International Journal of Progressive Sciences and Technologies (IJPSAT)
ISSN: 2509-0119.
© 2025 Scholar AI LLC.
https://ijpsat.org/

Vol. 49 No. 1 February 2025, pp. 507-515

Study And Analysis Of The Implementation Of Ssl On The Indonesian Air Force Recruitment Website

Wikik Andhitias Sutrisno[1], Teddy Mantoro [2]

[1]Cyber Defense Engineering
Republic of Indonesia Defense University
Jakarta, Indonesia
wikikandhitias@gmail.com

[2]Faculty of Science and Defense Technology
Republic of Indonesia Defense University
Jakarta, Indonesia
teddy.mantoro@sampoernauniversity.ac.id

Abstract— Security related to website data defense is becoming increasingly important because more and more cybersecurity threats can attack websites and steal confidential and sensitive data. One solution to secure against this threat is to implement SSL security on the Indonesian Air Force website. In this study, SSL implementation will be carried out on the website. Test Method Using Quality of Service, for network testing tools, use Wireshark. The purpose of this study was to determine the impact of using Qos parameters on websites when SSL was implemented and before SSL was implemented. Based on the test results with the QoS parameters with Wireshark, it obtained an average response time value of 0.508 before implementation and obtained a response time of 0.516 ms after implementation. SSL. Based on the results of tests conducted using SSL is better done to secure sensitive information data such as phishing attacks, and MITM from unauthorized parties.

Keywords— Secure Sockets Layer, QoS, Domain Validation, Response Time, Wireshark.

I. Introduction

In today's Internet Advancement, security related to defense website data is becoming increasingly important as more and more cybersecurity threats can attack websites and steal confidential and sensitive data.

To overcome these threats, many efforts are being made to improve data security on defense websites. One of the efforts made is to use encryption technology such as SSL (Secure Sockets Layer) or TLS (Transport Layer Security) to protect information sent between the website server and the user [1][2].

SSL (Secure Sockets Layer) is one of the network security technologies that provides data encryption and authentication to protect communication between the user's web browser and the web server. SSL provides a secure channel for transferring sensitive information such as credit card numbers, login information, and other confidential information over the Internet. SSL works by ensuring that the information transferred between the user's web browser and the web server is encrypted so that it can only be read by legitimate parties [1].

By using SSL, defense websites can ensure that confidential information sent and received can only be accessed by legitimate parties. In addition, SSL also helps avoid attacks such as Man-in-the-Middle (MITM) and phishing, where attackers try to obtain sensitive information by posing as legitimate parties.

In this study, a method will be implemented to secure the data integrity of the Defense Website using Secure Socket Layer. This SSL will be applied to Apache-based web server hosting. This Webserver will forward access that has been protected by the Secure Socket Layer publicly from the Server to the Client.

II. Background

A. Related Work

a. Quality Of Service

Quality of Service (QoS) is used to measure performance and quality levels on IP networks to provide a guaranteed level of performance on different services. QoS parameters commonly used for measuring the performance of a network include packet loss, delay, throughput, and jitter [3].

Packet Loss is a parameter that shows the total number of packets lost or not reaching their destination. This can happen because there is an overload on the network [4].

The standards regarding packet loss of a network are described in TIPHON shown in Table 1.

Table 1. Packet Loss

Category	Packet Loss
Very good	0 %
Good	3 %
Keep	15 %
Signs	25 %

Delay is one of the QoS parameters that indicates the time it takes to reach a packet and the distance from source to destination. Some of the things that affect delay are distance, hardware, and congestion [5]. The following standard delay has been agreed upon in the TIPHON rules shown in Table 2.

Table 2. Delay

Category	Delay
Very good	< 150 ms
Good	150 ms – 300 ms
Keep	300 ms – 450 ms
Signs	> 450 ms

Throughput is a QoS parameter that shows an average speed of actual bandwidth, measured by a certain unit of time under certain network conditions to send packets of a certain size as well [6]. The throughput result is taken from the number of data packets sent divided by the amount of time it takes to send the data packets.

Table 3. Troughput

Category	**Throughput**
Very good	> 2.1 Mbps
Good	700 – 1200 kbps
Keep	338 – 700 kbps
Signs	0 – 338 kbps

B. Air Force Recruitment Website

The https://diajurit.tni-au.mil.id/ website is one of the websites managed by Disminpersau, where the website is used to handle online member recruitment. The website can be accessed by all people who will or have the intention to register with the Indonesian Air Force

On this recruitment website, there is sensitive data related to login information, and recruitment data such as diplomas, photo ID cards, etc. Information like this requires security such as the use of SSL to ensure information is maintained safely and not easily accessed by irresponsible parties.

C. Secure Socket Layer

SSL (Secure Sockets Layer) is one of the network security technologies that provide data encryption and authentication to protect communication that occurs between the browser and the web server. SSL will provide a secure channel for transferring sensitive information such as credit cards, over the internet. SSL works by ensuring that the information transferred between the web browser and the web server is encrypted so that it can only be read by legitimate parties [7]-[9].

SSL allows sensitive information such as credit card data, usernames, passwords, and important information to be transmitted from server to client or vice versa securely because the data sent will be encrypted (encrypted). The Web server must have an SSL certificate before establishing a connection over SSL. When activating the SSL protocol on a web server, you are asked to be able to answer a question that will determine an identity. The question will ask about information and the company. once SSL certification is requested, the web server will generate two private keys, a cryptographic key, and a public key here is the flow of the Encryption Process Using SSL:

a. Client /Browser requests SSL connection (SSL Hello)

b. The server replies to the request by sending an SSL Certificate containing the public key.

c. The client receives and validates the validity of the certificate (checking the signing CA, validity period, owner, etc.)

d. The client creates a Symmetric Encryption key (often called a session key) and encrypts the session key with the public key contained in the certificate and sends it to the server.

e. The server decrypts with the private key the data from the client containing the symmetric session key and uses the key to send the data from the server to the client. SSL connection is established.

D. Types of SSL

SSL has its type and character, the types of SSL are:

a. Domain Validation (DV) SSL Certificate. Domain Validation SSL is considered the cheapest and easiest SSL because it is only validated via email. Indonesian web hosting users must have several requirements if they want to apply for a Domain Validated SSL Certificate, including you are required to have the same email as the domain data in WHOIS [10][11].

b. Organization Validation (OV) SSL Certificate This SSL is used for validating the organization, or business entity behind the registered domain name. For the OV verification process to run smoothly, Indonesian cheap hosting users must have several requirements, such as preparing several supporting documents that acknowledge the legality of your business or organization and following state law.

c. Extended Validation (EV) SSL Certificate. The last type of SSL that Indonesian web hosting users need to know is the Extended Validation (EV) SSL Certificate, which is the highest validation standard for an organization or company. This type of SSL is categorized as the most premium because it is considered to provide its prestige value on a website.

A feature of a site that implements an Extended Validation (EV) SSL Certificate is that there is a green bar with the name of a company in it. Then, this certification also supports all types of browsers and uses the highest current security standards.

E. Lets Encrypt

Let’s Encrypt is one of the service providers related to SSL/TLS certificates based on Open Source. Using the services of Let's Encrypt allows websites to use a secure connection with SSL/TLS encryption which allows data transferred from the browser to the website server to be encrypted and inaccessible to unauthorized parties. Let's Encrypt also uses certificate automation protocols, which allow easy and automatic installation and renewal of SSL/TLS certificates. This makes it easier for website owners to renew SSL/TLS certificates regularly and keep their websites secure. In this study, the authors used SSL from the Let’s Encrypt service provider to secure recruitment sites [6].

F. Apache Web Server

Apache Web Server functions as a web service provider by delivering HTML files or other web content to users over HTTP or HTTPS protocols. Apache Web Server can be used on various operating system platforms such as Linux, Windows, Mac OS, and Unix [10]. Apache Web Server has a very wide range of features and capabilities, such as support for various programming languages such as PHP, Perl, Python, Ruby, and more. Apache Web Server also provides the ability to configure security levels, manage user access, and manage server configuration very easily. In addition, Apache Web Server has features to manage multiple websites from a single server, thus allowing users to save costs and time. Apache Web Server can also be used to run web applications such as Content Management Systems (CMS) or discussion forums.

G. Web Server

A web server is a software that provides services in the form of data. Webserver Serves to receive HTTP or HTTPS requests from clients or we are familiar with web browsers (Chrome, Firefox) [7]. Then it will send a response to the request to the client in the form of a web page. The following are the types of web servers:

a. Apache Web Servers. The most popular and most widely used web server by most people, namely the Apache type. At first, Apache was designed to fully support the UNIX operating system. Apart from being quite easy to implement, Apache also has several supporting programs to provide complete services, such as PHP, SSI, and access control, including TCP and UDP mod security [12].

b. Web Server Nginx. One of Apache's superior competitors is Nginx. Nginx is known to be able to serve all kinds of requests, such as requests at very high traffic levels. Nginx is indeed superior in terms of quality, speed, and in terms of performance.

c. Web Server IIS. Web server IIS (Internet Information Services) adalah server web yang bekerja pada jenis protokol seperti DNS, TCP/IP, atau beragam perangkat lunak lainnya yang berguna untuk merangkai sebuah situs.

d. Web Server Lighttpd. German programmer has created a web server based on open source to support Linux and Unix systems. When viewed in terms of advantages, this web server has several advantages based on the additional features available. Such as FastCGI, Output-Compression, Fast CGI, and URL Writing. If you use the Lighttpd web server, you will experience faster and more effective performance.

III. Method And Desain

The network design method used in this study is PPDIOO (Prepare, Plan, Design, Implement, Operate, and Optimize) also known as network lifecycle is a research method developed by Cisco System [8]. The following are the stages of research using PPDIOO:

A. Prepare

Prepare is the initial stage in the research process to compile a work plan so that the research can be properly organized. This stage concerns matters related to the analysis of the subject matter such as problems that arise, analysis of research needs in SSL Implementation on Apache Web Server, both in terms of hardware or software, and analysis of the topology of the network to be built.

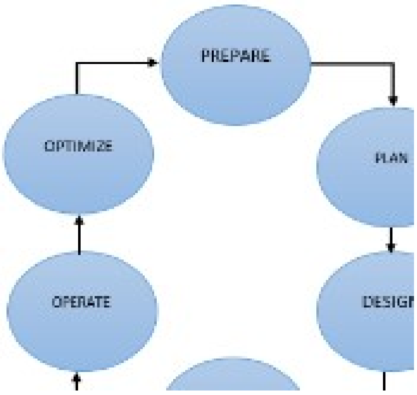


Figure 1. PPDIOO method

B. Plan

The The plan is a network planning stage that is made both in terms of hardware and software needed and test scenarios that will be carried out in research. The following flowchart diagram explains the stages of design:

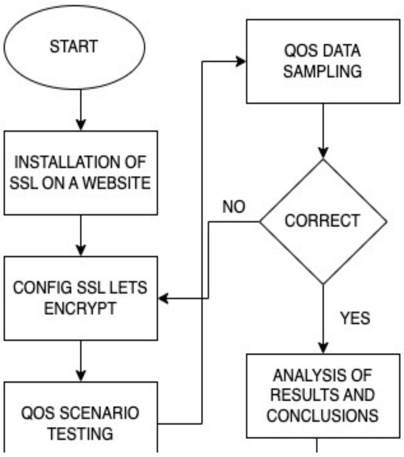


Figure 2. System Flowchart

The test scenario carried out in this study is QoS testing with the Response Time parameter.

C. Design

Design is the stage for making research designs that will be carried out following the design of the SSL implementation system on the website in figure 3:

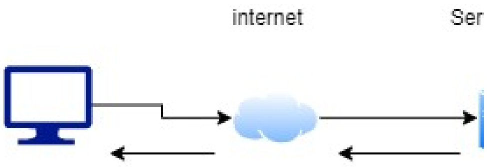


Figure 3. System Design

D. Implement

At this stage, the implementation is carried out according to the system design that has been made before. Starting from server configuration, SSL implementation, and use of the Let's Encrypt service.

E. Operate

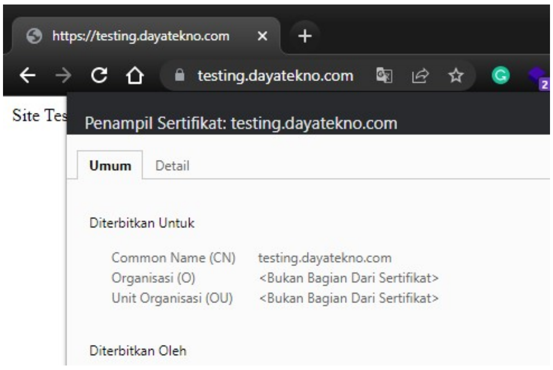
This stage is done for scenario experiments that have been prepared. Testing experiments were conducted using Wireshark tools.

F. Optimize

At this stage, an analysis of the operation stage is carried out. This stage is necessary to determine whether to require a system redesign if there are too many problems with SSL implementation.

G. Result And Discussion

The implementation has been successfully carried out. The next stage is the testing process using the response time parameter in Quality of Service. Testing is carried out to stem the response time before SSL is applied and after SSL implementation. The parameter used in this study is the response parameter. In the picture



Penampil Sertifikat: testing.dayatekno.com

Diterbitkan Untuk

Common Name (CN)	testing.dayatekno.com
Organisasi (O)	<Bukan Bagian Dari Sertifikat>
Unit Organisasi (OU)	<Bukan Bagian Dari Sertifikat>

Diterbitkan Oleh

Figure 4. SSL Implementation Results

Response Time or delay is the amount of time used to travel the distance from source to destination. Responsiveness can be affected by distance, hardware, or long processing time [13][14].

From responsive testing conducted using the Wireshark application, the average results were obtained which had a slight difference [15]. In testing before SSL implementation, the average response time of 0.508 ms is shown in Table 4. Meanwhile, in testing after the implementation of SSL on the Air Force Recruitment website, an average response time of 0.516 ms was obtained which is shown in Table 5.

Table 4. Testing Before Implementation

Testing	Response time
Testing 1	0,506 ms
Testing 2	0,506 ms
Testing 3	0,512 ms
Average	0,508 ms

Table 5. Testing After SSL Implementation

Testing	Response time
Testing 1	0,518 ms
Testing 2	0,518 ms
Testing 3	0,513 ms
Average	0,516 ms

From the explanation and explanation in Section 4, the results of the Quality of Service analysis at the time before SSL implementation and after SSL implementation, for example in a Mobile ad hoc Network (MANET) or Cloud Video Surveillance System [16-17]. The measurement process uses the Response time/Delay parameter in QoS. The following are some analysis results:

- Implementation of SSL has been successfully carried out on the TNI AU recruitment website.
- The results of the Response time test obtained values that did not have a significant difference.
- The HTTPS protocol using SSL is better used to secure data or information that is private.

IV. Conclusion

Website Security Implementation using SSL has been successfully implemented on the TNI AU recruitment site. Based on the tests carried out, the use of SSL is better done to secure sensitive information data such as phishing attacks, and MITM from unauthorized parties. The use of SSL does not significantly affect the responsiveness of the website. So that the website can be accessed quickly and has SSL-based data security.

With the application of SSL, it is hoped that it can anticipate data leaks so that the information security of the personal data of prospective applicants can be protected. suggestions for future study are the implementation of OLSR2 for optimizing the VoIP system, optimizing resources to extend the lifetime of each VoIP node, and optimizing the use of the 2.4Ghz channel for the system

References

[1] Purchina, O. & Poluyan, A. & Fugarov, Dmitry. (2023). Improving the security level of the information system using the SSL protocol. E3S Web of Conferences. 371. 10.1051/e3sconf/202337103067

[2] Mantoro, T., Ayu M.A., Borovac A., Zuhra A. (2012). IPv4 and IPv6 Server Designs: The Sockets Performance, Proceedings of the 3rd International Conference on Multimedia Computing and Systems, Tangier, Morocco. pp.1-5.

[3] Syahab, A. (2023). Analisis Audit Keamanan Informasi Website Menggunakan Metode Network Mapper Dan Qualys SSL. Jurnal Manajemen Informatika dan Sistem Informasi. 6. 39-47. 10.36595/misi.v6i1.742.

[4] Rahmat M.F.E. Rohadi, I. Siradjuddin, and F. Chrissandy, (2021). "Study and Analysis of Network Topology Performance Using Wireless Distribution System Technology", JITeCS, vol. 6, no. 2, pp. 130–136.

[5] Manescu, V. & Alexandra, N. & Barbu, A. & Rodica, G. & Militaru, G.. (2021). Analysis Of Ssl Certificates Trends And Extended Validation Of Ssl Usage For E-Commerce Websites And Internet Things. UPB Scientific Bulletin, Series C: Electrical Engineering. 83.

[6] Josh Aas, Richard Barnes, Benton Case, Zakir Durumeric, Peter Eckersley, Alan Flores-López, J. Alex Halderman, Jacob Hoffman-Andrews, James Kasten, Eric Rescorla, Seth Schoen, and Brad Warren. (2019). Let's Encrypt: An Automated Certificate Authority to Encrypt the Entire Web. In Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security (CCS '19). Association for Computing Machinery, New York, NY, USA, 2473–2487. https://doi.org/10.1145/3319535.3363192.

[7] Chandra, A. Y. (2019). Analisis Performansi Antara Apache & Nginx Web Server Dalam Menangani Client Request. *Jurnal Sistem Dan Informatika (JSI)*, *14*(1), 48-56. https://doi.org/10.30864/jsi.v14i1.248.

[8] Yuliana, D. , Mogi, I. K. A. (2020). Computer Network Design Using PPDIOO Method With Case Study of SMA Negeri 1 Kunir. JELIKU (Jurnal Elektronik Ilmu Komputer Udayana), [S.l.], v. 9, n. 2, p. 235-240,. ISSN 2654-5101. Available at:

<https://ojs.unud.ac.id/index.php/JLK/article/view/64496>. Date accessed: 19 Oct. 2023. doi: https://doi.org/10.24843/JLK.2020.v09.i02.p10.

[9] Azamuddin, W.M.H.; Hassan, R.; Aman, A.H.M.; Hasan, M.K.; Al-Khaleefa, A.S. (**2020).** Quality of Service (QoS) Management for Local Area Network (LAN) Using Traffic Policy Techniques to Secure Congestion. *Computers*, 39. https://doi.org/10.3390/computers9020039.

[10] E Rohadi et al. (2020). Cluster implementation on mini Raspberry Pi computers using Round Robin Algorithm J. Phys.: Conf. Ser. 1450 012068.

[11] M. A. Bahari, P. H. Trisnawan, and R. A. Siregar, (2018). "Analysis of AODV (Ad Hoc On-Demand Distance Vector) and AOMDV (Ad Hoc On-Demand Multipath Distance Vector) Protocol Performance Against Active Attacks on the MANET Network (Mobile Ad Hoc Network), " vols. 3, no. 4, p. 3235–3244.

[12] Mantoro T., N.A Aziz, N. D. M. Yusoff, N. A. A. Talib, (2013). Log Visualization of Intrusion and Prevention Reverse Proxy Server Against Web Attacks, International Conference on Informatics and Creative Multimedia 2013 (ICICM'13), Kuala Lumpur, pp. 3-6.

[13] Guo Y., Cao Z. & Yang W., Xiong G. (2018). A Measurement and Security Analysis of SSL/TLS Deployment in Mobile Applications. 189-199. 10.1007/978-3-319-66625-9_19.

[14] K. R. BORUT, (2017). "Analysis of Blackhole Attack Detection on the Network Manet (Mobile Ad-Hoc Network) Using Genetic Algorithm Method Dan Ant Colony Optimization," vol. XII, p. 35–44.

[15] llyan, D. F., Nasution, S. M., and Siswo, A. (2016). Real-time video surveillance data security using video encryption algorithm. e-Proceedings of Engineering Vol. 3, No. 2.

[16] S. N. M. P. Simamora, (2015). "Dynamic Topology Design Randomly in Mobile Ad-Hoc Network with a Modeling Approach," Simetris J. Tech.Mechanical, Electrical and Computing Sciences., vol. 6, no. 1, p. 119.

[17] Yong-Hua, X., Wan S.Y., He Y., dan Su D. (2013). Design and Implementation of a Prototype Cloud Video Surveillance System. Journal of Advanced Computational Intelligence and Intelligent Informatics Vol. 18, No. 1.