A research for encryption based TLS security

Md Amanullah
Student
Universal Group of Institute,

Prabhjot Kaur
Teacher,
Universal Group of Institute.

***Abstract*- Current research explain the Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols, how they can be applied to a web application, and the requirements necessary to create a secure link between a server and a client machine. In addition, a development history of the protocols will be given, and a brief discussion of the impact that secure communications protocols have had on the electronic commerce arena. This paper particularly serves as a resource to those who are new to the information assurance field, and provides an insight to two common protocols used in Internet security. Though SSL and TLS are not the only secure protocols currently in use, they are very common for sites dealing with transactions that could involve sensitive data However, Transport Layer Security (TLS) is a standard encryption protocol in the Internet in which all the functionalities are assumed to be at endpoints by making it absurd to use services in-network that can enhance network resource usage, improvement in user expertise and assures clients and servers from security risks. The focus is to improve security of transport layer by overcoming the drawbacks.**

***Keywords*— TLS(Transport Layer Security), SSL(Secure Socket Layer), DHE(Deffie Hellman Key Exchange), RSA(Rivest Shamir Adleman), WSN(Wireless Sensor Networks)**

I. INTRODUCTION

URING the past decades, wireless communications infrastructure and services have been proliferating with the goal of meeting rapidly increasing demands [1], [2]. According to the latest statistics released by the International Telecommunications Union in 2013 [3], the number of mobile subscribers has reached 6.8 billion worldwide and almost 40% of the world's population is now using the Internet. Meanwhile, it has been reported in [4] that an increasing number of wireless devices are abused for illicit cyber-criminal activities, including malicious attacks, computer hacking, data forging, financial information theft, online bullying/stalking and so on. This causes the direct loss of about 83 billion Euros with an estimated 556 million users worldwide impacted by cyber-crime each year, according to the 2012 Norton cybercrime report [4]. Hence, it is of paramount importance to improve wireless communications security to fight against cyber-criminal activities, especially because more and more people are using wireless networks (e.g., cellular networks and Wi-Fi) for online banking and personal emails, owing to the widespread use of smartphones. Wireless networks generally adopt the open systems interconnection (OSI) protocol architecture [5] comprising the application layer, transport layer, network layer [6], medium access control (MAC) layer [7] and physical layer [8], [9]. Security threats and vulnerabilities associated with these protocol layers are typically protected separately at each layer to meet the security requirements, including the authenticity, confidentiality, integrity and availability [10]. For example, cryptography is widely used for protecting the confidentiality of data transmission by preventing information disclosure to unauthorized users [11], [12]. Although cryptography improves the achievable communications confidentiality, it requires additional computational power and imposes latency [13], since a certain amount of time is required for both data encryption and decryption [14]. In order to guarantee the authenticity of a caller or receiver, existing wireless networks typically employ multiple authentication approaches simultaneously at different protocol layers, including MAC layer authentication [15], network-layer authentication [16], [17] and transport-layer authentication [18]. To be specific, in the MAC layer, the MAC address of a user should be authenticated to prevent unauthorized access. In the network layer, the Wi-Fi protected access (WPA) and the Wi-Fi protected access II (WPA2) are two commonly used network layer authentication protocols [19], [20]. Additionally, the transport-layer authentication includes the secure socket layer (SSL) and its successor, namely the transport layer security (TLS) protocols [11]. It becomes obvious that exploiting multiple authentication mechanisms at different protocol layers is capable of enhancing the wireless security, again, at the cost of high computational complexity and latency. In wired networks, the communicating nodes are physically connected through cables. By contrast, wireless networks are extremely vulnerable owing to the broadcast nature of the wireless medium. Explicitly, wireless networks are prone to malicious attacks, including eavesdropping attack [14], denialof-service (DoS) attack [15], spoofing attack [16], man-inthe-middle (MITM) attack [17], message falsification/injection attack [18], etc. For example, an unauthorized node in a wireless network is capable of inflicting intentional interferences with the objective of disrupting data communications between legitimate users. Furthermore, wireless communications sessions may be readily overheard by an eavesdropper, as long as the eavesdropper is within the transmit coverage area of the transmitting node. In order to maintain confidential transmission, existing systems typically employ cryptographic techniques for preventing eavesdroppers from intercepting data transmissions between legitimate users [19], [20]. Cryptographic techniques assume that the eavesdropper has limited computing power and rely upon the computational hardness of their underlying mathematical problems. The security of a cryptographic approach would be compromised, if an efficient method of solving its underlying hard mathematical problem was to be discovered.

II. TRANSPORT LAYER SECURITY

Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL), both of which are frequently referred to as 'SSL', are cryptographic protocols that provide communications security over a computer network.[5] Several versions of the protocols are in widespread use in applications such as web browsing, email, Internet faxing, instant messaging, and voice-over-IP (VoIP). Major web sites use TLS to secure all communications between their servers and web browsers. The primary goal of the TLS protocol is to provide privacy and data integrity between two communicating computer applications.[1]:3 When secured by TLS, connections between a client (e.g., a web browser) and a server (e.g., wikipedia.org) have one or more of the following properties: The connection is private because symmetric cryptography is used to encrypt the data transmitted. The keys for this symmetric encryption are generated uniquely for each connection and are based on a shared secret negotiated at the start of the session. The server and client negotiate the details of which encryption algorithm and cryptographic keys to use before the first byte of data is transmitted. The negotiation of a shared secret is both secure (the negotiated secret is unavailable to eavesdroppers and cannot be obtained, even by an attacker who places himself in the middle of the connection) and reliable (no attacker can modify the communications during the negotiation without being detected).

The identity of the communicating parties can be authenticated using public-key cryptography. This authentication can be made optional, but is generally required for at least one of the parties (typically the server).

The connection is reliable because each message transmitted includes a message integrity check using a message authentication code to prevent undetected loss or alteration of the data during transmission.[3] In addition to the properties above, careful configuration of TLS can provide additional privacy-related properties such as forward secrecy, ensuring that any future disclosure of encryption keys cannot be used to decrypt any TLS communications recorded in the past.[2] TLS supports many different methods for exchanging keys, encrypting data, and authenticating message integrity (see Algorithm). As a result, secure configuration of TLS involves many configurable parameters, and not all choices provide all of the privacy-related properties described in the list above. Attempts have been made to subvert aspects of the communications security that TLS seeks to provide and the protocol has been revised several times to address these security threats (see Security). Web browsers have also been revised by their developers to defend against potential security weaknesses after these were discovered. The TLS protocol is composed of two layers: the TLS record protocol and the TLS handshake protocol.

Client-server applications use the TLS protocol to communicate across a network in a way designed to prevent eavesdropping and tampering. Since protocols can operate either with or without TLS (or SSL), it is necessary for the client to indicate to the server the setup of a TLS connection. There are two main ways of achieving this. One option is to use a different port number for TLS connections (for example, port 443 for HTTPS). The other is for the client to use a protocol-specific mechanism (for example, STARTTLS for mail and news protocols) to request that the server switch the connection to TLS. Once the client and server have agreed to use TLS, they negotiate a stateful connection by using a handshaking procedure.[4] During this handshake, the client and server agree on various parameters used to establish the connection's security:

The handshake begins when a client connects to a TLS-enabled server requesting a secure connection and presents a list of supported cipher suites (ciphers and hash functions).

From this list, the server picks a cipher and hash function that it also supports and notifies the client of the decision.

The server usually then sends back its identification in the form of a digital certificate. The certificate contains the server name, the trusted certificate authority (CA) and the server's public encryption key.

The client confirms the validity of the certificate before proceeding.

To generate the session keys used for the secure connection, the client either:

encrypts a random number with the server's public key and sends the result to the server (which only the server should be able to decrypt with its private key); both parties then use the random number to generate a unique session key for subsequent encryption and decryption of data during the session

uses Diffie-Hellman key exchange to securely generate a random and unique session key for encryption and decryption that has the additional property of forward secrecy: if the server's private key is disclosed in future, it cannot be used to decrypt the current session, even if the session is intercepted and recorded by a third party.

This concludes the handshake and begins the secured connection, which is encrypted and decrypted with the session key until the connection closes. If any one of the above steps fail, the TLS handshake fails, and the connection is not created.

III. Basic Network Security Requirement

Again, in wireless networks, the information is exchanged among authorized users, but this process is vulnerable to various malicious threats owing to the broadcast nature of the wireless medium. The security requirements of wireless networks are specified for the sake of protecting the wireless transmissions against wireless attacks, such as eavesdropping attack, DoS attack, data falsification attack, node compromise attack and so on [14], [15]. For example, maintaining data confidentiality is a typical security requirement, which refers to the capability of restricting data access to authorized users only, while preventing eavesdroppers from intercepting the information. Generally speaking, secure wireless communications should satisfy the requirements of authenticity, confidentiality, integrity and availability [16], as detailed below. Security is described through some basic security properties that are: Data compression [3], confidentiality, integrity, availability, authentication and accountability (non-repudiation) [6]. All security risks, problems and attacks can be classified under these properties.

Authenticity: Authenticity refers to confirming the true identity of a network node to distinguish authorized users from unauthorized users. In wireless networks, a pair of communicating nodes should first perform mutual authentication before establishing a communications link for data transmission

Data Compression: It is the process used to decrease the size of data. Data size can be decreased by removing redundancy, deleting irrelevant data and discarding duplicate data packets. CS technology is used for compressing the data that ensures the data compression in WSNs.[3]

Confidentiality: It is a technique of protecting the data from all the users that are unauthorized. The non intended uses are generally called unauthorized users. In confidentiality the data is protected from passive attacks. We can ensure confidentiality using cryptography encryption so that during transfer one can see it but not know it.[1]

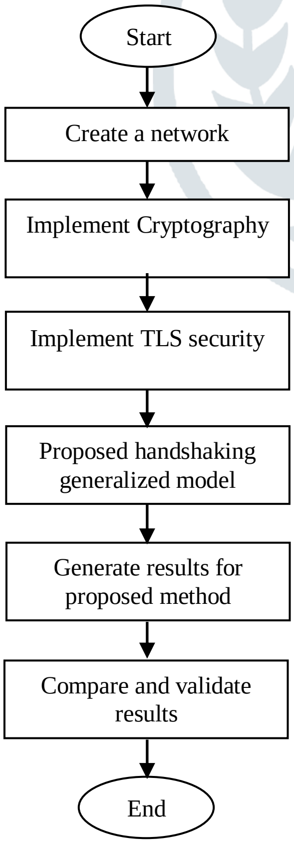
Integrity: Integrity means the information received is same as the information sent by the authorized entity that means data is not altered. It is an active attack. The user altering con not be stopped but it can be detected very easily. Once it is detected user can decide whether to accept data packet or not. We can calculate hash based time at sender side before sending packet and at receiver side on received message and then test both hash, if both are same than no stop but if hash is not same then stop the communication.[1]

Availability: Availability ensures the data is available when it is needed to authorized users. It is the property of protecting information from non-authorized temporary or permanent with holding of information. Availability concern is at almost all layers of OSI. Now a day availability threats are increasing very fast. But it can be protected by selection appropriate security solutions like firewall, intrusion detection system etc.[1]

Accountability: It is the record of the actions done by the users. Accountability concern with keeping record and audit checking about non-repudiation, isolate fault, IDP, recovery and legal action. As we know security never 100% achievable we have to trace possible breaches. It is very essential for forensic evident and analysis also.[1]

IV. Proposed Work

Two main security challenges in secure data aggregation are confidentiality and integrity of data. While traditionally encryption is used to provide end to end confidentiality in Wireless Sensor Network (WSN), the aggregators in a secure data aggregation scenario need to decrypt the encrypted data to perform aggregation. This exposes the plaintext at the aggregators, making the data vulnerable to attacks from an adversary. Similarly an aggregator can inject false data into the aggregate and make the base station accept false data. Thus, while data aggregation improves energy efficiency of a network, it complicates the existing security challenges The process of grouping the sensor nodes in a densely deployed large-scale sensor network is known as clustering. The intelligent way to combine and compress the data belonging to a single cluster is known as data aggregation in cluster based environment. There are some issues involved with the process of clustering in a wireless sensor network.



Flow Chart

V. Results and Discussion

During preliminary study, it has been studied that for creating any network some assumptions are taken into account. There are a number of parameters that are to be assumed before the simulation like Frame Duration, frequency Bandwidth, Mode of transmission, network size etc. The area taken into consideration is 100*100m and the simulation time to be considered is 300sec.

Simulation Parameter	**Value**
Frame duration	1.0 millisecond
Frequency Bandwidth	25MHZ
Mode of transmission	TDD
Number of mobile station	20
Packet size	5kb
Simulation grid size	100 m X 100 m
Simulation time	3000 Rounds

Table 1: Simulation parameters

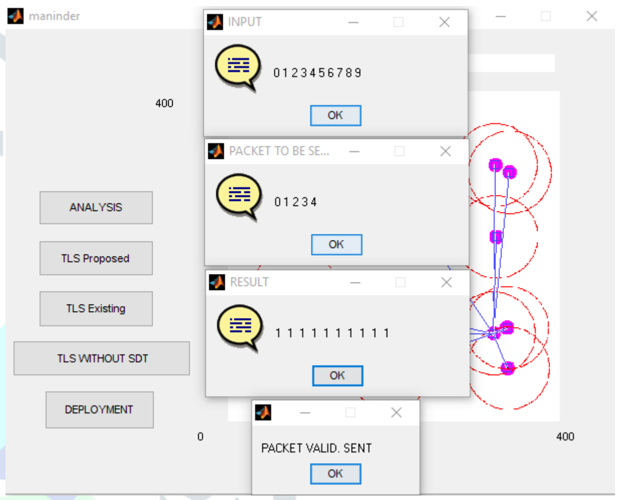


Fig 1: Packet Reception

Above figure is presenting about the results of the packet reception at the destination end after embedding the encryption schemes. From the fig it is cleared that all the packets are received at the destination without any loss. This figure is giving the summary results of all the steps that are performed above.

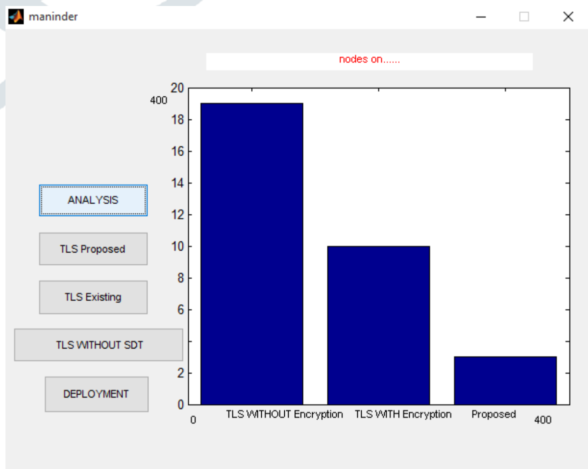


Fig 2: Graph for overheads in TLS Encryption

Figure 2 is defining about the encryption overheads in Transport Layer Security. This is quite clear in this figure that even by introducing a generalized model of encryption in Transport Layer Security the proposed model is showing least encryption overheads.

VI. CONCLUSION & FUTURE WORK

Current implementation is a verified reference implementation of TLS 1.2. It fully supports its wire formats, ciphersuites, sessions and connections, re-handshakes and resumptions, alerts and errors, and data fragmentation, as prescribed in the RFCs; it interoperates with mainstream web browsers and servers. In the current research the proposal is competent with all kind of networks and APIs. It is a generalized structure which can be applied in any network which was not possible in existing research. It presents security specifications for its main components, such as authenticated stream encryption for the record layer and key establishment for the handshake and describe their verification using the F7 typechecker. In the future scope, the focus will be on the standard model of cryptography, resulting in rather strong assumptions for the Handshake for the DHE key exchange. Relaxing these assumptions and developing concrete security bounds for our implementation is left as important future work.

VII. REFERENCES

1. William Stallings, "Cryptography And Network Security: Principles and practices", 5th Edition, Pearson Education, pages: 15-25, 2011
2. Karthikeyan Bhargavan, C´edric Fournet, Markulf Kohlweiss, Alfredo Pironti, Pierre-Yves Strub, "Implementing TLS with Verified Cryptographic Security", Security and Privacy (SP) IEEE Symposium on Security and Privacy, ISSN: 1081-6011, pp:445-459, 19-22 May 2013
3. Jin Qi, Xiaoxuan Hu, Yun Ma, Yanfei Sun, "A Hybrid Security and Compressive Sensing-Based Sensor Data Gathering Scheme", IEEE Access, ISSN: 2169-3536, Volume 3, pp: 718-724, 2015
4. M. Cheng, L. Deng, X. Wang, H. Li, M. Tang, C. Ke, P. Shum, D. Liu, "Enhanced Secure Strategy for OFDM-PON System by Using Hyperchaotic System and Fractional Fourier Transformation", IEEE Photonics Journal Secure Strategy for OFDM-PON System, ISSN: 1943-0655, Volume: 6, Issue: 6, pp:2-10, 2014
5. Edoardo Biagioni, "Ubiquitous Interpersonal Communication over Ad-Hoc Networks and the Internet", 47th Hawaii International Conference on System Science, INSPEC Accession Number: 14179222, pp: 5144-5153, 2014
6. Muhamed Elezia, Bujar Raufia, "Conception of Virtual Private Networks using IPsec suite of protocols, comparative analysis of distributed database queries using different IPsec modes of encryption", World Conference on Technology, Innovation and Entrepreneurship, Procedia - Social and Behavioral Sciences, Volume: 195, pp: 1938-1948, 2015
7. Harun Ozkisia, Murat Topaloglu, "The University Students' Knowledge of Internet Applications and Usage Habits", 4th World Conference On Educational Technology Researches, WCETR, Volume: 182, pp: 584-589, 2015
8. Hartini Saripan, Zaiton Hamin, "The application of the digital signature law in securing internet banking: some preliminary evidence from Malaysia", Procedia Computer Science, Volume: 3, pp: 248-253, 2011
9. Sanaz Rahimi Moosavi, Tuan Nguyen Gia, Amir-Mohammad Rahmani, Ethiopia Nigussie, Seppo Virtanen, Jouni Isoaho, Hannu Tenhunen, "SEA: A Secure and Efficient Authentication and Authorization Architecture for IoT-Based Healthcare Using Smart Gateways", 6th International Conference on Ambient Systems, Networks and Technologies, Volume: 52, pp: 452-259, 2015
10. Manar Jaradat, Moath Jarrah, Abdelkader Bousselham, Yaser Jararweh, Mahmoud Al-Ayyou, "The Internet of Energy: Smart Sensor Networks and Big Data Management for Smart Grid", The International Workshop on Networking Algorithms and Technologies for IoT, Volume: 56, pp: 592-597, 2015
11. Overview of SSL/TLS encryption, https://technetmicrosoft.com/en-us/library/cc781476%28v=ws.10%29.aspx
12. Neeraj Kumar, Manoj Kumar, and R. B. Patel, "A Secure and Energy Efficient Data Dissemination Protocol for Wireless Sensor Networks", International Journal of Network Security, Vol.15, No.6, pp.490-500, Nov 2010.
13. N. Akilandeswari, B. Santhi and B. Baranidharan, "A Survey on Energy Conservation Techniques in Wireless Sensor Networks", ARPN Journal of Engineering and Applied Sciences, Vol. 8, No. 4, April 2013.
14. Eugene Shih, Seonghwan Cho, Nathan Ickes, Rex Min, Amit Sinha, Alice Wang, Anantha Chandrakasan, "Physical Layer Driven Protocol and Algorithm Design for Energy Efficient Wireless Sensor Networks" AMC SIGMOBILE7/01 Rome,Italy,2001 ACMISBN 1-58113-422-3/01/0.
15. Shashidhar Rao Gandham, Milind Dawande, Ravi Prakash, S. Venkatesan, "Energy Efficient Schemes for Wireless Sensor Networks with Multiple Mobile Base Stations.",GLOBECOM'03.IEEE 1,pp:377-381, Nov 2010.
16. Mark Adam Perillo, "Role Assignment in Wireless Sensor Networks: Energy-Efficient Strategies and Algorithms", National Science Foundation(NSF)-(CNS-0448046),Vol 3,Issue 5,May 2013.
17. Mohit Saini, Rakesh Kumar Saini, "Solution of Energy-Efficiency of sensor nodes in Wireless sensor Networks ", International Journal of Advanced Research in Computer Science and Software Engineering, Vol 3, Issue 5, pp. 353-357, May 2013.
18. Wei Ye, John Heidemann, Deborah Estrin, "An Energy-Efficient MAC Protocol Wireless Sensor Networks" INFOCOM 2002,Twenty First Annual Joint Conference of the IEEE Computers and Communication Societies. Proceeding IEEE,Vol:3,2002,pp:1567-1576 May 2014.
19. Stefanos A. Nikolidakis, Dionisis Kandris, Dimitrios D. Vergados, Christos Douligeris, "Energy Efficient Routing in Wireless Sensor Networks Through Balanced Custering" International Journal of Scientific and Research Publications, Vol 6, Issue: 1, April 2013.
20. Gyanendra Prasad Joshi, Seung Yeob Nam and Sung Won Kim, "Cognitive Radio Wireless Sensor Networks: Applications, Challenges and Research Trends." Sensors ,Vol 13, Issue:9,2013.
21. Xun Li, Geoff V Merrett, Neil M White, "Energy-efficient Data Acquisition for Accurate Signal Estimation in Wireless Sensor Networks", Journal on wireless Communications and Networking ,Vol 8, Issue:4, June 2010.
22. Karim Seada, Marco Zuniga, Ahmed Helmy, Bhaskar Krishnamachari, "Energy Efficient

Forwarding Strategies for Geographic Routing in Lossy Wireless Sensor Networks", International Journal of Network Security, Vol 5,Issue:3 ,July 2009.

23. Neeraj Kumar Mishra, Vikram Jain, Sandeep Sahu, "Survey on Recent Clustering Algorithms in Wireless Sensor Networks ", International Journal of Scientific and Research Publications, Vol 3, Issue 4, April 2013.
24. Prakashgoud Patil, Umakant P Kulkarni, "Energy Efficient Aggregation With Divergent Sink Placement For Wireless Sensor Networks", International Journal of Ad hoc, Sensor & Ubiquitous Computing (IJASUC) Vol.4, No.2, April 2013.
25. Sanjay Eknath Gawali, Prof. D. S.Mantri, "Lifetime Energy Efficient Optimization for WSN", International Journal of Network Security,Vol.16,No.6,pp.490-500,Oct 2012.
26. Neeraj Kumar, Manoj Kumar, R. B. Patel, "A Secure and Energy Efficient Data Dissemination Protocol for Wireless Sensor Networks", International Journal of Network Security, Vol.15, No.6, pp.490-500, Nov 2012.
27. N. Akilandeswari, B. Santhi and B. Baranidharan, "A Survey On Energy Conservation Techniques In Wireless Sensor Networks", ARPN Journal of Engineering and Applied Sciences, Vol. 8, No. 4, April 2013.
28. Mohit Saini, Rakesh Kumar Saini, "Solution of Energy-Efficiency of Sensor Nodes in Wireless sensor Networks", International Journal of Advanced Research in Computer Science and Software Engineering, Vol 3, Issue 5, May 2013.
29. Xun Li, Geoff V Merrett, Neil M White, "Energy-efficient data acquisition for accurate signal estimation in wireless sensor networks", Journal on Wireless Communications and Networking, Vol: 2, Issue: 6, July 2011.