International Journal of Engineering Research and Technology. ISSN 0974-3154, Volume 14, Number 9 (2021), pp. 895-900
© International Research Publication House. http://www.irphouse.com

Trends and Impact Advances in the Implementation of the Transport Layer Security (TLS) Security Protocol

Johana A. Mendoza Aguilera[1] and Norberto Novoa Torres[2]

[1, 2] Engineering Department, Universidad Distrital Francisco José de Caldas, Bogotá D.C. – Colombia.

Abstract

Although, it presents the use of SSL and TLS as protection mechanisms of communication trough encryption in data transportation making it been the most used crucial service, like messaging, financial transactions, etc., At the same time, it becomes in an attack target through its different versions which they have managed to be successful because of different methods. Making the protocol to evolve rapidly in its implementation modes and present improvements by means of hybrid solutions with the aim to solve those found security breaches or to give power to other services. In this document it is presented an analysis of these affirmations, managing to determine how safe the protocol is at the moment and how it prepares to the future.

Keywords: SSL, TLS, Comunication, Encryption, Accreditation, Security, Safe protocols, Cryptography.

I. INTRODUCTION

Nowadays, technology presents high advantages ahead of the challenges of security communication. These advantages have been appearing through years by reason of ensure the information that is transmitted through them. Talking about more specifically security communication in internet, we enter to assess the security methods about safe protocols, as is already known SSL and TLS provide authentication services in costumer-server architectures making them to overcome the confidentiality and integrity challenges, although it gets shorter when it does not bear the principle of not rejection generating somehow a type of vulnerability in its implementations.

In this current document we will make an analysis about the protocol in general, firstly the interaction and its way of work, then we can assess studies and researches that have been worked by different authors in seeking to improve the weakness factors that have been discovered among years about the protocol and its implementations.

To enter to see the SSL/TLS orientation, its last versions and the challenges that it must face to the future according what provides classic cryptography and the arrival of quantum, there is a fact that it must be examined with the objective to know if this is able to keep protecting the information with the same or better efficiency that it has been done until now. Or, if it is planned to include improvements that keep it situating as one of the best solutions talking about information and safe communications it refers.

II. BRIEF DESCRIPTION AND TLS FUNCTIONING

When we refer to SSL and TLS protocols, in fact we are talking about at the same method of information protection. TLS is known as the upgraded version of SSL, as it is shown in [1], in addition [2] the protocol is detailed in its way to provide cryptography security methods in the transportation layer through certifications and key interchanging specially in costumer-server architecture and additional features that allow to establish a secure communication like mutual authentication, confidentiality and integrity, trading setting protected by security, key production and key interchanging between two entities also related in [3] and [4], making it as an standard and taking it to be the most implemented protocol to the network traffic assurance, as in HTTPS, SMTP, SFTP, LDAP, which they use TLS to ensure the traffic up to application level [5] .

Getting more in context to the network security, there are many solutions with similarities in their services, but they differ from their application method and layer work of model OSI, we can see ways of web protection using IP security, others more general it is in the top layer of TCP, but the most outstanding example is the Secure Sockets Layer (SSL) and the standard of TLS internet [6].

The SSL/TLS protocol presents an architecture that is capable to protect the information due to 5 sub-protocols, in [7] the authors establish them as the *Record Protocol*, 3 *Handshake* protocols, the heart of TLS, and the *Application Data Protocol.* At the moment to establish connection through TLS before any type of information is transmitted, this one begins with the *Handshake,* which proceeds over the session layer to establish the cryptographic parameters and the session key to be used in the encryption over the presentation layer [8] [9], and this being responsible of trading and setting secure connection.

Once the *Handshake* process is finished, the session turns to data transfer. Here, the globalization protocol starts doing a massive encryption using the key generated by the *Handshake,* ensuring the channel and in addition, to initiate the information interchanging in a secure way [10], it is important to highlight that the massive encryption process or information protection is made by protocols of passwords interchanging, the same way is used by secure solutions as SSH, IPsec and QUIC protocols, as it is shown in [11].

III. IMPLEMENTATION AND USES

TLS is a protocol of advanced transportation, once the concepts are understood and its operation it can be seen in a general way the crowd of applications it has had since its first appearing until today. This is implemented in: Electronic commerce, on line bank services, VPNs, Data encryption about VoIP, email, LDAP services and the cloud, making a possible and secure efficient data retention as it is mentioned in [12]

In general, there are execution examples among application protocols like:

- HTTP over TLS is HTTPS, to offer security to the webs especially in electronic commerce transactions. Using public password certificates to verify the identity of both sides.
- SSH uses TLS under it.
- SMTP and NNTP can operate also over TLS in a secure manner, to the secure access to the News service.
- POP3 and IMAP4 over TLS are POP3S and IMAPS

The main difference between these protocols is the use of the safe transportation layer, which is provided by TLS and the assignation of own TCP port numbers: 443 for HTTPS and 563 to NNTP; however, they work exactly the same as the originals (without use of the TLS).

Without leaving apart the rest of TLS uses, it is possible to go further a little bit in OpenVPN, determined as VPN free tool multi-platform based on TLS. OpenVPN uses the extended SSL/TLS protocol to operate the creation of tunnels and cryptographic elements needed to create a VPN (the dame VPN that creates IPsec) as is related in [1].

IPsec is used according [1], to create most of the VPN products actually created. Open code *Chekpoint VPN-1, Cisco PIX and OpenSWAN* are examples of common use VPN solutions which implements this protocol.

In addition, OpenVPN offers communication confidentiality via symmetrical encryption, also allows the use of digital certificates for the interchanging and authentication of asymmetrical passwords, offering integrity in the sent data through the use of Hash functions and Messages Authentications Codes (MAC). However, it is important to take into account that exists VPN based on IPsec.

On the side of APIs there is GNUTLS as complement of free software from the protocols, its purpose is to offer a programming interface for applications capable of allow the secure communication protocol, used over the transportation net layer. Due to three independent parts: TLS protocol part, certificate, and back end cryptography.

Finally, it is noted that JSSE being the extension of Java safe sockets, it uses both protocols, the Transportation Secure Layer (TLS) as well as, the Secure Socket Layer (SSL). They allow safe crypted communications between costumers and servers. Also, it works as infrastructure that abstracts the underlying mechanisms of SSL and TLS. By means of this abstraction that grants to programmers use encrypted secure communications at the same time the security vulnerabilities are minimized.

TLS is the most powerful cryptographic mode from the point of view of security (and, of course, the computational complexity point of view). The comparison with the TLS authentication mode revealed that there was a reduction in 5% of efficiency, ensured in [1].

IV. VULNERABILITIES

In [13] it is believed that the only propose of TLS protection of communication between two final reliable spots, in other words, is both communication partners known each other and trust themselves.

Base on this, along 20 years after the first official implementation of the SSL, nowadays TLS, it has identified a series of vulnerabilities that get to severely affect the provided security levels by these protocols, even when these have had different improvements and upgrades.

Besides, it has identified the most noticed weakness what TLS had, was related to the encrypted and decrypted connections. As the SANS institute said when in [14] described 4 approaches to describe the SSL / TLS connections: 1) to realize a verification in the server itself; 2) the proxy server from the terminals; 3) decryption by the proper IDS, 4) independent tool to encrypt the connection.

To assess concerning the weaknesses of TLS, is necessary to start with the explanation that even when a web site has “https”, it does not really guarantee the web site is reliable; this goes linked to the mode the communication is implemented. Thus, as is indicated in [15] people found that SSL / TLS protocols are not exempted of deficiencies based on PKI weak links, and it has found some targeted attacks to SSL / TLS in internet.

To be clearer, a simple example of this is: If the hand-shake is done with fake certifications, any attacker could have a phishing site capable of forge the contact information without the victim notice it. As they indicate in [16] was a situation in which the mutual authentication (with the costumer authentication using a certification of public password) it changes from the server authentication during a session. What is more, in the implementation can remain security breaches without identify. In fact, there was an opportunity in which it could access to stored data in the server memory allowing an attacker to access to critical data, it was known as the Heart bleed vulnerability in the OpenSSL implementation. This (Heart bleed) attack permits the attacker to steal confidential data besides the use of TLS. It provides any person the power of having access in the system storage that previously was protected by OpenSSL. According to [17], this vulnerability breaks the confidentiality of the secret passwords used to encrypt all the traffic.

One of most significant attacks among history, it has been the time attack based on Lucky 13. This is about a new Padding Oracle Attack alternative at the moment of MAC integrity verification. The most of the implementations of TLS are vulnerable to this. In [18], it is claimed that the Padding Oracle

Attack explodes simple problems (as implementations that send filled error warnings after the encryption) till more advanced attacks that use side channels. It can be assembled by a man standard attack in the (MITM) environment which only obtains encrypted texts also can inject encrypted texts from its own network composition as it is indicated in [19].

Also, there is the “Beast attack”. BEAST is an “exploit browser against SSL / TLS” and it was revealed in September 2011. It is said in [5], this attack takes advantage of the CBC weaknesses to explode the SSL / TLS protocol. It is based on an exploitation JavaScript code that works with a network sniffer to decrypt the cookies that transport the users´ accreditations to access the accounts.

After BEAST, it was known another new technic named as CRIME to jeopardize the integrity of HTTP sessions, they protected by SSL. This means “Compression Ratio Info-leak Made Easy". In [5], claims that is a security attack against secret web cookies, this through connections that use the protocols of (HTTPS) Hypertext Transference Protocol and SPDY (speedy) also uses data compression.

CRIME can be consider a MITM (man-in-the-middle attack) as well, where the attacker get access to independent connections with the victims and transmits messages among them. A MITM violates the security (and the privacy) that the final points try to impose, in this manner is mentioned in [20].

Finally, we cannot let to mention one last vulnerability, the “Bleichenbacher” attack also known as ROBOT. This stands for “*Return of Bleicherbancher´s Oracle Threat”.* Specified as an attack that [5], permits to perform encrypted operations and RSA signature with the private password of a TLS server. This one, with several different signals, uses its own exploration methodology to differentiate between the types of error as waiting periods, connection re-establishments and TLS duplicated alerts.

V. IMPROVEMENT PROTOCOL MECHANISIMS

Taking as reference what is presented previously, TLS is a protocol because of its usability and workability is too appealing for attackers. For this reason among its history it has resulted in detection of failures in operation mode. Different organizations and work teams independently look for the reinforcement and improvement of mechanisms that uses to traffic transport, besides the fast technology development growth hast let the TLS protocol has improvements, as it must be able to be used in any technologic devise that requires the information be sent.

The improvements made in this protocol, look for information integrity and confidentiality be the most important factor for use, as the pass of the years it has been seen how TLS has succeed in different versions of other protocols and itself, we have the SSL 3.0 protocol which in its moment was standard use however due to studies and its high vulnerabilities this starts being replaced till was obsolete, resulting in as priority and standardization the TLS 1.0, illustrating that the implemented improvement in this version was not so meaningful but relevant to not permit these protocols could interoperate.

In this protocol the security of information is an important factor, for this reason the developed and applied improvements are done as the transported information is safer ensuring a complete transference in an efficient manner, it has received important improvements to protect itself from encrypted attacks by blocks, initialization adding vectors, MD5 addition, methods as SHA and AES inter alia.

The relation concept in the TLS protocol lays foundations on the improvements can be made when it requires to establish any type of connection, as it can be seen in [21], association formalizes what protocols sessions pretend to communicate between them. This idea in necessary to identify trivial attacks in which the adversary reveals a member´s session password from a tested session, suggesting it as an improvement to catch the security of protocols with password´s interchange, in the same way the improvements to insecurities detection are mentioned by the authors in [22], they extend the PMD rules “source code analyzers” adding a group of innovative rules, it is about three rules to detect the unsafe selectors SSL / TLS patterns. The general terms are translated in type of improvement of implementation.

The protocol constant investigation causes companies and organizations that offer products and implement previous version migrate and upgrade their systems to be protected before new threats, different researchers and organizations destined to improve and implement new techniques. In this section we will approach some of the improvements that have been applied to the protocol and how these contribute to the transportation advance and communications´ security that are used daily.

One presented improvement but not implemented is mentioned in [23], modification to the SSL / TLS protocol replacing the password agreement, currently is implemented through a public password, with QKD. QKD refers to the attribution term of quantic key, it is not new to mention the evolution of quantic computing and how this will bring benefits to the cryptography and the manner in which the information is transmitted, and the combination of quantic computation and TLS protocol allows unconditionally generated passwords are transported but never unprotected, bringing more security to the currently attacks that are already difficult to make due to the limited processing level the current machines have.

On the other hand, we find the TLS protocol provides security in endings point to point, this means if it wants to implement an authentication between more than two points this could not be applied, its structure does not work with this type of architecture due to it considers a third action from other user can be seen as an attack to the established communication. In [3], it is proposed to elaborate an improved version to establish a TLS session between N entities. To simplify, we describe a solution with N = 3. Set more than 2 points means the passwords´ distribution will be exposed, however one of the options to make a correct application without this one tends to be misinterpreted is the encrypted implementation by cryptographic means as the RSA is, which permits to do a group of encryptions that lead to allotment of two or more points of indirect sessions as it allows multiple sessions and its feasibility and integrity keeps preserving in secure and reliable manner.

As it exposed in [4], the authors highlight to improve the protocol to link TLS through the use of IBDC, Using TLS as a framework in which IBC is integrated. This can avoid the requirement to implement a completely new security library. At the same time, TLS can be used by interchanging successfully the IBC cryptographic settings without changing the TLS code [4]. The IBC corresponds to certificated mechanisms of double identity applied to the target of making improvements over IBC as this is restricted for lack of security. Conducting the improvement of this IBDC implementation requires an adjustment to the TLS protocol, as a result it gets performance advantages and efficiency, as well as the form of effective recovering passwords are generated.

Describe the traffic that TLS transports is one of the most sensitive points its implementation has, this one cannot be detected in a simple way, because is too different, in [24], the authors suggest a new method to generate service signatures automatically starting from SSL / TLS loading useful data and classify the network traffic according to its application services.

The performance and viability of the suggested method to get an experimental result that classify the 95% approximately from SSL / TLS traffic with the 90% approx. of precision to each SSL / TLS service, it is stated in [24]. If one of the TLS protocol´s use advantages is its security however it can complicate the type of information it can transport. To organizations as well as the users, one of the options to be sure that the sent information really belongs to what they want to transmit is the traffic classification, having the knowledge of this implies knowing what applications or processes are the ones making the actions over TLS.

The protocol security is an investigation topic and constant improvement, and as is, an industry standard reveals some interest form other people who want to find vulnerabilities to rake advantage of this information for personal or commercial purposes, as the authors talk about in [5], to protect ourselves from this threats, in the TLS protocol many security improvements can be used, in these ones it is emphasized the use and implementation is strictly personal, as the users always are given by the possibility to choose the tools they consider more suitable, to improve the protocol it is recommended to manage the last software special versions of OpenSSL, NSS untrusted protocols activation and deactivation, or the ones are not required in traffic, the several mechanisms and their types of use of this protocol always are focus of investigation and constantly are upgraded, or they are marked as development tendency that allows many versions as it was TLS 1.2 up to TLS 1.3.

VI. DEVELOPMENT TENDENCIES AND PROTOCOL EVOLUTION

As the TLS protocol is a standard, is mentioned in [5], which is used in an important layer so it cannot be alone, to be sure this one keep being 100% secure, trustable, and solid for whoever use it. Nowadays, with the vision to build new super computers based on new models like quantum, they have made that TLS concepts make improvement and development processes. All the evolution process of the protocol started after its use was becoming in a vulnerability more than an ally. As it is known, the substitution of SSL for TLS and its versions until the 1.3 have been developed based on the current needs the systems present, but starting from the concept of new technologies and environments, people start making proposals to set the lines the development should follow.

In [25], the information of quantum technology could accept completely new modes of information processing based on quantum principles. In fact, there are many useful tasks in the field, as QC Quantum Cryptography, this only involve a few consecutive quantum computational steps. The use of quantum models and its structure allows the transported passwords in the TLS protocol are completely secure and efficient to avoid that any intruder person can access to data and use this information to their own benefit. Its application goes further than this, as it is about to understand that security among costumers and servers will have such integrity that the needs in a security level will be mitigated, as more studies and investigations are conducted. This approach has allowed to avoid the design of a completely new protocol, as it can have the expected security failures. In fact, this integration has efficiently facilitated SSL as well as QC obtain mutual benefits. On one side, SSL can get new secret passwords from QKD. On the other side, the public conventional discussions required of QC can be transmitted by SSL encapsulation, as the authors expose in [25].

One of the most wanted element is the signals identification, noises received by the communication channels, blind identification using n-samples excessively, where is included the noises to the received signals of the exposed channel in [26]. This will permit by the use of TLS protocol it can be able to perform and identify the transmitted traffic application, inasmuch as do this in a linear manner or with the actual used tools it can be exhausting as requires a too high computational level. In the future, we plan to do an ID-IP frame policy to use the storage in an effective way, also increase the speed of system identification. It can be deleted the expired ID session and the group of the IP server, which is mentioned in en [24]. This lead us in a different processes to identify the traffic over this protocol can be faster and more efficient but at the same time allow tis security increases.

As is presented in [27], a difference motivated by the 0-RTT mode in TLS 1.3, is the introduction of the called semi-static passwords. These passwords are a bit between transitory and static passwords, which they start to establish the mode the produced passwords should be compounded leading out to its future implementations and applicability, some others prefer to base on the OPTLS design as is in the case of authors in [28], which ones are centered in the OPTLS design and its applicability to the cryptographic core of TLS 1.3. The analysis presented here, includes in a basic security model, these ones managing always the criteria to improve and permit the evolution of this would be more efficient and secure.

In [29], is mentioned that, TLS 1.3 is about in a Diffie-Hellman hand shake that generally uses an elliptic curve, followed by the application data encryption using an AEAD framework like AES-GCM. The 1-RTT essential structure has held stable since the first drafts of TLS 1.3. Where the conception of the best and secure methods always have been the priority, each version brings its own substantial improvements, but these ones are represented in some documents which are the bases to the protocol generation and implementation. In TLS its initial and planned documentation, continues and improves as new mechanisms are accepted that allows reinforcement and incident mitigation, and they can be presented at the moment the information travels along the transport layer.

To [30], as the last modifications are made to the TLS 1.3 specifications, the model will upgrade more and the analysis will execute again. This will make sure new errors do not be introduced, regarding the current properties, and it will substantially simplify the analysis of new properties. Currently, is the most upgraded standard protocol, but it does not mean this one is based to avoid all vulnerabilities can exist, because of this as the time goes by and the organizations tend to conduct the TLS 1.2 and TLS 1.3 upgrade, it will generate new improvements that allow properties and risks get adjusted.

VII. CONCLUSION

Analysing the SSL protocol from its beginnings and later call TLS due to the improvements and new functionalities, is important to highlight the given contributions to each security solutions displayed on internet, and they have been constantly applied to offer point to point, costumer – server protection. Their different communication processes and key interchanging in each state or each communication link task, before it passes any type of information between sender and receiver, it offers reliability for data protection in light of reading and modification (Integrity) and only will be read by its receivers (Confidentiality), thus, it continues working for its constant improvement.

Yet, when its security is high level one, among time its first implementation, it has had different attacks which have gotten to infringe TLS as well as its predecessor SSL. Nevertheless, even we talk about vulnerabilities, are these the ones that have allowed to focus on this matter, to intensify high security levels.

The improvement and trend showed in this paper, is only a fraction on how this protocol can be so important in its study field, allowing we can search, establish, and propose different solutions with the intention to enhance the protocol, it was demonstrated, and that is a fundamental base to the constant communicating traffic and its potential vulnerabilities where the majority of the devices could be replaced.

Finally, the application and use of the TLS protocol is too big, as this is a standard of the industry and make the device suppliers use a transportation layer making them to implement the last proposed techniques. Thus, it makes the organization migrate or upgrade their technological tools, the security becomes in the most important feature due to the costumer and server interaction, applying in examples like business and e-trading.

REFERENCES

[1] I. Kotuliak, P. Rybár y P. Trúchly, *«Performance comparison of IPsec and TLS based VPN technologies,»* de 2011 9th International Conference on Emerging eLearning Technologies and Applications (ICETA), Stara Lesna, 2011.

[2] A. A. a. S. T. P. Sirohi, *«A comprehensive study on security attacks on SSL/TLS protocol,»* de 2016 2nd International Conference on Next Generation Computing Technologies (NGCT), Dehradun, India, 2016.

[3] B. M, *«Securing Communications between Multiple Entities Using a Single TLS Session,»* de 2011 4th IFIP International Conference on New Technologies, Mobility and Security, Paris, Francia, 2011.

[4] B. F. a. Z. B. Y. Dai-Rong, *«Improving TLS Protocol Using Identity-Based Double-certificate Mechanism,»* de 2012 International Conference on Industrial Control and Electronics Engineering, Xi'an, China, 2012.

[5] V. R. a. R. O. O. Ivanov, *«Comparison of Modern Network Attacks on TLS Protocol,»* de 2018 International Scientific-Practical Conference Problems of Infocommunications. Science and Technology, Kharkiv, Ucrania, 2018.

[6] A. Thiruneelakandan y T. Thirumurugan, *«An approach towards improved cyber security by hardware acceleration of OpenSSL cryptographic functions,»* de 2011 International Conference on Electronics, Communication and Computing Technologies, Pauls Nagar, India , 2011.

[7] R. D y W. L, *«A hybrid method for service identification of SSL/TLS encrypted traffic,»* de 2016 2nd IEEE International Conference on Computer and Communications (ICCC), Chengdu, China, 2016.

[8] V. K. a. M. H. A. K. Ranjan, *«Security analysis of TLS authentication,»* de 2014 International Conference on Contemporary Computing and Informatics (IC3I), Mysore, India, 2014.

[9] H. Choi y H. Lee, *«Extraction of TLS master secret key in windows,»* de 2016 International Conference on Information and Communication Technology Convergence (ICTC), Jeju, South Korea, 2016.

[10] M. B. H. Y. a. M. A. R. Mzid, *«Adapting TLS handshake protocol for heterogenous IP-based WSN using identity based cryptography,»* de 2010 International Conference on Wireless and Ubiquitous Systems, Sousse, Tunisia, 2010.

[11] M. Fischlin y F. Günther, *«Replay Attacks on Zero Round-Trip Time: The Case of the TLS 1.3 Handshake Candidates,»* de 2017 IEEE European Symposium on Security and Privacy (EuroS&P), Paris, France, 2017.

[12] I. A. Sukhodolskiy y S. V. Zapechnikov, *«An access control model for cloud storage using attribute-based*

encryption,» de 2017 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus), St. Petersburg, Russia, 2017.

[13] P. Kieseberg, P. Frühwirt, S. Schrittwieser y E. Weippl,*«Security tests for mobile applications — Why using TLS/SSL is not enough,»* de IEEE Eighth International Conference on Software Testing, Verification and Validation Workshops (ICSTW), Graz, Austria, 2015.

[14] T. Radivilova, L. Kirichenko, D. Ageyev, M. Tawalbeh y V. Bulakh, *«Decrypting SSL/TLS traffic for hidden threats detection,»* de IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT), Kiev, Ukraine, 2018.

[15] W. Liu, P. Ren, Y. Zhang y H.-x. Duan, *«SSL-DP: A Rootkit of Network Based SSL and TLS Traffic Decryptor,»* de Second Cybercrime and Trustworthy Computing Workshop, Ballarat, VIC, Australia, 2010.

[16] Y. Suga, *«Countermeasures and Tactics for Transitioning against the SSL/TLS Renegotiation Vulnerability,»* de Sixth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, Palermo, Italy, 2012.

[17] L. Alqaydi, C. Y. Yeun y E. Damiani, *«Security enhancements to TLS for improved national control,»* de 2017 12th International Conference for Internet Technology and Secured Transactions (ICITST), Cambridge, UK, 2017.

[18] A. Delignat-Lavaud, C. Fournet, M. Kohlweiss, J. Protzenko, A. Rastogi, N. Swamy, S. Zanella-Beguelin,K. Bhargavan, J. Pan y J. K. Zinzindohoue, *«Implementing and Proving the TLS 1.3 Record Layer,»* de 2017 IEEE Symposium on Security and Privacy (SP), San Jose, CA, USA , 2017.

[19] J. Wang, Y. Yang, L. Chen, G. Yang, Z. Chen y L. Wen, *«A Combination of Timing Attack and Statistical Method to Reduce Computational Complexities of SSL/TLS Side-Channel Attack,»* de 2015 11th International Conference on Computational Intelligence and Security (CIS), Shenzhen, China , 2015.

[20] V. A. Cunha, M. B. d. Carvalho, D. Corujo, J. P. Barraca, D. Gomes, A. E. Schaeffer-Filho, C. R. P. d. Santos, L. Z. Granville y R. L. Aguiar, *«An SFC-enabled approach for processing SSL/TLS encrypted traffic in Future Enterprise Networks,»* de 2018 IEEE Symposium on Computers and Communications (ISCC), Natal, Brazil , 2018.

[21] M. Fischlin, F. Günther, B. Schmidt y B. Warinschi, *«Key Confirmation in Key Exchange: A Formal Treatment and Implications for TLS 1.3,»* de 2016 IEEE Symposium on Security and Privacy (SP), San Jose, CA, USA , 2016.

[22] M. Alhanahnah y Q. Yan, *«Towards best secure coding practice for implementing SSL/TLS,»* de IEEE INFOCOM 2018 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Honolulu, HI, USA, 2018.

[23] M. Pivk, C. Kollmitzer y S. Rass, *«SSL/TLS with Quantum Cryptography,»* de 2009 Third International Conference on Quantum, Nano and Micro Technologies, Cancun, Mexico , 2009.

[24] K. U. K. Sung-Min KimDept. of Computer and Information Science, Y.-H. Goo, M.-S. Kim, S.-G. Choi y M.-J. Choi, *«A method for service identification of SSL/TLS encrypted traffic with the relation of session ID and Server IP,»* de 2015 17th Asia-Pacific Network Operations and Management Symposium (APNOMS), Busan, South Korea , 2015.

[25] S. T. Faraj, *«A novel extension of SSL/TLS based on quantum key distribution,»* de 2008 International Conference on Computer and Communication Engineering, Kuala Lumpur, Malaysia , 2008.

[26] M. Komatsu, T. Odake, H. Matsumoto y T. Furukawa, *«A proposal of blind channel identification based on TLS using over-sampling method for the received signals including noises,»* de 2012 International Symposium on Intelligent Signal Processing and Communications Systems, Taipei, Taiwan, 2012.

[27] X. Li, J. Xu, Z. Zhang, D. Feng y H. Hu, *«Multiple Handshakes Security of TLS 1.3 Candidates,»* de 2016 IEEE Symposium on Security and Privacy (SP), San Jose, CA, USA, 2016.

[28] H. Krawczyk y H. Wee, *«The OPTLS Protocol and TLS 1.3,»* de 2016 IEEE European Symposium on Security and Privacy (EuroS&P), Saarbrucken, Germany , 2016.

[29] K. Bhargavan, B. Blanchet y N. Kobeissi, *«Verified Models and Reference Implementations for the TLS 1.3 Standard Candidate,»* de 2017 IEEE Symposium on Security and Privacy (SP), San Jose, CA, USA , 2017.

[30] C. Cremers, M. Horvat, S. Scott y T. v. d. Merwe, *«Automated Analysis and Verification of TLS 1.3: 0-RTT, Resumption and Delayed Authentication,»* de 2016 IEEE Symposium on Security and Privacy (SP), San Jose, CA, USA , 2016.