A Survey for Cryptography Based TLS Security

Maninder Kaur¹ & Er. Sheenam Malhotra²
Department of Computer Science and Engineering
Sri Guru Granth Sahib World University, Fatehgarh Sahib-140406

Abstract—In today’s era of technology every software depends on networks, it may be local, Internet, Intranet, extranet, wired or wireless. Every network needs security at high level to ensure confidentiality and integrity for sharing information. The issues of network security particularly at Transport layer, that allow end to end sharing of information among users is discussed here in the paper. Everything should be secure on internet, as security is needed for privacy in communication and big projects in business and industries. But security is not always 100%, security risks and vulnerability is increasing and becoming serious issue for business. In transport layer the security is mainly related with authentication, confidentiality, integrity and availability. 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 (Diffie Hellman Key Exchange), RSA (Rivest Shamir Adleman), WSN (Wireless Sensor Networks)

1. INTRODUCTION

Internet security is a main part of computer science which is specially related with internet, it also involves browser security and network security. Internet security can also be applied to the applications that work with the internet.[2] The channel represented by the internet is not secure for communication as it leads to a high risk of information leakage such as phishing. There are many different methods that are being used to protect the transfer of data for example encryption. The security protocols and cryptographic methods may be used to secure TCP/IP protocols. The TCP/IP protocols include secure socket layer (SSL), followed by TLS, and for email there is PGP (Pretty Good Privacy) and IPSec is for network layer security. IPSec is basically designed for securing TCP/IP communication. It uses encryption to transform data for providing security and authentication. The bases of IPSec are formed by two basic transformations that are:

- Authentication Header (AH)
- Encapsulating Security Payload (ESP)

Data integrity, data originality, authentication and anti replay services are provided by these two protocols. To provide preferred set of security services of IP layer these protocols can be used alone or by combining the two. [6]

To increase the working of encryption, a hybrid security and compressive sensing (CS) based data collection scheme is presented.[3] TLS is a collection of dynamically configured protocols, controlled by internal state machine which uses a large number of cryptographic algorithms. It provides bigger flexibility for connecting clients and servers, basically at cost of security, so TLS applications should properly configured and review their changed connections before further proceeding. TLS is widely used for securing web traffic (HTTPS) and VPNs, mails and wireless communication. Some attacks target the protocol logic, for instance causing the client and server to negotiate the use of weak algorithms even though they both support strong cryptography. Some exploit cryptographic design flaws, for instance using knowledge to set up adaptive plaintext attacks. Some, such as padding-oracle attacks, use a combination of protocol logic and cryptography, taking advantage of error messages to gain information on encrypted data. Many algorithms, like MD5, DES, or PKCS#1, are ultimately busted or subsumed by others, so TLS features cryptographic quickness, enabling users to decide at runtime between different methods and algorithms for related purposes. Ciphersuites and extensions are its main quickness mechanisms; together with the protocol version, they control the method and algorithms for the key exchange and the transport layer.[2]

Many techniques that secure the passive optical nerves (PON) are recently discovered. It has been confirmed that high speed secure communication can
be get in wavelength division multiplexing (WDM) PONs by embracing optical chaos.[4]

II. BASIC NETWORK SECURITY REQUIREMENT

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.

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]

Authentication: It is property to verify or check originality of entity for the assurance that it is same as it claims to be. It ensures that user is who they identify themselves and that each inputs arriving at the system comes from a trusted source. Authentication can be ensuring by many techniques like, login-password, biometric, Certificate based, OTP 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]

III. RELATED WORK

Jin Qi et al. [3] 2015 proposed a hybrid security and compressive sensing-based system for multimedia sensor data collection is presented. It decreases the complexity and energy usage as the mechanism is light weighted. The analysis of performance about security and compression is done. The use of cryptographic techniques such as encryption and hashing largely increases the energy consumption of sensors, which aggravates the original critical energy constraint problem of wireless sensor networks (WSNs). To reduce the burden of sensors, compression can be utilized. Since the usual chaos-based schemes are not straightly relevant for WSNs, a hybrid security solution is presented. The hybrid security consists of 8-bit integer chaotic block encryption and a chaos-based message authentication codes. Thus, the security and performance of data gathering is promoted.

M. Cheng et al. [4] 2014 proposed and experimentally express a scheme whereby hyperchaos and fractional Fourier transform (FrFT) techniques are integrated in an orthogonal frequency-division multiplexing (OFDM) passive optical network system. In an experiment, both security issues and transmission performance are investigated under an overall frame, and 7.64-Gb/s 16-quadrature-amplitude-modulation OFDM data with a four-level encryption scheme are successfully transmitted over a 25-km standard single-mode fiber. It is proved that the security of system and transmission performance can be enhanced at the same time.

Edoardo Biagioni [5] 2014 started to influence capability to provide interpersonal communication both over the Internet and over ad-hoc and delay-tolerant networks composed of mobile devices themselves. This network is decentralized in the form that it can function without any infrastructure, but does take advantage of infrastructure connections when available. All interpersonal communication is encrypted and authenticated so packets may be carried by devices belonging to others-untrusted networks. The decentralized model of security builds a flexible trust network on top of the social network of communicating individuals. This social network can be used to prioritize packets to or from individuals closely related by the social network. The priority is given to the network that uses fewer network resources.

Muhamed Elezi et al. [6] 2015 offered a set of simulated secure data communication tunnels together with a comparison of results of the speed variables measured against the security through different encryption protocols between remote LAN’s. The world of Internet is openly used and can have a risk of insecurities. Companies and organizations use huge possibilities to enable communication and data sharing capabilities...
inside their corporate platforms. With this, they continuously provide a fast, efficient and secure working environment by protecting their organizational resources. Enterprises build their network infrastructure with intention to find reliable solutions to protect themselves from untrusted and cybercrime activities. In this sense, Virtual Private Networks (VPN) is primarily concerned about Data privacy. VPNs represent an addition of a private network made through added features like encapsulating the data packets with a header on both ends, along the lines of the communication as well as setting proper suite of protocols available. HarunOzkisi et al. [7] 2015 defined that with the rise of the mobile devices, mainly the students have started to use the internet more aggressively. This study aims to examine the level of the university students’ knowledge of internet and online applications. The internet has become major part of our life in accordance with the information technologies that has been growing rapidly. The limitations concerning time, place, equipment and cost have been eased recently. Therefore, the frequency, purpose and quality of internet use have been greatly improved and the number of internet users has been increased tremendously. HartiniSaripan et al. [8] 2011 highlight a methodological process and a preliminary finding of eight multiple-case studies amongst banks offering Internet banking services in Malaysia. The research, at the onset revealed that in ‘the real life situation’, the digital signature technology is hardly being adopted in securing Internet banking transactions, which has consequently shaped the extent of the application of the digital signature law in Malaysia. Whilst the Digital Signature Act 1997 has always been acknowledged as one of the pioneers of a technology-specific legislative approach, the Act nevertheless, has been greatly exposed to numerous critiques, suggesting its inability to secure online transactions, including Internet banking. Moreover, the lack of any of its provisions being tested in the Malaysian courts has in turn, suggested that the law has an inconsequential application in securing Internet banking transactions. SanazRahimiMoosavi et al. [9] 2015 proposed a secure and efficient authentication and authorization architecture for IoT-based healthcare is developed. Security and privacy of patients’ medical data are crucial for the acceptance and ever-present use of IoT in healthcare. Secure authentication and authorization of a remote healthcare professional is the main focus of this work. Due to resource constraints of medical sensors, it is infeasible to utilize conventional cryptography in IoT-based healthcare. In addition, gateways in existing IoTs focus only on trivial tasks without alleviating the authentication and authorization challenges. In the presented architecture, authentication and authorization of a remote end-user is done by distributed smart e-health gateways to unburden the medical sensors from performing these tasks. The proposed architecture relies on the certificate-based DTLS handshake protocol as it is the main IP security solution for IoT. Here the architecture is providing scalable and reliable end-to-end security for healthcare systems. ManarJaradat et al. [10] 2015 discussed and provides recommendations and practices to be used in the future of smart grid and Internet of things. Smart sensor networks provide wide range of opportunities for smart grid applications that includes power monitoring, demand-side energy management, coordination of distributed storage, and integration of renewable energy generators. Smart sensor networks can be used on a large scale because there cost is low and they have ease-of-development. Processing and analyzing these data reveals deeper insights that can help expert to improve the operation of power grid to achieve better performance. The technology to collect massive amounts of data is available today, but managing the data efficiently and extracting the most useful information out of it remains a challenge.

IV. ENCRYPTION SCHEMES IN TLS

Server-Gated Crypto (SGC): OpenSSL servers have a feature called SGC that allows clients to again start a handshake after getting a ServerHello. Further code inspection reveals that the state created during the first exchange of hello messages is then supposed to be discarded completely. OpenSSL is an open source for implementing cryptographic libraries such as symmetric key, public key and hash algorithms. It is basically used for making and organizing keys and certificates. [9]

- **Symmetric Key:** In this, one key is used for encryption and decryption that is same for both operations. If two persons want to exchange the data they must have the same copy of key. Mostly symmetric key is used for encryption of data because it is faster that asymmetric key. Most common algorithms for symmetric key are RC2, RC4, DES(Data Encryption Standard), 3-DES(Triple DES) and AES(Advanced Encryption Standard). [11]

- **Asymmetric Key:** It is also known as public key. It uses a set of two keys that are derived together through a mathematical process. One key is public and other is private. RSA is most commonly used algorithm.[11]

- **Hash Algorithm:** In this algorithm, original values are mapped into a smaller set of values. A hash is similar to the fingerprints as the fingerprint is similar to the unique person but smaller in size. Hashing is used for establishing data integrity. The most common hash algorithms are SHA-
1. (Standard Hash Algorithm) and MD-5 (Message Digest 5). MD5 gives 128 bit hash value and SHA gives 160 bit value. [11]

V. CONCLUSION & FUTURE WORK

A. CONCLUSION

Day by day application works on network increasing drastically, now almost all gazettes depend on network/internet. This new application and devices raise many security related issues. As number of network enabled devices increases, so, the requirement of application based on network increase. As a result, the footprint of network becomes very large and need complex security solutions. We have to continuously strengthen the security, and security standards which we are using today for tomorrow. We have seen that what we believe best security before 2013, has lot of vulnerability today. As in chain weakest part becomes the strongest level of security same in network weakest point becomes the strongest security. SSL/TLS the most secure web security protocol has lot of vulnerability and need quick solutions.

B. FUTURE WORK

In the future work the security in the transport layer may be achieved by overcoming the drawbacks does not formally account for side channels attacks based e.g., on timing, even though this implementation tries to mitigate them; proving the absence of such attacks would require specific tools. We focussed on the standard model of cryptography.

VI. REFERENCES


