VULNERABILITIES OF SECURE SOCKET LAYER (SSL) INSPECTION

By

Shahid Rafiq

A thesis submitted to the faculty of Information Security Department, Military College of Signals, National University of Sciences and Technology, Rawalpindi in partial fulfillment of the requirements for the degree of MS in Information Security

September 2020

THESIS ACCEPTANCE CERTIFICATE

Certified that final copy of MS/MPhil thesis written by **Shahid Rafiq** Student of **MSIS-15** Course Registration.No: **00000201398** of Military College of Signals has been vetted by undersigned, found complete in all respect as per NUST Statutes/Regulations, is free of plagiarism, errors and mistakes and is accepted as fulfillment for award of MS/Phil degree. It is further certified that necessary amendments as pointed out by GEC members of the student have also been incorporated in the said thesis.

Signature:_____

Name of Supervisor: Dr Mehreen Afzal

Date: _____

Signature (HOD): _____

Date: _____

Signature (Dean): _____

Date: _____

Declaration

I hereby declare that no portion of work presented in this thesis has been submitted insupport of another award or qualification either at this institution or elsewhere.

Dedication

This thesis is dedicated to my family, teachers and friends, without their love and support it was not possible to complete this document.

Acknowledgement

First of all I am extremely thankful to Allah Almighty for His endless blessings bestowed upon me. I am immensely grateful to my supervisor DrMehreenAfzal for her worthy supervision and support that enabled me to complete my thesis work. I would also like to thank my committee members, Maj (Retd) Muhammad Faisal Amjad and Asst Prof DrHaider Abbas for their valuable technical support and worthy guidance. Further I am obliged to all my teachers and colleagues for their endless support.Finally I would thank my parents and family for their continuous help and prayers to complete this work.

Copyright Notice

Abstract

HTTPS is used to secure the communication (transactions and other activities) over Internet using SSL. HTTPS enables entire encryption of the data to be kept confidential being transmitted from the client browser to the server and vice versa. But all of this is a sort of normal defences which are not visible due to encryption as encryption is also being used by criminals to hide their activities which may include hiding malicious actions/ messages, initial infection, C&C servers and intentional/ unintentional data exfiltration.For example, whenever a user downloads file (which may contain malware) through a phishing email supposing that its a safe file. It establishes an encrypted session to Command and Control (C&C) server and the attackers' malware gets downloaded directly. It results encryption of the attacks that occurred in the session and the intended malware evades the network security [1]. To defend against malicious payload encrypted by SSL, there may be a need to inspect SSL traffic as well. It means that some middleboxes inspect encrypted traffic in different ways to check whether it is malware free, this is called full SSL or deep inspection. The traffic is decrypted at middlebox and inspected by edge security tools and after inspection traffic is re-encrypted and transmitted to client [1],[2]. These middleboxes deploy different methods to decrypt SSL traffic for inspection like man-in-the-middle approach which in turn violates the end to end security of SSL[3],[9]. Such approaches violates end to end security and thus purpose of SSL security cannot be achieved in true spirit. Different vendors provide monitoring solutions for SSL traffic to guard against threats already mentioned. Our research aims are to explore different methods of SSL inspection deployed by the middleboxes, finding the vulnerabilities of the methods and improve upon the methods in order to ensure privacy and end to end security for which SSL was introduced.

Contents

Chapter 1

INTRODUCTION

1.1 Background

Nowadays, the use of HTTPS is made to have secured communication (transaction and different other activities) done over the internet through SSL. HTTPS allows data encryption to be more confidential that is being sent to the server from the client. However, all of this is a kind of normal defense that encryption cannot see as criminals also use encryption for hiding their activities involving hiding malicious messages/actions, C&C servers, initial infection, and unintentional/intentional exfiltration of data. For instance, when a user downloads such a file (having malware) with the help of phishing email, believing that the file is safe. It makes an encrypted session to the Command and Control (C&C) server, and the malware of the attacker is then directly downloaded. It outcomes in encrypting attacks that are seen in the given session. The intended malware then results in evading the security of the network. SSL is a standard in online security. Its use is done for data encryption, which is sent over the internet between server and client. It prevents any type of attack automatically. In case if a hacker does the interception of the encrypted data, thenthe hacker cannot use or read it without having the key for private decryption. SSL results in making secured websites. It gives protection to data from getting spoofed, modified, or stolen.

There can be no perfectly secure website. However, any such site that stores sensitive data or personal information should have SSL to give more security to the website. Assaults over trust because of TLS/SSL encrypted traffic are very common nowadays, and it is also developing in sheer brazenness, sophistication, and frequency. The high-reward and low-risk nature of the vulnerability of TLS/SSL make sure the continuation of these trends. It places the companies at risk of breach, unplanned downtime of the system, and failed audits [2]. Malware is designed for stealing certifications and keys of TLS/SSL to be used in data exfiltration and communication fraud. For instance, the operators of Advanced Persistent Threat exploit heart-bleed malware stole certificates and digital keys that outcome into breaching the records of patients of Community Health System (CHS).

The use of Heartbleed exploit was done in opposition to the system behind the firewall of CHS to increase the attack for reaching the highly regulated records of patients [3]. The heartbleed remediation needs the placement of all of the certificates and keys, not only for the patched system. Incomplete remediation implies that spoofing of government and business services can be done with a trust given by valid digital certification. Moreover, it can also result in the decryption of sensitive communication. Forgiving protection against persistent malware, companies should do the identification of systems through SSL/TLS, installing new certificates and keys over servers, revoking vulnerable certifications. It should be validated that proper installation of new certifications and keys has been done and that they are working positions [4]. TLS and SSL are mainly used for two reasons [5]. It is used for the server's authentication to which client communication. It is also used to encrypt data that is sent in between server and client. TLS or SSL attempts to acquire the given objectives on an end-to-end basis. However, this assumption is not valid. TLS and SSL can practically acquire encryption and secure authentication only over the basis of point-to-point, not based on end-to-end [6]. In figure 1, it is given that point-to-point communication can also be end-to-end communication. The client here gets the capability to do verification of secure communications through the next point, which it communicates. In figure 1, it can be seen the client makes a connection with TLS or SSL directly through the target system [7]. The client software then does the verification of system connected to have got verified through one of the hundreds of root CA that can be over the system. However, considering that if the system that is communicated with is following the expectations of the user is another subject [8].

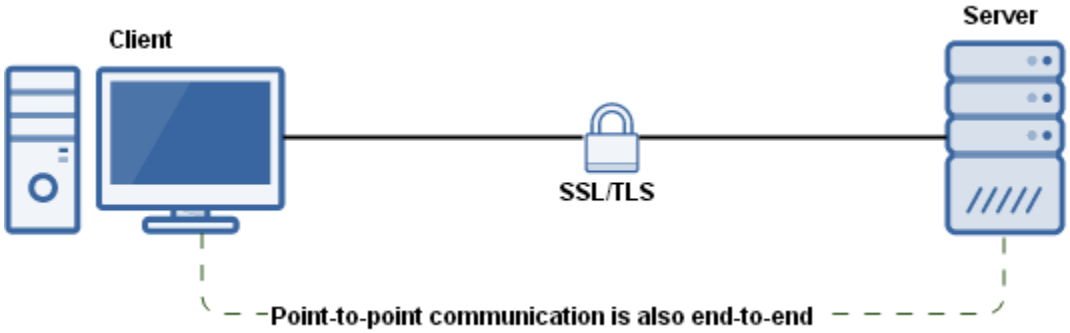

Figure 1: Point to point communication is also end-to-end

When the user loads a particular website into the browser that should have the protection of HTTPS (subsequently TLS or SSL), the browser confirms that the system to be communicated is giving a certificate issued through root CAs that can be trusted by the browser. It implies that it is trusted that root CA has performed the diligence for verifying the server's identity, to which connection has to be established [9]. In some of the cases, root CAs get tricked. It is also trusted that every root CA takes the right steps for giving protection to the systems. Sometimes, compromise is made over the root CAs [10]. For defending against malicious payload that is encrypted through SSL, the SSL traffic should be inspected. It implies that some of the middleboxes have done the deployment of various procedures for decrypting SSL traffic to inspect like the approach of man-in-the-middle, which does the violation of SSL's end to end security. These approaches tend to do violations of end to end security, and the objective of SSL security cannot be acquired in the right way.

1.2 Research Aim

Various vendors give monitoring solutions for the traffic of SSL to get protected against threats. The research aims to identify various methods of SSL inspection deployed through middleboxes. This research aims to find the vulnerabilities of the given methods and to make improvements in methods for ensuring an end to end security and privacy for which SSL was introduced.

1.3 Research Objectives

- To explore various methods of SSL traffic inspection deployed by middleboxes
- To find vulnerabilities of SSL inspection methods
- To suggest a way out against the vulnerabilities while achieving the objective of DPI.
- To recommend an environment where deep packet inspection middleboxes need to be introduced.

1.4 Significance of Research

In past researches, some working has been done over deep packet inspection (DPI) for HTTP. Various challenges and techniques of integration of deep packet inspection have been identified for these inspections [11]. In addition to this, in the past, some researchers have been done highlighting decryption through SSL inspectors and forward decrypted data for edging different tools of security such as forensic tools and DLP for more inspection. After the inspection, the re-encryption of data is done, and it is transmitted to the desired location [12]. Some of the

researchers have also done work over two schemes of encryption for searching securely over encrypted data for avoiding end-to-end security [13]. The use of SSL connection is made for doing communication on the internet as these are identified as a secured communication channel between two parties. Around 80 percent of the traffic of enterprise use SSL encryption. Sensitive companies need SSL traffic to leave the company. These companies deploy different middle/boxes of monitoring through various vendors such as FortiGate, Gigamon, Sonic Wall, and Secure Box. However, in the case when devices do the decryption of SSL data/packet at the middlebox, then it can be utilized incorrectly/insecurely. The users of the company can lose confidential information despite the deployment of SSL inspectors [14]. Different methods that get deployed through middleboxes should be studied to inspect the traffic of SSL to avoid leakage/loss of data and to avoid attacking through malicious traffic. This research will be helpful for companies who look forward to doingthe monitoring, whether to integrate middleboxes or not. In addition to this, new searchable schemes of encryption can be integrated intomiddleboxes for avoiding compromises on the privacy of these devices. This research will have theoretical and practical implications in the field of information technology. It will help to inspect the vulnerabilities of SSL inspection methods and can help in making improvements in these.

1.5 Structure of Research

The division of the research is done into different parts. First of all, the research has a chapter of introduction. Second chapter is about the literature review. In a literature review, past researches that have been done related to this subject is given. Research methodology adopted for the research is described in third chapter. Fourth chapter elaborates analysis and the research objectives. While last chapter encompasses a conclusion of the entire research summarizing the main points of this research.

Chapter 2

LITERATURE REVIEW

2.1 SSL

Secure Socket Layer (SSL) or Transport Layer Security (TLS) is a protocol of encryption that is designed for giving secure communication and for ensuring secure transferring of data over the internet. SSL permits customers to do authentication of the server's identity through the verification of X.509. Moreover, it makes rejection of the links in case if the certificate of the server does not get issued through the trusted authority of certificate (CA). SSL is famous for enabling HTTP traffic encryption between browsers and websites and for different other applications like email transfers and instant messaging [15]. An SSL man-in-the-middle attack is an interception connection between server and client where the attacker mainly impersonates server with the help of forged certificates of SSL that is SSL certificate not authorized or provided through the legitimate owner. Practically, certificates getting issued from more of the CAs are trusted automatically through client operating systems and browsers. CA can issue certificates that are trusted to any of the sites present over the internet. Therefore, CAs should ensure that certificates get issued only to the legal owners of every site.

2.2 SSL Encryption

SSL encryption is considered important for the protection of data within transit during the usage of mobile apps, email communication, and web transactions. Data that gets encrypted through this method can get uninspected by all of the parts of the framework of security, both outbound and inbound. SSL encryption has now transformed into a major ubiquitous tool for the enemy for hiding transfers of sensitive data and for obfuscating the control communications and command. For instance, imagine a user succumbing to one phishing email that is acquired each day, has followed a bad link of URL and downloaded encrypted malware of Zeus to the computer of the financial officer that is utilized for transfers of ACH bank [16]. Under encryption cover, Zeus sends that information of password and similar other sensitive data towards the external user. It results in making it doable for the remote attacker to get the session of login.

Moreover, the attacker can also get the transmitted password and then can deposit the money of the company into an account present offshore. Through all of the traffic and commands transmitted out and into the network through SSL, the security tools of the organization get blind to such practices. Now organizations are admitting the traffic that is even more encrypted as they make a shift towards even greater usage of services of cloud [17]. This implies malware will look forward to more of the innovative ways to take benefit of the common type of transport encryption. For instance, attackers can make use of cloud services for bypassing the firewall and can then do the synchronization of malware in one computer and on some other computer. With bad guys and good guys, both make use of encryption that results in making the traffic more visible through decryption. Its inspection becomes important. The decryption should be done in a way that it does not have any interference with the traffic of legitimate network while doing work with different systems for optimum performance and accuracy. The re-encryption of traffic should be done before sending it over the destination to give protection to the sensitive information that can get caught up in decrypted packets. SSL, also called transport layer security (TLS), is a general-purpose encryption PKI (public key infrastructure). It works in between the application having data that has to be protected and underlying transport protocol (TCP). It can be the major component of any of the applications involving email apps or web browsers. It gives protection to data through making it unreadable by different other recipients that unintended. This protocol is utilized for giving protection to proprietary, health care, and sensitive data, which is transferred from applications of e-commerce, workforce applications like public clouds like Amazon, SalesForce, and social applications of networking like Facebook and Twitter. Its use is also done for securing a VPN to secure FTP and remote clients, among other kinds of transport. SSL includes exchanging public keys that are utilized for the encryption of the symmetric keys, and its decryption can be done only through the private key of the other party [18]. This kind of exchange is done in communications done in between two of the entities, for passing the symmetric key of encryption that is utilized for the protection of data that is followed. Figure 2 shows the simple version of how its working is done.

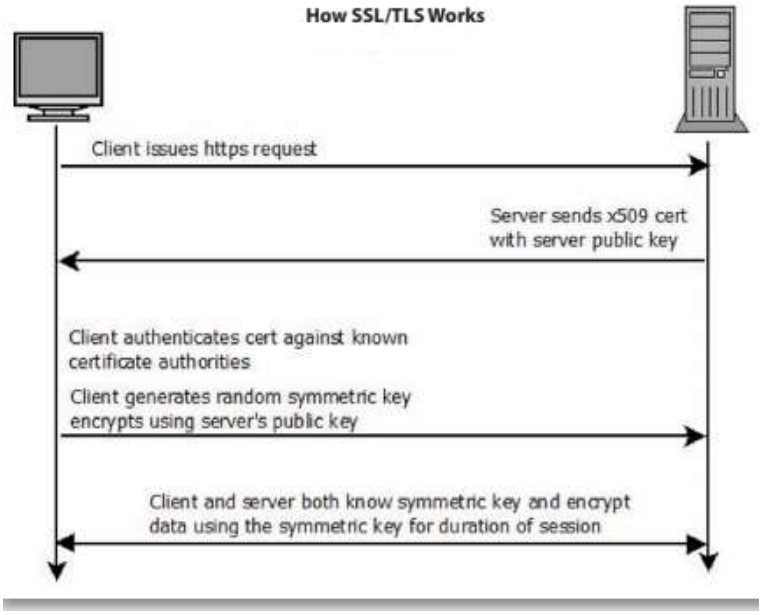

Figure 2: Process

The advantages of SSL are even beyond data protection and encryption to assure non-repudiation and data integrity. These are the major tenets of any program of risk management. However, it is significant to notice that SSL can be used without even the right kind of authentication, like in using the self-signed certificates of the server.

2.3 Security Impact of HTTPs Interception

2.3.1 TLS Interception

Network middleboxes and client-side software that inspect the traffic of HTTPs through acting like more transparent proxies. The client-started session of TLS is terminated and decrypted. The inner plaintext of HTTP is then analyzed, and a new link of TLS with the website is made. Through design, TLS results in making this kind of interception more complicated through the encryption of data and through defending against man-in-middle attacks through the validation of the certificate. In this case, the client then does the authentication of the server's identity, and impostors are rejected [19]. For circumventing the given validation, self-signed certification of CA is injected through the software into the root store of the browser of the client at the time of installation. For middleboxes of the network, administrators deploy the CA certificate of middleboxes to devices present within the company. Subsequently, in the case when the proxy

does the interception of a link to some specific site, it makes a certificate dynamically for the domain of that site signed with a certificate of CA. Then the delivery of this chain is done towards browser. Unless users do the verification of the certificate chain manually, they cannot notice that the interception and re-establishment of the connection have been done.

2.3.2 TLS Feature Negotiation

TLS servers and clients make negotiations on different parameters of the protocol while making the connection. In the very first message of protocol, Client Hello, the client does the specification that what is the version of TLS and then do the featuring of its support. Afterward, it sends cipher suites' ordered lists, extensions, and compressional methods. These involve some of the additional parameters, like the signature algorithm and supported elliptic curves. The server then makes the selection of agreeable choice through all of the given options [20]. This mainly supports the evolution of characteristics and gives adaptability while waking new kinds of attacks. As in the year 2016, there were around 340 of the cipher suites, 28 signature algorithms, 36 elliptic curves, 27 extensions that can get advertised by clients, and three elliptic formats of curve point. Practically, security products and browsers make use of different libraries of TLS and do advertisements of various parameters of a handshake. These variations in features permit the unique identification of individual integration of TLS dependent on the handshakes.

2.3.3 HTTP User-Agent Header

The protocol of HTTP permits the server and client to give more information during the connection through involving header fields within the messages. For instance, Accept-Charset can be involved by the client: utf-8 header for showing that it assumes the encoding of content into UTF-8. The user-Agent header is one of the standard client headers. It shows the operating system and browser of the client in a more standardized form. More research has also been done over the spoofing of the header of User-Agent. The User-Agent header is not spoofed through the end user [21]. Around 0.03percent of the links with User-Agent of Firefox give facilitation to the features that are unique to the internet, showing spoofing [22]. The researches related to fingerprinting trust the string of User-Agent.

2.4 Measuring TLS Interception

The rates of international interception can be measured through making the deployment of heuristics at three points of network vantage: popular websites of e-commerce, servers updated through Mozilla Firefox, and the content distribution network named as Cloudflare. 7.74 billion of the handshakes of TLS were used across three of the given networks [23]. Through making the deployment of the given heuristics over various networks, the bias inherent of one of the vantage points can be avoided. However, different kinds of abuse and interception are seen at every network.

2.5 Firefox Update Servers

Firefox browsers look forward to making updates in software through retrieving the document of XML through HTTPs, which is the central server. This check makes use of the standard TLS library of Firefox. It is done after every 24 hours, while the working browser and launch are done over browser in case if the last update gets occurred over 24 hours earlier. Bro [49] was used for monitoring the connections made to aus5.mozilla.org [24]. It is the updated server that Firefox versions utilized in between February 14 to February 26. In the given period, 4.36 billion links were observed from 249 ISO-described countries. It is because of the reason that traffic was collected utilizing an on-path monitor than using some web server. However, only some of the particular Firefox versions are configured to get linked to the server. Instead of finding a mismatch to the User-Agent of HTTP, the mismatch is found in between the handshake of TLS and any such version of Firefox that gets configured to get linked to the server. There is no such content that user-accessible over the site. This point of vantage gives the cleanest idea of clients that get influenced through the interception of TLS. However, it only gives data for Firefox, one browser that gets least influenced through the software intercepted through the side of the client.

2.6 Popular E-commerce Sites

In two weeks in September and August, JavaScript was hosted by a set of famous sites of e-commerce that loaded a pixel through external server recording client HTTP headers, HTTP user-agent string, and raw TLS Client hello. This approach observed traffic through all of the browsers and can suffer falsified headers of user-agent. However, because of the reason that measurement needed the execution of JavaScript, the simple fetches of the page were excluded from the dataset. The sites are present globally. However, the link is more skewed towards the

users of desktop [25]. It is because the provider of e-commerce has famous applications of mobile. The dataset has another advantage that it involves headers of HTTP even beyond the User-Agent. It permits the other avenue to detect interception. It involves looking forward to the proxy linked headers and X-BlueCoat and X-Forwarded-For.

2.7 Cloudflare

Cloudflare is a famous DDoS protection and CDN company that gives services to around 5 percent of the traffic on the web. Cloudflare gives such services through acting as some kind of reverse proxy. Clients make a connection to the servers of Cloudflare while making access to the website. The website server proxy the link or cached content to the initiated web server.The Hello messages of TLS Client and HTTP User-Agent were logged for 9.5 samples of all of the connections of TLS to the frontend of Cloudflare between May 13 to May 20, the year 2016 [26]. Interception is measured through the detection of mismatches between TLS handshake and HTTP User-Agent. Cloudflare gives a representative browsers' sample as compared to Firefox update servers. However, on the other hand, the major objective of Cloudflare is the prevention of attacks of DDoS and such other kinds of abuse (like attempts of scripted logins). Therefore, it can be stated that the data tends to be messier as compared to the other two given sets of data, and a portion of links can falsify the HTTP headers of User-Agent.

2.8 Analyzing Forced SSL Certificates in Wild

2.8.1 The SSL Protocol

The design of Secure Socket Layer (SSL) was made for securing the communication done in between two of the entities over different untrusted networks. The SSL protocol gives authentication dependent on the infrastructure of the X.509 public key. It gives protection to the confidentiality of data through symmetric encryption. Moreover, it also ensures the integrity of data with the digests of the cryptographic messages. SSL is mainly utilized to secure mail servers and websites, preventing attackers of the network from replaying the messages of client or eavesdropping [27]. It is mainly identified as the best activity for the security of the website. Through enabling encryption, websites can avoid eavesdropping of the data that is confidential and unencrypted. For making the connection of SSL, the server and client do handshake for authenticating one another and for making negotiation.

2.8.2 The SSL Man-in-the-Middle Attack

SSL man-in-the-middle (MITM) attack is a kind of active interception of the network where the attacker gets inserted into the channel of communication between the server and client (mainly to manipulate communication or to eavesdrop) [28]. The attacker makes two separate connections of SSL with server and client, and then the messages are relayed in between these. The messages are relayed in a way so that both the server and client remain unacknowledged about the middleman. This setup lets the attacker record all of the messages over a wire, and even the selected modification of data can also be done.

2.8.3 Certificate Observatories

More of the server surveys of SSL have identified certificate authorities and SSL certificates over the internet. It was identified that there are 1.3 million of the unique certificates of SSL by EFF SSL. It was done with the help of scanning of the whole space IPv4. It was found that around 1482 trusted signers of certificates are utilized. Same like this, more than 42 million certificates were collected through scanning around 109 million of the hosts, and through this, 1832 trusted signers of the certificate were determined [29]. The analysis of SSL certificates was done through monitoring the traffic of SSL over the network of research along with the scanning of popular websites. It was then identified that more than 40 percent of the certificates were not valid because of the incorrect names of host and expiration. Following the research of ABC ( ), SSL certificates can be analyzed through better monitoring the traffic of live users at different networks. These can be categorized as current warnings of the certificate, involving decisions related to browser design and misconfigurations of the server. However, present researches do not give perception related to the forged certificates. It can be because of the reason that there isa lesser number of network attackers over the networks ofresearch institutions.

2.8.4 Tamper Detection Techniques for WebSites

Different strategies have been proposed to help websites identify that if the network connection of the client gets more tampered with. Such methods of detection can be used that do not need interaction with the user and do not need installing extensions of browser or any other additional

software [30]. Client-side JavaScript code can be used for detecting modifications in-flight to the page of the web.

2.8.5 TLS Proxies

Secure communication over the internet tends to be dependent on the digital certificates that central and certificate authorities sign. This system of validation gets compromised by using proxies of TLS. It can mainly work like man-in-the-middle for connections of TLS. A substitute certificate can be issued through TLS proxy for any of such websites that are visited by the user. Therefore, it let the users make an encrypted link with proxy than the given site. The proxy can then result in decrypting and modification or monitoring the traffic of all users before giving it through the second channel of encryption to the given site. The use of TLS proxies is made for different legitimate objectives, like blocking malware [31].

Malicious entities can also use it for compromising the security or privacy of different end-users. Isolated attacks had been seen in the wild. The most dangerous approach of TLS proxies is the fact that the user remains unacknowledged that the attacker or company intercepts encrypted traffic. There is the controversial use of proxies of TLS because of the reason that browser software still depicts a lock icon in such a session, compromising the security and misleading different users. Detecting the prevalence and presence of TLS proxies is quite a challenging issue of measurement. For the detection of the proxy, the certification of the client should be acquired, and like a web browser, then it should be compared with some other valid certificate that is presented through the server. A mismatch shows that some type of proxy, either malicious or benevolent, intercepts the traffic of the client to some specific server. To identify the prevalence of proxies of TLS, this measurement should be repeated over as many systems of the client as possible. Different researches have identified the ecosystem of the certificate through scanning some of the secured servers through one viewpoint or passive monitors belonging to different vantage. However, detection of necessitates of proxies at the client, and lesser work has got done in this area. Two current works have identified some proof for proxies of TLS through measuring certificates that clients give. It has been identified that the prevalence of proxies of TLS that intercept traffic through clients linking to Facebook, identifying that 1 in around 500 TLS links get proxied through personal antivirus and internet filters [32].

Along with it, a smaller number of links were seen as getting intercepted through malware. It is because of the reason that this research makes use of Flash for detecting the mismatch of certificates. It does not perform detection of proxies influencing most of the mobile phones. The Netalyzer project did the measurement of certificates that is acquired through various Android apps. It involves the assessment of 15,000 sessions and identification of only 1 case of proxy of TLS running in the app of analytics [33]. This is a lower prevalence rate; the application was identified to be whitelist different websites involving Facebook. This shows that proxies measurement should analyze the sites of low-profile that cannot get whitelisted—the measurement of proxies' prevalence through a Flash app deployed with the campaign of Google AdWords. Like Huang, the measurements make use of Flash for detecting mismatch without any interaction of the user [34]. However, the tool was deployed through the campaign of Google AdWords, which affords different benefits. Firstly, the clients are measured, dependent on how money is spent over the ad [35].

Chapter 3

RESEARCH METHODOLOGY

3.1 Introduction

In the given chapter, a research method that has been used for this study is given. The objective of this chapter is to give a reason for the selection of a specific methodology for this study. It is ensured that such methods of research are selected that allows them to fulfill the aim of the study in the best possible way.

3.2 Interpretivism Research Philosophy

The current study is dependent onthe interpretivism philosophy of research. The major assumption of the philosophy of this study is that reality gets constructed through individuals making interaction with the social world. There exist different realities. This philosophy of research is dependent on the understanding of factors of the research. Interpretivism stated that access to reality could be made with the help of social meanings and construction that cannot exist without consciousness [36]. Therefore, it can be stated Vulnerabilities of SSL Inspection could not be identified in the case of mindfulness, perception, and consciousness of the researcher get ignored. The target of research-based oninterpretivism philosophy is to explore the research meaning through doing the employment of different perspectives and methods to identify various approaches to the research problem [37]. Consistent with this approach, this research makes use of different methods for identifying vulnerabilities of SSL Inspection.

Interpretivism is seen as dependent on naturalistic approaches to do a collection of data like interviews and observation [38]. It has been identified that this study is dependent on two beliefs of interpretive philosophy, like subjectivist epistemology and relativist ontology. An ontology describes the reality's nature, while epistemology identifies the nature of the link between the research and reality. In relativist ontology, the inter-subjectivity gets identified through a reality, where the analysis of interpretation and meanings is done at social and experiential levels. In addition to this, as per interpretivism's ontology, it is identified that different realities can be based on other systems. This results in making it quite complicated to understand the reality within the fixed terms. The knowledge that is attained through such philosophy does not tend to be objective than being constructed socially [39]. Following subjectivist epistemology,

individuals cannot be separated through knowledge. Therefore, there is a requirement for a clear link between the research problem and research. Therefore, while doing research related to the subject of Vulnerabilities of SSL Inspection, it is believed that both the participants and researchers are mutually interdependent and interactive. The promotion of flexibility is done to give meaning to what is identified as being the reality. With the good insight of the research context, interpretivism gets entered into the field of research; therefore, they owe more to the complex, complicated, and unpredictable nature of reality [40]. The rigid and fixed design of research cannot be made. In the entire research, new knowledge is considered important, and it gets developed more through the respondents. This is consistent with the interpretation of interpretivism that is adapted by humans, and prior knowledge cannot be gained, ignoring context and time.

Along with it, the study is more dependent oninterpretivism philosophy and aims to interpret the meanings than a generalization of outcomes [41]. Being the researcher that is interpretivism, more significance should be given to interpreting the opinions, motives, reasons, meanings, and subjective experiences that are time and context-bound. It is significant to identify that interpretivism has its base over critical analysis of positivism, and it ignores the objectivist approach. Therefore, the objectivist view was not adopted by the researcher. The rationale for not choosing positivism is that it is seen as dependent on artificial and rigid approaches. It does not permit an effective interpretation of meanings linked with the particular problems of research.

Similarly, positivism does not permit the development of theories. In addition to this, it does not tell about the actions that policymakers should take in the future for solving the issues. Conclusions and objective inferences are seen possible when the researcher gets more objective, which is not seen possible due to the reason that human conduct mainly includes the responses related to emotion. However, it results in disregarding the emotions of humans; it is not sure if it will always be ignored. Positivism research philosophy is dependent onthe belief that the measurement and calculation of everything can be done, and the unexplored process then gets disregarded [42]. Therefore, it does not encourage lateral thinking, which assists in answering the issue of research in the most creative way. Therefore, continuing with the positivist philosophy of research was more feasible.

On the contrary to this, interpretivism research philosophy has been chosen in this research, because of the reason that it permits the interpretation of meanings behind the problem of research. It allows formaking adjustmentsto new issues and ideas. This philosophy of research makesmajor contributions to the process of development of theory. Therefore, for this study, it is more feasible. In addition to this, the collection of data is done in a natural environment. Unlike the positivist philosophy of research, an artificial environment is not needed for the collection of data. Therefore, its outcomes are identified as being closer to reality. Considering all of the given approaches, the most accurate philosophy for this study is interpretivism.

3.3 Research Methods Adopted

There exist two alternatives for choosing the methods of research, like quantitative or qualitative. Qualitative methods of research are utilized for exploratory researches, and these are identified as being more appropriate for such researches that target to interpret opinions, reasons, and motivations. To uncover trends in thoughts and opinions, the qualitative methods of research are identified as being more suitable. Quantitative methods of research are utilized for the quantification of the issue of study with the help of numerical data. Through this approach, the quantification of opinions, behavior, and attitude is done, and the generalization of outcomes is made to the entire population. In the quantitative methods of research, there is a higher structural element, and the collection of data is done with the help of closed-ended and structured tools of research [43]. The selection of the method of research is seen based on the question of research that the researcher tries to answer. Taking this into account, in the current study, the researcher used qualitative methods of research. The reason for the selection of this method is over the alternative that it gives required detail and depth to the objectives and aim of the study. It let the researcher look deeper into the problem of research and to perform in-detailed analysis through doingrecording the attitude, behavior, and opinion of individuals. This method also gives required openness where respondents are motivated to increase their response. Hence it helps in exploring new insights that are not known earlier. With the help of this model, the development of a detailed picture is done, and pre-judgments related to the problem of study are ignored,which is not possible in the case of quantitative researches. Therefore, qualitative methods have been used in the given study.

There are different strategies of research that a researcher can adopt. Some of the examples involve survey questionnaires, case studies, focus groups, and interviews. In the given study, interview strategy of research has been used for the collection of qualitative data [44]. The reason why this technique has been used is that it let the researcher analyze different perspectives in a particular way, and the human dimension is also added to the data this way. It also permits asking more of the questions through respondents, and it is seen possible in the questionnaire. Interviews give findings that are more accurate as participants get the chance to do clarification of ambiguities, which are not seen in different other alternatives [45]. In interviews, others cannot make any impact, as is seen in the strategy of the focus group. Therefore participants get able enough to give honest answers. The reason why the strategy of the questionnaire should not be used is that participants can avoid some of the specific questions. Getting the answers to such questions is not possible then because of the problem of anonymity. Questionnaires can be impersonal, and in most cases, participants incorrectly answer these questions because of the structural reasons [46]. The long and complicated problems of research, such as the national business system, cannot be studied in the right way with the help of the given method. The case study can also be utilized by the research. The use of the case study has not been done for the given research. It is because of the reason that this method has some of the limitations, because of the rigor of methodology. The case study does not own methodology rigors [47].

Moreover, the research can make decisions related to his direction, as there exist no such systematic processes for the analysis and collection of the case study. In addition to this, lower external validity is seen in the method of the case study. Therefore, this study is not dependent on the method of the case study, and instead, interviews have been conducted.

3.4 Generalizability, Validity, and Reliability

Generalizability and reliability are identified as of more significance for positivistic researches [48]. However, their applicability towards qualitative researches is lower. Qualitative research cannot generalize the outcomes, but it targets to understand events [49]. Therefore, following its nature, the replication of a qualitative study cannot be done. Indeed, every research gets interpreted uniquely. Therefore, certain research cannot be replicated. Therefore, researchers of management and business doing qualitative study do not give significance to the study's external validity. Instead of external validity, it is an internal one, which is considered significant for

qualitative researches [50]. Qualitative researchers should target on the consistency of outcomes of the research to the reality as given by researchers, and the current research targeted the internal validity of outcomes of the study, where it was ensured that experiences of individuals get presented most accurately.

The improvement can be made in understanding qualitative researches through dependability, confirmability, creditability, and transferability [51]. The current study fulfills the given four aspects in the given way.

- To ensure conformability, more trust was developed between participants, and researchers and different viewpoints were acquired related to the similar process of study. All of the respondents were given the sheet of information, which had the detail related to the study. In addition to this, the agreement of confidentiality was not signed before the interview. To get a different approach, multi-actor approaches were acquired.
- To ensure credibility, the triangulation of methods and participants is ensured. In the given study, document analysis is also than interviews. As defined previously, multi-actor approaches were acquired to get more credible data. The participants of this research were different IT employees of software houses of Lahore in Pakistan
- Transferability gets ensured through the selection of the right interviewees. This study is related to the analysis of vulnerabilities of SSL. Therefore, different employees of software houses were contacted [52]. In addition to this, this research has involved small and medium software houses that were also contacted for increasing the transferability of the outcomes of the research.
- To ensure dependability, respondents were identified to identify the past and current experience through examples. Dependability deals with the reliability of qualitative research, which ensures that outcomes are more dependable and consistent [53]. The reflexivity also ensures dependability where the researcher maintained the diary of personal reflection during the process of data collection and research, which shows that how the background and interest of the researcher have assisted in the study.

3.5 Ethical considerations

It was significant to refer to the ethical standards during the process of data collection; the ethical standards have been taken into account. Before taking the interview, consent was considered significant. Therefore, it was acquired through interviewees in written form. The interviewees were asked to sign the consent form. For this study, a written request to make participants was sent to interviewees. Within one week, the phone calls were also made. The interview was taken from only such individuals who agreed to make participation. Confidentiality and anonymity of interviewees should be ensured [54]. Therefore, it has been ensured that there is no disclosure of personal information in this study. The researcher has ignored the collection of sensitive information, like the interviewee's name within the interview. For the protection of participants' identity, pseudonyms are utilized during the transcription of the interview. Interviewees' confidentiality was ensured through the agreement of confidentiality between interviewee and researcher.

The interviewees were given information related to the introduction of a study where the aim of the research, contact details and name of research, contact details, institutional affiliation, and supervisor name were given in the sheet of information. It was communicated very clearly that any of the information collected through them would not be given to the third party. Before starting the interview, the interviewees were sent a request. Interviewees also had the right to stop the recording permanently or temporarily if they wanted during the session of the interview. All of the interviewees were permitted to do a recording of the interview, and just a few of the interviewees asked to stop the recording temporarily during the session of the interview. In addition to this, these were also given the right to skip any question that they did not want to answer. It was ensured that the personal information of interviewees would not be disclosed to anyone.

3.6 Chapter Summary

In the given chapter, methods that have been used for this study are given. This study is dependent oninterpretivism philosophy, where the selection of qualitative data is made for the study. An interview research strategy is chosen for the given study. In addition to this, the researcher ensured the reliability, validity, and generalizability of research in the most appropriate way. Along with it, ethical standards and norms were taken into account for the given research.

Chapter 4

ANALYSIS

4.1 Vulnerabilities of SSL inspection methods

Different abusive employees and external attackers have given more attention to the research of encryption. As NSS Labs have stated in a current report, 'ironically, enhanced usage of SSL in a trail to make the online lives securer can result in doing the blind sports. It can then result in decreasing security. Even with all of the general practices of security of enterprise in the right place, monitoring tools can just see the destinations. In some of the cases, the hostname can be seen in the unencrypted part of the handshakes of SSL [55]. The full path cannot be seen, the content itself, or content type. It can be an issue where the control channels and command or encryption hides sensitive data's exfiltration.

4.1.1 Hiding Malicious Actions and Messages

- Bad actors do and can use SSL for doing of the malicious actions and for exfiltration of data in the given ways:
- An encrypted kind of critical, sensitive and protected data can be sent outbound using the firewall of the user or through normal ports like 80 or 443, for which the tuning of firewall is done to accept it. It is because of the reason that these are approved parts.
- The malware communication gets obfuscated where the botnet or virus worm is sent for stealing the data to download instructions or to a master the computer or for the malicious code [56].
- The phishing of threats tends to be legitimate, as even the recipients that are informed believe that the use of SSL results in making it a bit more secure. However, clicking over the link results in taking them to the SSL server, having malware. It then outcomes into infecting the client, due to the encryption of malware traffic or because IPS does not identify it. Such real threats make it possible to make the given scenarios, all of these play again across all of the verticals, following which different media reports.

4.1.2 Hiding the Initial Infection

An initial infection comes through a port, and a secure browser acts as the most common way; the launch of infections is done beneath IPS or firewall radar. Following CGI Security, attacking a company gets easier using different applications that make use of encryption as compared to those that don't. With a FAQ over the scripting attacks cross-site. Websites having SSL (https) are not more protected as compared to the encrypted sites. The web applications work similarly, except the attack is done in an encrypted link. Individuals often believe that a lock is seen over the browser; it implies the security of everything. However, it is not the right case. In other words, it can be stated that using encryption gives the perfect cover and results in making a phish for which users fall. In [57], it has been identified that malicious users can often steal cookies with the help of cross-site scripting. It can then be utilized for different things, involving false advertisement or poisoning of the cookie, altering the settings of users, session, or account hijacking. All of this gets accomplished while getting hid in the traffic encrypted through SSL.

4.1.3 Hiding the Command and Control Channel

Malware families like Zeus tend to be notorious for using encryption and for various other tricks to control and command communication through devices for monitoring security. Gameover is the current example banking Trojan that results in opening an SSL connection through servers that are compromised and utilize that channel to control and command different practices. Spam is used for sending the starting infection, and after the browser of the user touches the site that is infected, the opening of the channel is done automatically. Gameover has been connected to banking credential attacks of theft and DDoS.

4.1.4 Hiding Data Exfiltration

An enhancing number of families of malware also makes use of encryption for hiding any information related to network, involving sensitive data or passwords. These are sent out to the servers of SSL. In the hypothetical cases, the phish gets undetected because of the reason that programs of infrastructure do not involve inspection of SSL over the outbound response towards email. Moreover, its firewalls did not sound any kind of alarms for blocking the packets. Afterward, the malware makes connections for controlling and commanding servers through

deep inside the given network. Afterward, financial account data was sent out of the company under the sessions encrypted through SSL [58]. It looked more legitimate to the security of the edge network. The encryption resulted in making the monitoring systems to get blind to these practices of the internal network. Therefore, the attack was then made for around nine months until the company got alerted through the external party that a thousand accounts associated with the processing systems of the company had been abused and exploited.

4.2 Suggesting a way out against the vulnerabilities while achieving the objective of DPI

Most of the network middleboxes do deep packet inspection (DPI) to give different services that can give benefits to both network operators and the end-users. For instance, Network Intrusion Detection/ Prevention (IDS/IPS) systems do detection in case if packets through a compromised sender have any attack. Devices for exfiltration prevention block any kind of leakage of private data present within enterprises by looking for the confidentiality watermarks of the document in the data that get transferred through the network of the enterprise. The devices that are used for parental filtering also prevent children from making access to the adult materials present within homes, libraries, and schools. These devices share a common type of feature that they inspect payloads of packets [59]. The market for these devices of DPI was expected to get developed to more than $2B by the year 2018 [60]. Simultaneously, HTTPs and similar other protocols of encryption have observed dramatic development in its usage in current years. Encryption gives protection to the private data of users through eavesdropper within the network, involving a middlebox. Unfortunately, HTTPS is posing a major challenge for the devices of DPI. The encryption of packet payload implies that now middleboxes cannot do the inspection of payloads, and these cannot complete the task. To enable the processing of middleboxes, some of the presents deployed in middlebox systems give support to HTTPS in an insecure way. A man-in-the-middle attack is mounted over SSL, and then the traffic gets decrypted at the middlebox. This approach does the violation of end-to-end security, and therefore, it results in different problems. In addition to this, clients and users have also made more criticism over the approach. Some show worries that the private that gets lodged over middleboxes is then provided to the marketers. Therefore, an individual faces the unfortunate choice of one of the given two characteristics: the privacy that encryption gives and the middleboxes' functionality. BlindBox is a system that gives the advantages of both functionality and encryption at the DPI middlebox [61]. The name 'BlindBox' shows that the middlebox cannot observe the private content that

gets over to the traffic. The approach is to do the direct inspection over the payload that is encrypted without doing the decryption of payload present at the middlebox. The development of this system is though quite challenging. Networks operate at higher rates needed different cryptographic practices over the critical path to run in nano or microsecond. In addition to this, some of the middleboxes need support to perform various rich practices, like matching different regular expressions. A potential candidate is just like a cryptographic scheme like functional encryption or fully homomorphic [62]. However, these are slow, reducing the rates of the network through different magnitude orders. For overcoming the given challenges, BlindBox identifies and does the specialization in the setting of the network. BlindBox enables two of the classes of the computation of DPI, each owning some guarantees of privacy: probable cause privacy and exact match privacy. Both of the privacy models of BlindBox are stronger as compared to the approach of state-of-the-art 'man in the middle.' In both models, BlindBox gives protection to the data through randomized schemes of encryption, giving the same guarantees of security to the encryption notion. Based on the computation class, BlindBox permits the middlebox to have some information related to the traffic for the detection of rules in an efficient way. The first computation class involves applications of DPI that are dependent on the exact matching of string, like limited IDS, parental filtering, and watermarking. Under the model of associated privacy, exact match privacy, the middlebox gets to know that at which of the places, a flow attack keywords get occurred. It happens for the flow substrings that are not as an attack keyword. Middleboxes do not learn anything in a virtual environment. The second computation class can facilitate all of the applications of DPI, involving those which do scripting or regular expressions. The BlindBox has been integrated as a new secure protocol of transport for HTTP, which is termed as BlindBox HTTPS. BlindBox HTTPS has been evaluated through different applications of real DPI: intrusion detection, parental filtering, and data watermarking. The attack signatures have been utilized through industrial IDSes and open-source communities. It has been identified that the performance of BlindBox is practical for different settings. For instance, the rate at which the middlebox can perform the inspection of packets is as higher as around 186 Mbps. When referring to the implementations of IDS, this is seen as going to the peak at under 100Mbps. There is more competitiveness in this performance with the existing deployments. BlindBox Detect and DPIEnc have helped to achieve this performance [63].

4.3 To explore various methods of SSL traffic inspection deployed by middleboxes

There exist four of the parties: sender (S), receiver (R), rules generator (RG), and middlebox (MB). These show the deployment of standard middleboxes nowadays. RG causes attack rules that are termed as a signature to be utilized through MB in doing detection of attacks. Every rule tries to define an attack, and it involves different fields like one or more than keywords to get matched in the given traffic, offset information for every word, and in some instances, regular expressions. Nowadays, companies perform the role of RG, such as Symantec, McAfee, Emerging Threats. R and S are sending traffic with the help of MB. MB permits R and S to do communication unless MB sees a rule of attack in the traffic. Today, the administrators of traffic do the deployment of in-network middleboxes. It is because of the reason that it provides them a central control point for enforcing the policies of security within the network.

Moreover, it is also easier to do management and upgrades using a single in-network device. The deployment of the alternative edge was considered where endpoints did the processing of middleboxes on the traffic [64]. The distribution of rules is then done towards endpoints. BlindBox targets to make alterations incompatibility with the approach of the network. In addition to this, this edge-based model does not have compatibility with the requirement to keep rules hidden through endpoints.

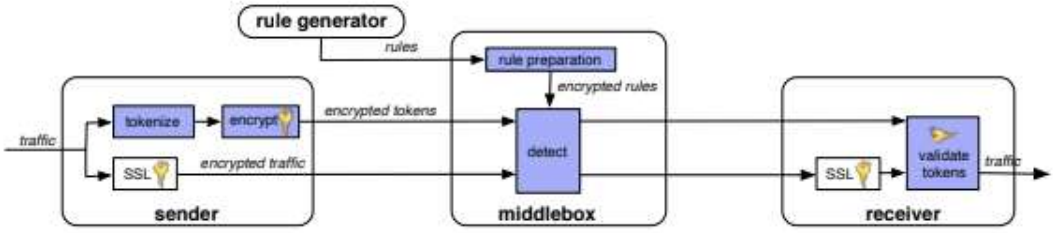

Figure 3: System architecture, Shaded boxes indicate algorithms adopted by BlindBox

In deployments today, MB can read traffic that is sent in between the sender and receiver. Through Blindbox, MB gets able enough to do detection of attack rules developed through RG match the traffic in between R and S. However, it does not learn traffic contents that do not match the attack rules of RG.

4.4 Recommendations

In paper [68], a method was introduced to detect SSL man-in-the-middle attacks as opposed to the users of the website. The feasibility to detect man-in-the-middle attacks has been demonstrated through the integration of a system on different SSL connections at the top international website. In [69], the analysis of forged certificates of SSL in the wild was given. Direct proves been revealed that around 0.2 percent of the connections of the real-world got substituted through unauthorized forged certificates. While some of the major interceptions of SSL were because of the antivirus software and because of different devices of surveillance, some of the amateur attempts of the attack were seen. Also, some of the malware traces in the wild were seen that intercepted the connections of SSL. The data given in [70] recommends that browsers could detect different forged certificates dependent on the characteristics of size, like checking if the depth of the certificate chain is larger as compared to one. Popular websites are motivated strongly, and also other mobile apps are encouraged to do the deployment of the same procedures to initiate the detection of SSL interception.

For encountering such threats, companies require visibility into the traffic encrypted through SSL. It implies that through SSL, inspectors working with secure gateways and other edge security get able enough to inspect traffic after its decryption. Visibility into sessions of SSL-encryption should involve inspection of outbound, inbound, and even suspect the SSL traffic present internally for detecting control and command communication, malware distribution, and outbound sensitive data. Any of the solutions to give visibility into the traffic of TLS/SSL should fulfill the given criteria:

- It should be parallel, so it can make automatic and immediate responses to outbound and inbound traffic (there can be cases where preference is given to the inspection done out of bound).
- It should send decrypted traffic towards network and towards the security devices present at endpoints like advanced network gateways, forensic devices, IPS and IDS for doing the inspection immediately.
- It should decrypt outbound and inbound traffic, having complied with the policy depends on what is known better and suspected or known bad practice and also other considerations.

- It should be capable of decrypting both outbound and inbound communications, involving the email communication and web through which external attacks are caused.
- It should be capable of filtering or whitelisting some data that should be encrypted, like information of patients having protection through HIPAA. This avoids revealing such data that we are trying to keep safer.
- It should do the processing of larger data more quickly.
- Decryption should assist in accelerating the analysis of traffic, then coming in the way of the given programs.

The provision of visibility into the traffic of SSL is not similar to the analysis of data. While the inspection of SSL may be capable of following some of the rules that govern which traffic needs decryption upon getting inspected. The real analysis of such decrypted packets is done with the help of tools that work with the device of SSL inspection. These involve firewalls, monitoring systems, data loss prevention (DLP), secure web gateways, firewalls, IDS/IPS, and other forensics tools dependent on the policy among various devices.

4.4.1 Deployment Options

Security tools can either be passive (tapped over the line) or active (generally inline). Passive monitoring includes simpler detection and getting logged in after the decryption. When the device for SSL inspection gets into the passive configuration, then it can only assist in feeding the passive tools of security. Passive tools, like IDSs, can analyze the traffic and then can send alerts too. However, it cannot do the blockage of threats. Powerful tools of monitoring like IPSs permit more of the actions to get performed, involving segmentation of data into a secure zone to perform analysis or blocking the traffic that is being suspected. The inline model should be used to support active monitoring. It is ideal for most of the inspection abilities of SSL [71]. This is mainly true during some live investigations, where time is important. Figure 2 depicts a device that is used in line for decrypting the internal traffic between client PC and server within the firewall of corporate.

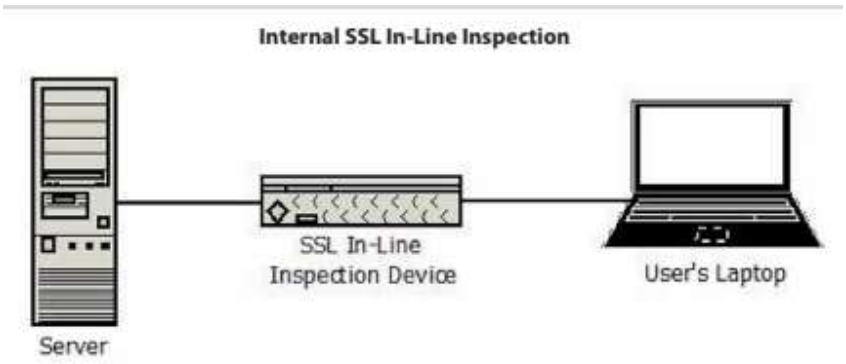

Figure 4: Inline Packet Inspection for Internal Systems

Internal communication between different servers is common among different families of malware that make use of encryption for giving protection to the communication. For instance, malware could be sniffing more sensitive data over the network or can even copy it off over various infected devices and then can part it over the internal server before moving the data out of the network.

4.4.2 Making SSL-Encrypted Traffic Visible

Assisting other tools of monitoring

The inline appliance of SSL-inspection does the detection of the session of SSL. It makes a consultation to its policy for identifying that if the inspection of the session should be done. In the given case, the sessions could raise some flag in case of abnormality of the kinds of servers and applications talking to each other. In case if the session needs any kind of decryption, then it causes the decryption of data at higher speed and then transfers the decrypted data to the tools of security where the data should move. The other option is the deployment of the appliance of an inspection outside the firewall [72]. Figure 3 depicts the configuration with the connection to the linked security tools.

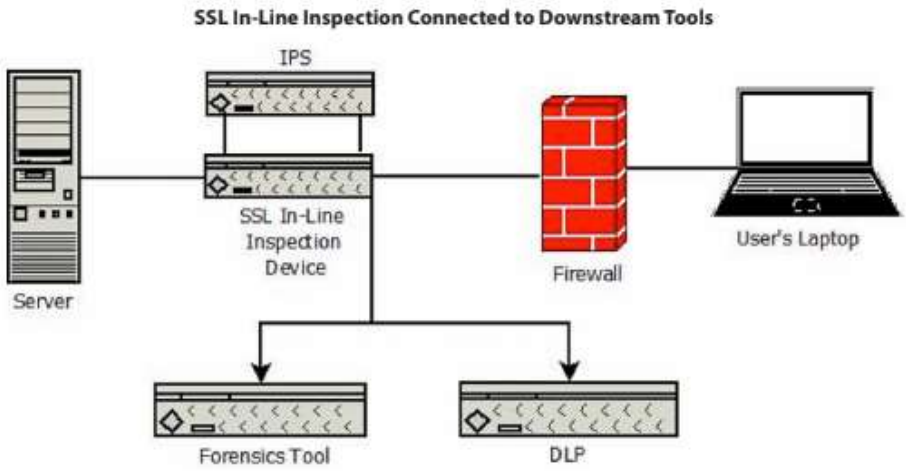

Figure 5: Inspection Working with other Security Tools for Analysis

The regulation of policies should be made for coordinating the actions that NGFW device, proxy, IDS, or SSL-inspection device takes. For instance, outbound commands that get detected through the device for inspecting SSL can be sent directly to the tool of malware analysis. In other instances, outbound SSL traffic having sensitive data related to the finance of customers can go to an audit or DLP or other compliance systems of reporting [73].

All in One

The other choice is to make use of a multifunctional gateway that can do the decryption. The benefit is a decrement in the total number of devices that a company needs to manage or purchase. The limitation is that given the drawbacks of the present processor, asking a single device to perform many tasks can decrease the performance of the network, or it can detect more threats. This is true in the case of decryption. Along with it, a security device having a built-in inspection of SSL implies writing off or tearing out the investments in present IPS, security infrastructure, secure network gateways, and making new policies of IT and to facilitate issues present around the key management and certificate authorities (CAs) [74]. Figure 4 depicts the all-in-one security of the network and configuration of the decryption of SSL through the firewall and multifunctional gateway.

Figure 6: External Traffic Inspection

4.5 Discussion

Before the formalization of the threat model, the usage scenario has been illustrated through three examples [65]. For every person in these instances, the party has been indicated in the model (RG, MB, R, or S) to which they correspond.

Example No. 1: University Network

Alice (S or R) is the student at SIGCOMM University and brings the laptop to the dorm room. However, the policy of university needs that all of the traffic of students to get monitored for illegal activity and botnet signatures through the middlebox that is running an IDS. Alice is very much worried about the computer getting infected because of the botnet software. Therefore she also wishes for this policy to get integrated into the traffic. McAfee (RG) is the service that gives attack rules to the middlebox, and it gets trusted by Alice. However, she is not comfortable with the concept of having someone she does not even know (who can access middlebox) potential capable of reading her private emails and messages at Facebook. Alice then does the installation of BlindBox HTTPS with the public key of McAfee, permitting the IDS to do scanning of traffic for signatures of McAfee, but not reading her private messages.

Example No. 2: ISP Service

Bob has two of the young children (R or S) at home, and do registration for the parental filtering with the help of ISP to filtering of traffic for the content of adult. However, Bob also read different stories in ISPs' news selling data related to the browsing of users to different marketers and wishes to do the prevention of ISP to use his data in the given way. Bob has trust over the Electronic Filtering Foundation (RG); it is non-profit and makes rulesets to do filtering. It pledges not to do the selling of the data of the user. Bob does the installation of BlindBox HTTPS over his computer through the public key of the Electronic Filtering Foundation, permitting his traffic to get scanned for the rules of EFF, but not any other data. In the given examples, Alice and Bob wish to have middleboxes within the network check to attack rules permitted by the trusted parties [66]. However, the middleboxes should not know anything else related to the traffic content. A major requirement is that an RG exists, which Bob, Alice, and MB trust with the generation of the rule. If this is not the actual case, then BlindBox cannot be used by the parties.

Anti-Example No. 1: Political Dissident

Charlie (S or R) is a political dissident who does the browsing of sensitive sites and is more concerned with monitoring government. In case, if the government coerces one of RG or MB, Charlie can have protection. However, the use of Blindbox should not be made in a setting where an attacker controls both RG and MB. In the given case, RG can make a signature for different sensitive terms. MB will then make use of these terms for matching the traffic. Therefore, if the government can do the coercion of both RG and MB together, then BlindBox should not be used by Charlie. Same as this, if the government can do the coercion of the root developers of the certificate, then Charlie should not make use of vanilla HTTPs too, as it can result in man-in-the-middle attacks over traffic [67].

Chapter 5

CONCLUSION

Since the early days of the web, the SSL protocol has been successfully provided the encryption and security with the help of which the modern commencing has become possible. Various practices and techniques have been adopted by the technicians as for bringing peace with the increasingly sophisticated attackers. Within this thesis, the importance of SSL has been discussed, SSL stands for Secure Socket Layer, it was the original name of the protocol when it was first developed in mid-1990 by the Netscape, as this company was the most famous company who was making web browsers at that time.

SSL is a system that allows sensitive information such as social security numbers, credit cards, and also the login credentials to get transmitted safely. Normally the data which is sent between the browser and the web server consists of plain text. If the hacker or the attackers can hack or intercept the data which has been sent between the browser and the web server, the hackers will become able to see and also use the particular information as it is written in plain-text form. In this scenario, SSL is a tool or the system which helps in providing security protocol, and these protocols will describe how the algorithms can be used. In this case, the SSL protocol helps in determining the variable of the encryption for both the link and also for the data provided or being transmitted. Thus in today's browsing system, all the browsers can get interacted with the secured and safe web browser as with the help of SSL protocol. Thus the browser and the server both required SSL certification as it helps in ensuring that a safe and secured connection has been developed.

Further, if discussing the SSL encryption, it will be considered important for the protection of the data while the person is using mobile phone apps, email, and browsing the internet. The SSL system helps in providing security to data of millionsof people, as it helps in securing the online data on the internet, especially when online transactions have been done among the banks by people as it helps in securing the information when data is being transmitted online. Most of the internet users are concerned about their online security with the lock icon, which only appears with the websites that havean SSL secured website. Rather than this green address bar also appeared on the website, which has an extended validation of

the SSL secured website. The website which has SSL security also comes with HTTPs rather than just HTTP.

Now the next step is to understand how SSL certification helps in establishing a secure connection. The answer will be when the browser attempt to have access to any of the website which has been secured by the SSL system the browser or either the website in result develops an SSL connection by using a process which is called SSL handshake, this connection is actually invisible and happens spontaneously and thus cannot be seen by the users. For setting up the SSL connection, there are three main keys which are considered to be essential which are

- Public
- Private
- And the session key.

Anything which has been encrypted by the public key can only be decrypted by using the private key. Thus, the process keeps ongoing as the encrypted and then decrypted with the public, and private key takes a lot of the processing power due to which they only can be used during the SSL handshake as for creating the symmetric session key. Once the system becomes able to establish a secure connection, then the session key is the one which helps in transmitting all of the secured data.

In the first step, the browser connects directly to the web browser or the website, which has been secured with the SSL (https). Further, the browser request that the server should identify itself. The next stage will send the copy to the SSL certification, which also includes the server's public key. After this step, the server checks the certification root against a list of the CAs, and thus that certification will be unexpired, unrevoked. Thus its common name became valid for the website through which the server is connected. In case if the website is secured and trusted, then only the certificate encrypts and thus further sends back a symmetric session key as by using the server’s public key. Here at the next stage, the server then decrypts the symmetric key as by using its private key and thus sends back the acknowledgment which has been encrypted with the session key as for actually stating up the encrypted session. At this stage, the server and the browser here now become able to encrypt

all of the transmitted data with the help of the session key. And thus, a journey of online transition and save web browsing starts.

The SSL protocol has been used for encrypting and for securely transmitting the data, over time, many of the improvements can be seen in this system and thus over time new and latest versions have been established and thus the version number is changed to tell the users about the change in their service, currently the system which has been used is TLSv1.2. When any of the peopleare purchasing the SSL certification from us, they are getting the SSL certification.

Several benefits can be availed by using the SSL system, such as it helps in protecting the data. The core function of this is to secure the client's information. On installing SSL, every bit of the encrypt can be secured. The second primary task of the SSL certificate is to provide authentication to the website identity verification is considered as one of the most important aspects while using this system. The SSL system helps in satisfying the PCI/DSS requirements. SSL also helps in developing a good relationship with the customers some of the people also call this function as the TTL trust transmitting software, due to its several benefits in 2018 Google made the SSL system mandatory, Google decided to flag the websites which do not have the SSL and TLC certification installed at their website. With the help of SSL, the person or the user gets the notification about not secured website to save your system and also save your personal information. Hence these all are some benefits that the users can get after the implication of the SSL system.

Further, in this thesis, different TLC interception and SSL inception will be analyzed for finding the vulnerabilities of SSL inspection methods. For doing so, the research has been conducted by using different research techniques. Here it is first important to understand how the SSL/TLS interception works. SSL interception is performed by the software on the “middlebox.” This is located between the clients and the HTTPS website, or it could be present in the machine of the client in case of any of the malware. The Middlebox software has both legitimate and also illegitimate uses, which may include the proxies or the content filters, content cachers, antivirus suits, advertising injectors, and the malware also. The Middlebox software proxy specifically relies on the root certification of its operating system, which has been previously installed. Once the connection has been established and transmitted by using the SSL and the TLS, the

connection is re-established by the proxy to the server, which acts as a middle attacker. Within the ideal deployment, the proxy's client hello mirrors, which are the TLS parameters expressed in the client's Client Hello, as for providing them the same expected parameters to the client. After this step, the proxy then becomes able to inspect the same plain text and thus become able to establish a safe and secure connection back to the client by using the installed certification as to intercept the connection between the client and the server silently.

In 2017 many of the researchers had teamed up with Google, Mozilla, and Cloudflareto measure the TLS interception within an internet-wide study. During they were doing the research team, find out that TLS interception software can easily be detected from the server's point of view by simply finding out the mismatch between the popular browsing software and the TLS handshake and also the observed handshake. Next, the team also finds out that as by analyzing the TLS handshake of the most popular interception software, they are also able to easily develop or construct the fingerprint as for some of the most widely used interception products. From all of the research done some of the most important findings were that about 5-10% of the measured HTTPS connection was actually intercepted and thus much of the software reduces the security of the end-users in a way or another with the percentage of the 97, 54 and 32% of the connection with the firefox, Cloudflare, and e-commerce are that website which has become less secure. Here the most important thing, which was investigated that the only middlebox software is the one who got Grade "A" and is bluecoat proxy software.

During the research, it has been accessed that SSL inception software tends to make a variety of mistakes some of the main mistakes are failure of validation of upstream validity as some of the software fails to validate the system certification the risk associated with this mistake is that the client does not know if they are connected with the legitimate site or not. The second mistake is some of the software is not able to convey the validation of the upstream certification to the client, and the associated risk is that the client will not be able to know if they are connected with the legitimate site or not. The system also uses layer as for conveying the validation of the certificate the associated risk with this mistakes is that not everything which accesses the data as by using the HTTPs indicates that the Human is using the web browser. Some of the SSL software also communicate before the warning, and the risk is due to this communication. The attacker will become able to view or either modify the sensitive data, and the user,asa result,will

have to go through severe circumstances. Some of the SSL software also uses the same root CA certification as they tend to install the same trusted root CA certification as for installing different software. As a result, the attacker or the hacker will become able to extract the private key from the software easily and thus will easily become able to sign in with all the sites which have been viewed recently with the universally used trusted CA certification. As by performing the web search for the "SSL inception," it has been found that there is a list of vulnerabilities that can easily affect the number of systems. Due to some limitations such as time and resource constraints, the researchers are not able to perform a test and thus are looking forward to getting feedback from the community to ascertain their status.

Thus from all of the above discussion and by using the appropriate research method it can be concluded that SSL and TLS are the software which does not provide the maximum level of end-to-end security which most of the users will expect after using the SSL system, even in some case if SSL inception is absent there exist a problem in defining that how well the browsers will become able to convey the SSL information to its users. Thus from all of the research, it is being concluded that the fact is "SSL inception" is a phrase that should be blazing the red flag showing all of the mistakes and problems associated with this system. Thus for the system developer, it is much important to re-access that whether they want to deploy the SSL inception capabilities. CERT Tapioca is the system that can be used widely to verify that SSL inspection is being used with the updated version to confirm that the user is using this system with minimum risk. In the last, it has also been accessed that the system administrator could easily contact the vendors of the SSL inception software to let them know or confirm the proper configuration option and the behavior.

Thus it can be stated that SSL is an important internet protocol that helps in encrypting the communication over the internet as between the client and the server. These protocols tend to use the certification as for establishing the identity, which helps in showing the user that the connection has been established in a secured way but with the legitimate server, which is further verified by the trusted third-party certificate authority. There are many vulnerabilities associated with this system middlebox can be used for resolving the issue. HTTPS inspection is the one that works by simply intercepting the HTTPS traffic networks and thus performing as a Man in

Middle (MiTM) attack, which can be made on the connection. Within this system, the sensitive data of the client can be transmitted to a malicious party spoofing the intended server.

For resolving all the issues which are associated with the security of the information of the data misuse the administrator must install the trusted certification on the device of the client, the browsers and the other client application can use this certification as to ensure the validation of the encrypted connection which could be created by the HTTPS inspection product. A proper set of strategies should be adopted by the administrator to make the system more secure and to remove all of the mistakes and the errors which are associated with the SSL implication. The main problem which has been identified is that the client system has no way of independently validating the HTTPs connection; the client is not able to verify the connection between itself and the HTTPS interception products. Thus the client must rely on the HTTPS validation performed by the HTTPS interception product.

Thus it is concluded and suggested that the organizations which are using the HTTPS inceptions should first identify the validation of the certificates chains and thus should pass any of the warning or either the errors to the client. Many of the organizations can use badssl.com as the process or method by determining as if their HTTPS inspection product properly validates the certificating and thus also prevents the connection to do site using by weak cryptography. Further, for making the system work more properly, proper management and upgrade versions will be required by using the single in the network device. Thus a system should be developed which will be able to decrypt the inbound and outbound traffic and thus should also be able to decrypt both inbound and outbound communication.

References

[1] Borgelt, K., Fiebig, T., Hao, S., Kruegel, C., and Vigna, G., 2018. Cloud strife: mitigating the security risks of domain-validated certificates.

[2] Brucker, A.D., and Herzberg, M., 2017. Combining the Security Risks of Native and Web Development: Hybrid Apps.

[3] Cekerevac, Z., Dvorak, Z., Prigoda, L., and Cekerevac, P., 2017. Internet of things and the man-in-the-middle attacks-security and economic risks. *MEST Journal*, *5*(2), pp.15-25.

[4] Devinney, T., 2019. Boeing: mitigating socio-political risks to the supply chain. *The Business & Management Collection*.

[5] Forman, I., 2018. Security risks of DNA testing.

[6] Gumenyuk, A., and Yanchuk, V., 2017. PAYMENT SOLUTIONS ONLINE USING CREDIT CARDS: ONLINE TRACKING VS THREATS AND SECURITY RISKS.

[7] Galindo, C.A.C., and Monge, E.L.P., 2018, June. Business intelligence: Evaluation of occupational risks using a dashboard focused on decision making. In *2018 13th Iberian Conference on Information Systems and Technologies (CISTI)* (pp. 1-4). IEEE.

[8] Mense, A., Steger, S., Sulek, M., Jukic-Sunaric, D., and Mészáros, A., 2016. Analyzing the privacy risks of mHealth applications. *Stud Health Technol Inform*, *221*, pp.41-45.

[9] Topanga, S.M.T., Zamora, M.E.C., and Gallegos, L.E.M., 2020. Appropriate Security Protocols to Mitigate the Risks in Electronic Money Management. In *Smart Trends in Computing and Communications* (pp. 65-74). Springer, Singapore.

[10] Raghavan, K., Desai, M.S., and Rajkumar, P.V., 2017. Managing cybersecurity and e-commerce risks in small businesses. *Journal of Management Science and Business Intelligence*, pp.9-15.

[11] Sample, B.E., Beyer, W.N., and Wentsel, R., 2019. Revisiting the Avian Eco-SSL for Lead: Recommendations for Revision. *Integrated environmental assessment and management*, *15*(5), pp.739-749.

[12] Safa, H.H., Souran, D.M., Ghasempour, M., and Khazaee, A., 2016. Cybersecurity of the smart grid and SCADA systems, threats, and risks.

[13] Sultana, A., and Raghuveer, K., 2017. Security Risks in Cloud Delivery Models.

[14] Wang, Y., Liu, X., Mao, W., and Wang, W., 2019, May. DCDroid: automated detection of SSL/TLS certificate verification vulnerabilities in Android apps. In *Proceedings of the ACM Turing Celebration Conference-China* (pp. 1-9).

[15] Tan, S.S.L., and Goonawardene, N., 2017. Internet health information seeking and the patient-physician relationship: a systematic review. *Journal of medical Internet research*, *19*(1), p.e9.

[16] Wojcik, G.L., Graff, M., Nishimura, K.K., Tao, R., Haessler, J., Gignoux, C.R., Highland, H.M., Patel, Y.M., Sorokin, E.P., Avery, C.L. and Belbin, G.M., 2019. Genetic analyses of diverse populations improve discovery for complex trait: n*ature*, *570*(7762), pp.514-518.

[17] Kohli, R., and Tan, S.S.L., 2016. Electronic health records: how can IS researchers contribute to transforming healthcare?. *Mis Quarterly*, *40*(3), pp.553-573.

[18] Lases, S.L., Arah, O.A., Busch, O.R., Heineman, M.J., and Lombards, M.K., 2017. The learning climate positively influences residents' work engagement and job satisfaction. *Caring for residents*, p.127.

[19] Zhang, S.S.L., Burkov, A.A., Martin, I. and Heinonen, O.G., 2019. Spin-to-charge conversion in magnetic Weyl semimetals. *Physical review letters*, *123*(18), p.187201.

[20] Joyce, S.J., Gupta, P.C., Vaidya, M.S., Alla, R., Eanuga, A.K.R., Ayalasomayajula, S., Gupta, R., Kaushal, A., Campana, V.L.J.S.K., Undavalli, P.N.V. and Nallajerla, K.R., 2019. *Enhanced communication platform and related communication method using the platform*. U.S. Patent Application 16/443,149.

[21] Joyce, S.J., Gupta, P.C., Vaidya, M.S., Alla, R., Eanuga, A.K.R., Ayalasomayajula, S., Gupta, R., Kaushal, A., Campana, V.L.J.S.K., Undavalli, P.N.V. and Nallajerla, K.R., 2018. *Enhanced communication platform and related communication method using the platform*. U.S. Patent 10,127,555.

[22] He, P., Zhang, S.S.L., Zhu, D., Liu, Y., Wang, Y., Yu, J., Vignale, G. and Yang, H., 2018. Bilinear magnetoelectric resistance as a probe of the three-dimensional spin texture in topological surface states. *Nature Physics*, *14*(5), pp.495-499.

[23] Lye, D.C., Archuleta, S., Syed-Omar, S.F., Low, J.G., Oh, H.M., Wei, Y., Fisher, D., Ponnampalavanar, S.S., Wijaya, L., Lee, L.K. and Ooi, E.E., 2017. Prophylactic

platelet transfusion plus supportive care versus supportive care alone in adults with dengue and thrombocytopenia: a multicentre, open-label, randomized, superiority trial. *The Lancet*, *389*(10079), pp.1611-1618.

[24] He, P., Walker, S.M., Zhang, S.S.L., Bruno, F.Y., Bahrami, M.S., Lee, J.M., Ramaswamy, R., Cai, K., Heinonen, O., Vignale, G. and Baumberger, F., 2018. Observation of out-of-plane spin texture in a SrTiO 3 (111) two-dimensional electron gas. *Physical review letters*, *120*(26), p.266802.

[25] Sokol, A.M., Uszczynska-Ratajczak, B., Collins, M.M., Bazala, M., Topf, U., Lundegaard, P.R., Sugunan, S., Guenther, S., Kuenne, C., Graumann, J. and Chan, S.S., 2019. Loss of the Mia40a oxidoreductase leads to hepato-pancreatic insufficiency in zebrafish (vol 14, e1007743, 2018). *PLOS GENETICS*, *15*(1).

[26] Hansson, A.A., Wenger, A.A., Henriksson, H.H.B., Li, S.S., Johansson, B.B., and Brisby, H.H., 2017, May. INVESTIGATION OF INFLUENCE BY DIFFERENT HYDROGEL FEATURES AND GROWTH HORMONE ON THE DIRECTION OF HUMAN MESENCHYMAL STEM CELLS INTO THE CHONDROGENIC LINEAGE: GP046. In *Spine Journal Meeting Abstracts* (p. 188). LWW.

[27] Sokol, A.M., Uszczynska-Ratajczak, B., Collins, M.M., Bazala, M., Topf, U., Lundegaard, P.R., Sugunan, S., Guenther, S., Kuenne, C., Graumann, J. and Chan, S.S., 2018. Loss of the Mia40a oxidoreductase leads to hepato-pancreatic insufficiency in zebrafish. *PLoS genetics*, *14*(11).

[28] Peppin, S.S.L., 2019. Theory of tracer diffusion in concentrated hard-sphere suspensions. *Journal of Fluid Mechanics*, *870*, pp.1105-1126.

[29] Xiao, Y., Li, M., Chen, S., and Zhang, Y., 2017, October. Stacco: Differentially analyzing side-channel traces for detecting SSL/TLS vulnerabilities in secure enclaves. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security* (pp. 859-874).

[30] Weerasinghe, T.D.B., and Dissanayake, C., 2018. A research study: Usage of RC4 stream cipher in SSL configurations of web servers used by Sri Lankan Financial Institutes. *International Journal of Cyber-Security and Digital Forensics*, *7*(2), pp.111-119.

[31] Cho, S., Choi, H., Heo, G., Cho, S., and Kim, Y.G., 2018. A System for SSL/TLS Vulnerability Detection of Servers. *Journal of the Korea Institute of Information Security and Cryptology*, *28*(1), pp.145-153.

[32] Wang, Y., Liu, X., Mao, W., and Wang, W., 2019, May. DCDroid: automated detection of SSL/TLS certificate verification vulnerabilities in Android apps. In *Proceedings of the ACM Turing Celebration Conference-China* (pp. 1-9).

[33] Weerasinghe, T.D.B., and Dissanayake, C., 2018, October. Usage of RC4 Cipher in SSL Configurations in Web Portals of Sri Lankan Banking/Non-Banking Financial Institutes and Awareness Levels of Relevant Staff About It. In *2018 National Information Technology Conference (NITC)* (pp. 1-6). IEEE.

[34] Liu, A., Alqazzaz, A., Ming, H., and Dharmalingam, B., 2019. IoTVerif: Automatic Verification of SSL/TLS Certificate for IoT Applications. *IEEE Access*.

[35] Zhao, R., Li, X., Xu, G., Feng, Z., and Hao, J., 2016, November. E-SSL: An SSL Security-Enhanced Method for Bypassing MITM Attacks on Mobile Internet. In *International Workshop on Structured Object-Oriented Formal Language and Method* (pp. 101-120). Springer, Cham.

[36] Kumar, R., 2019. *Research methodology: A step-by-step guide for beginners*. Sage Publications Limited.

[37] Ledford, J.R., and Gast, D.L., 2018. *Single case research methodology: Applications in special education and behavioral sciences*. Routledge.

[38] Bresler, L., and Stake, R.E., 2017. Qualitative research methodology in music education. *Critical Essays in Music Education* (pp. 113-128). Routledge.

[39] Humphries, B., 2017. *Re-thinking social research: anti-discriminatory approaches in research methodology*. Routledge.

[40] Wiek, A., and Lang, D.J., 2016. Transformational sustainability research methodology. *Sustainability science* (pp. 31-41). Springer, Dordrecht.

[41] Mahajan, H.K., 2018. Qualitative research methodology in social sciences and related subjects. *Journal of Economic Development, Environment, and People*, *7*(1), pp.23-48.

[42] Attia, M., and Edge, J., 2017. Be (com) ing a reflexive researcher: a developmental approach to research methodology—o*pen Review of Educational Research*, *4*(1), pp.33-45.

[43] Taherdoost, H., 2016. Sampling methods in research methodology; how to choose a sampling technique for research. *How to Choose a Sampling Technique for Research (April 10, 2016)*.

[44] Ørngreen, R., and Levinsen, K., 2017. Workshops as a Research Methodology. *Electronic Journal of E-learning*, *15*(1), pp.70-81.

[45] Clandinin, D.J., Cave, M.T., and Berendonk, C., 2017. Narrative inquiry: a relational research methodology for medical education. *Medical Education*, *51*(1), pp.89-96.

[46] Page, D., Gilroy, M., Hurrion, E., Clark, L., and Wilkinson, S., 2017. Optimizing early neonatal nutrition using translational research methodology. *Nutrition & Dietetics*, *74*(5), pp.460-470.

[47] Cuervo-Cazurra, A., Mudambi, R., Pedersen, T., and Piscitello, L., 2017. Research methodology in global strategy research. *Global Strategy Journal*, *7*(3), pp.233-240.

[48] Goldberg, S.B., Tucker, R.P., Greene, P.A., Simpson, T.L., Kearney, D.J. and Davidson, R.J., 2017. Is mindfulness research methodology improving over time? A systematic review. *PloS one*, *12*(10).

[49] Briggs, A., and Coleman, M., 2019. Research Methodology in Educational Leadership and Management. In *Oxford Research Encyclopedia of Education*.

[50] Basias, N., and Pollalis, Y., 2018. Quantitative and qualitative research in business & technology: Justifying a suitable research methodology. *Review of Integrative Business and Economics Research*, *7*, pp.91-105.

[51] Daniel, B.K., and Harland, T., 2017. *Higher education research methodology: A step-by-step guide to the research process*. Routledge.

[52] King, K.A., and Mackey, A., 2016. Research methodology in second language studies: Trends, concerns, and new directions. *The Modern Language Journal*, *100*(S1), pp.209-227.

[53] Hickson, H., 2016. Becoming a critical narrative using critical reflection and narrative inquiry as a research methodology. *Qualitative social work*, *15*(3), pp.380-391.

[54] Venable, J.R., Pries-Heje, J., and Baskerville, R., 2017. Choosing a Design Science Research Methodology. In *28th Australasian Conference on Information SystemsIEEE/ACIS International Conference on Computer and Information Science*. The University of Tasmania.

[55] Yuan, X., Wang, X., Lin, J., and Wang, C., 2016, April. Privacy-preserving deep packet inspection in outsourced middleboxes. In *IEEE INFOCOM 2016-The 35th Annual IEEE International Conference on Computer Communications* (pp. 1-9). IEEE.

[56] Sherry, J., Lan, C., Popa, R.A., and Ratnasamy, S., 2015, August. Blindbox: Deep packet inspection over encrypted traffic. In *Proceedings of the 2015 ACM Conference on Special Interest Group on Data Communication* (pp. 213-226).

[57] Fan, J., Guan, C., Ren, K., Cui, Y. and Qiao, C., 2017. Soapbox: Safeguarding privacy during deep packet inspection at a middlebox. *IEEE/ACM Transactions on Networking*, *25*(6), pp.3753-3766.

[58] Durumeric, Z., Ma, Z., Springall, D., Barnes, R., Sullivan, N., Bursztein, E., Bailey, M., Halderman, J.A. and Paxson, V., 2017, February. The Security Impact of HTTPS Interception. In *NDSS*.

[59] Han, J., Kim, S., Ha, J., and Han, D., 2017, August.Sexx-box: Enabling visibility on encrypted traffic using a secure middlebox module. In *Proceedings of the First Asia-Pacific Workshop on Networking* (pp. 99-105).

[60] Choffnes, D., Gill, P., and Mislove, A., 2017, September. An empirical evaluation of deployed dpi middleboxes and their implications for policymakers. In *Proc. of TPRC*.

[61] Wang, C., Yuan, X., Cui, Y. and Ren, K., 2017. Toward secure outsourced middlebox services: Practices, challenges, and beyond. *IEEE Network*, *32*(1), pp.166-171.

[62] Guo, Y., Wang, C., and Jia, X., 2018, May. Enabling secure and dynamic deep packet inspection in outsourced middleboxes. In *Proceedings of the 6th International Workshop on Security in Cloud Computing* (pp. 49-55).

[63] Jackson, E.J., Walls, M., Panda, A., Pettit, J., Pfaff, B., Rajahalme, J., Koponen, T., and Shenker, S., 2016. Soft flow: A middlebox architecture for the open switch. In *2016 {USENIX} Annual Technical Conference ({USENIX}{ATC} 16)* (pp. 15-28).

[64] Langley, A., Riddoch, A., Wilk, A., Vicente, A., Krasic, C., Zhang, D., Yang, F., Kouranov, F., Swett, I., Iyengar, J. and Bailey, J., 2017, August. The quick transport protocol: Design and internet-scale deployment in *Proceedings of the Conference of the ACM Special Interest Group on Data Communication* (pp. 183-196).

[65] Yamaguchi, F., Maier, A., Gascon, H., and Rieck, K., 2015, May. Automatic inference of search patterns for taint-style vulnerabilities. In *2015 IEEE Symposium on Security and Privacy* (pp. 797-812). IEEE.

[66] Jadhav, D.B., Sanap, S.K., Ghuge, R.C. and Somnath, D., Analyzing & Defining Web Application Vulnerabilities With Dynamic Analysis And Web Mining.

[67] Vastrad[1], S.R., Madani, M. and Hiremath, V., Detection of SQL Injection Vulnerability For Web-Based Applications.

[68] Watanabe, T., Akiyama, M., Kanei, F., Shioji, E., Takata, Y., Sun, B., Ishi, Y., Shibahara, T., Yagi, T. and Mori, T., 2017, May. Understanding the origins of mobile app vulnerabilities: A large-scale measurement study of free and paid apps. In *2017 IEEE/ACM 14th International Conference on Mining Software Repositories (MSR)* (pp. 14-24). IEEE.

[69] Huang, L.S., Rice, A., Ellingsen, E., and Jackson, C., 2014, May. Analyzing forged SSL certificates in the wild. In *2014 IEEE Symposium on Security and Privacy* (pp. 83-97). IEEE.

[70] Bates, A., Pletcher, J., Nichols, T., Hollembaek, B., Tian, D., Butler, K.R., and Alkhelaifi, A., 2014, November. Securing SSL certificate verification through dynamic linking. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security* (pp. 394-405).

[71] Watanabe, T., Akiyama, M., Kanei, F., Shioji, E., Takata, Y., Sun, B., Ishi, Y., Shibahara, T., Yagi, T. and Mori, T., 2017. A study on the vulnerabilities of mobile apps associated with software modules. *arXiv preprint arXiv:1702.03112*.

[72] Costin, A., Zaddach, J., Francillon, A., and Balzarotti, D., 2014. A large-scale analysis of the security of embedded firmware. In *23rd {USENIX} Security Symposium ({USENIX} Security 14)* (pp. 95-110).

[73] Junior, D.M., Melo, L., Lu, H., Amorim, M., and Prakash, A., 2019, May. A Study of Vulnerability Analysis of Popular Smart Devices Through Their Companion Apps. In *2019 IEEE Security and Privacy Workshops (SPW)* (pp. 181-186). IEEE.

[74] Sun, Y., Sun, L., Shi, Z., Yu, W. and Ying, H., 2019, March. Vulnerability Finding and Firmware Association in Power Grid. In *2019 Fifth Conference on Mobile and Secure Services (MobiSecServ)* (pp. 1-5). IEEE.