chokhani, S. (2014). Guidelines for the selection, configuration, and Use of transport layer security (TLS) implementations. NIST special publication, 800(52), 32.

[14]. Rescorla, E. (2000). Http over tls (No. rfc2818).

[15]. Dierks, T., & Allen, C. (1999). The TLS protocol version 1.0 (No. rfc2246).

[16]. Jager, T., Kohlar, F., Schäge, S., & Schwenk, J. On the security of TLS-DHE in the standard model. In Annual Cryptology Conference Springer, Berlin, eidelberg. (2012, August). (pp. 273-293).

[17]. Heinz, C., Zuppelli, M., & Caviglione, L. (2021). Covert Channels in Transport Layer Security: Performance and Security Assessment. J. Wirel. Mob. Networks Ubiquitous Comput. Dependable Appl., 12(4), 22-36.

[18]. Ayuninggati, T., Harahap, E. P., & Junior, R. (2021). Supply Chain Management, Certificate Management at the Transportation Layer Security in Charge of Security. Blockchain Frontier Technology, 1(01), 1-12.

[19]. Ahmad, M., Riaz, Q., Zeeshan, M., Tahir, H., Haider, S. A., & Khan, M. S. (2021). Intrusion detection in internet of things using supervised machine learning based on application and transport layer features using UNSW-NB15 data-set. EURASIP Journal on Wireless Communications and Networking, 2021(1), 1-23.

[20]. Yaseen, M., Kamel, M., & Ligeti, P. (2022). Security Analysis and Deployment Measurement of Transport Layer Security Protocol. In Recent Innovations in Computing (pp. 725-739). Springer, Singapore.

[21]. Rescorla, E. (2018). The transport layer security (TLS) protocol version 1.3 (No. rfc8446).

[21]. Thomas, S. (2000). SSL and TLS essentials. New Yourk, 3.

[22]. Oppliger, R. (2016). SSL and TLS: Theory and Practice. Artech House.