|Jurnal Jaringan Komputer dan Keamanan |JJKK|Vol. 6| No. 1|Feb|Year 2025|
This is an Open Access article, published by Institute of Information Technology and Social Science (IITSS), Indonesia

Analysis of Hotspot Network Security Using the OpenSSL (Secure Socket Layer) Security Method at the PTPN 7 Musi Landas Plantation Office

Al Harits Athif

Abstract

For wireless network security on access point devices, the security method often used is the WEP/WPA/WPA2 method. Almost all wireless network users, on average, implement their access point devices using this method. This method is well known for its ability to secure wireless network security. However, the WEP/WPA/WPA2 method can still be penetrated by hacking software using the brute-force attack and dictionary methods. This hacking software is widely available on the internet. The next weakness is that this method only uses a password when connecting to the access point device. Consequently, the password can easily spread if one user gives their password to another user, and it is easily known by other users, and so on. The SSL (Secure Socket Layer) method has been widely used for securing websites that require a high level of security, such as banking websites, hosting, online buying and selling, and so forth, which usually use the HTTPS (Hyper Text Transfer Protocol Secure) protocol. Implementation of a gateway server functions as an internet router on both wired and wireless networks. This is a solution that can help communication between computers and a hotspot internet security system. Users will first log in by entering a user name and password when accessing the internet using the Secure Socket Layer (SSL) security method.

Keywords

Security, Hotspot, Server, SSL, HTTPS

Article History

Received 02 December 2024
Accepted 21 February 2025

How to Cite

Athif, A.H. (2025). Analysis of Hotspot Network Security Using the OpenSSL (Secure Socket Layer) Security Method at the PTPN 7 Musi Landas Plantation Office. ***Jurnal Jaringan Komputer dan Keamanan,*** *6*(1), 1-8.

[1*] Universitas Bina Darma*,* Indonesia, Corresponding email: 16142024P@student.binadarma.ac.id

Introduction

The rapid development of wireless communication technology has profoundly transformed the way individuals and organizations access information and interact digitally. Wireless Local Area Network (WLAN) technology, commonly referred to as Wi-Fi, has become one of the most widely adopted innovations in modern networking. Unlike traditional wired networks, WLAN eliminates the need for physical cables, allowing users to connect to networks seamlessly through radio frequency transmission. This capability provides a high level of flexibility, mobility, and convenience, enabling users to stay connected anywhere within the coverage area. The adoption of WLAN continues to increase globally, with its presence now ubiquitous in public spaces such as restaurants, shopping malls, offices, campuses, and schools, offering ease of communication and collaboration in various contexts.

The growing popularity of WLAN is driven not only by its practical advantages but also by its role in supporting the digital transformation of work environments. Wireless networks allow organizations to expand their operational efficiency by enabling dynamic connectivity and resource sharing. However, despite these advantages, wireless networks are inherently more vulnerable to security threats than wired systems because data is transmitted through open airwaves that can be intercepted by unauthorized users. Without adequate security measures, WLAN users are exposed to risks such as data theft, unauthorized access, and network intrusion. Therefore, robust security mechanisms are required to ensure the confidentiality and integrity of information transmitted through wireless systems.

At the PTPN 7 Musi Landas Plantation Office, the wireless network infrastructure currently employs the WEP, WPA, and WPA2 encryption methods as its primary security protocols. These protocols have been the industry standard for years and are generally considered reliable for basic wireless protection. However, advances in hacking techniques and password-cracking tools have significantly reduced their effectiveness. Methods such as brute-force attacks and dictionary-based exploits can now penetrate these encryption protocols relatively easily using freely available software tools. Furthermore, these security systems rely solely on shared passwords, which are often circulated among users, thereby increasing the risk of password leakage and unauthorized network access.

The limitations of conventional WLAN security methods highlight the need for an enhanced wireless hotspot protection system that offers stronger authentication and data encryption mechanisms. To address these issues, this research proposes the implementation of the Secure Socket Layer (SSL) method as an alternative security framework. SSL is a cryptographic protocol designed to secure communications over a network by encrypting data transmitted between clients and servers. It is widely used to safeguard sensitive transactions on websites—such as online banking, e-commerce, and cloud-based services—through the HTTPS (Hypertext Transfer Protocol Secure) standard. The adoption of SSL in wireless network environments ensures that user credentials and transmitted data remain confidential and tamper-proof.

In the proposed system, an SSL-enabled gateway server will be implemented to function as an internet router for both wired and wireless connections within the PTPN 7 Musi Landas network. This gateway acts as a central authentication point, ensuring that users must first log in using a valid username and password before gaining internet access. All login requests and data exchanges between users and the server are encrypted using SSL, thereby preventing packet interception and session hijacking. The use of SSL thus introduces an additional layer of security that is both scalable and compatible with existing network infrastructure.

In summary, the application of SSL-based security in the wireless hotspot network of PTPN 7 Musi Landas aims to strengthen protection against unauthorized access and cyber threats. By combining secure authentication, data encryption, and centralized gateway management, the proposed system not only enhances network integrity and reliability, but also aligns with best practices in modern information security. This study therefore contributes to developing a more secure and efficient WLAN model that can be implemented in corporate and institutional environments facing similar network security challenges.

Methodology

The research method to be used is the action research method. According to Kock (2007:45), the Action Research Method is action-oriented research. The action research method is participatory and collaborative. This means the research is conducted by the researcher through action research. Action research is divided into several stages that form a cycle.

participants First Stage (Diagnosing)

In this stage, the researcher identifies the problem in the wireless network at the PTPN 7 Musi Landas Plantation Office. For wireless network security on the access point device, the security method still used is the WEP/WPA/WPA2 method. This method is known to be good in terms of securing wireless networks. However, the WEP/WPA/WPA2 method can still be penetrated by hacking/intrusion software. This application is widely available on the internet. The next weakness is that this method only uses a password when connecting to the access point device, so the password is easily spread and easily known by other users, and there is unlimited user usage.

Second Stage (Action Planning)

The researcher understands the core problem and then proceeds to formulate the appropriate action plan to solve the existing problem. In this stage, the author enters the phase of hardware and software preparation for testing, as well as network topology.

Third Stage (Action Taking)

The researcher implements the action plan with the hope of solving the problem. Next, a model is created based on the wireless network infrastructure sketch, followed by conducting an analysis of the running system by taking data screenshots. Then, an analysis of the wireless hotspot security system using the Secure Socket Layer (SSL) security method is performed using the Wireshark application.

Fourth Stage (Evaluating)

After conducting the implementation and testing stages and obtaining the test results, the next process is to evaluate and analyze the results obtained.

Fifth Stage (Learning/Reflecting)

After everything is complete, the final stage is that the researcher conducts a review and evaluation of the stages, step by step, and then the research can conclude. The results also consider future actions.

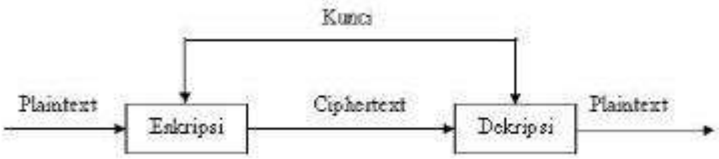


Figure 1: Symmetric Algorithm Encryption and Decryption Process

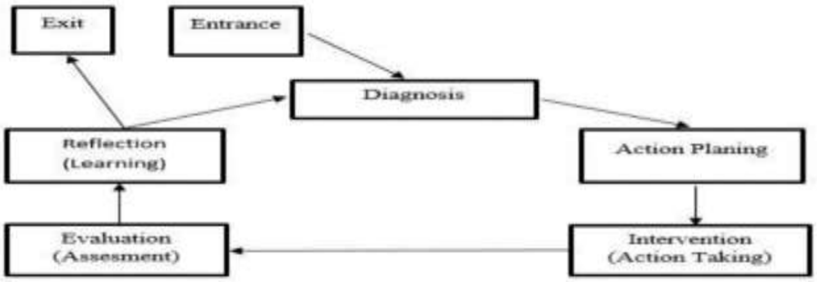
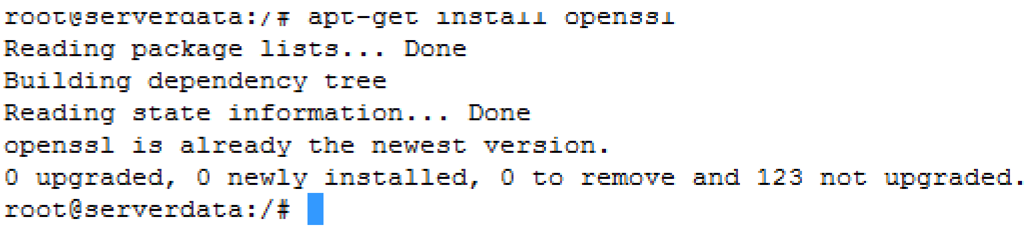


Figure 2: Action Research Method Cycle

Results

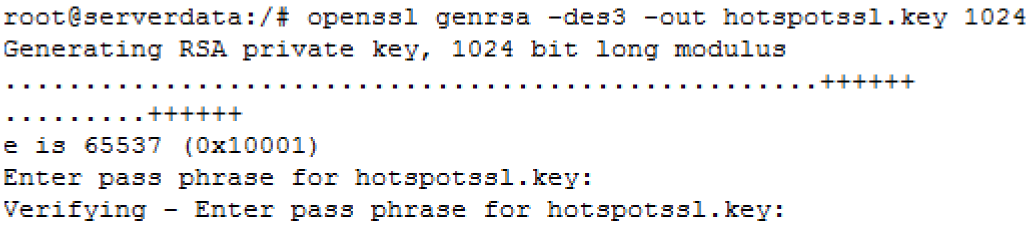
The Mikrotik Router Server configuration uses the Mikrotik Routerboard RB 750. Then, the certificate file and key file are created in the Linux operating system using the openssl software. To create the certificate, the openSSL application is needed, using the apt-get install command. Then, the hotspot key file is created with the name hotspot,ssl, key.



```
root@serverdata:/# apt-get install openssl
Reading package lists... Done
Building dependency tree
Reading state information... Done
openssl is already the newest version.
0 upgraded, 0 newly installed, 0 to remove and 123 not upgraded.
root@serverdata:/#
```

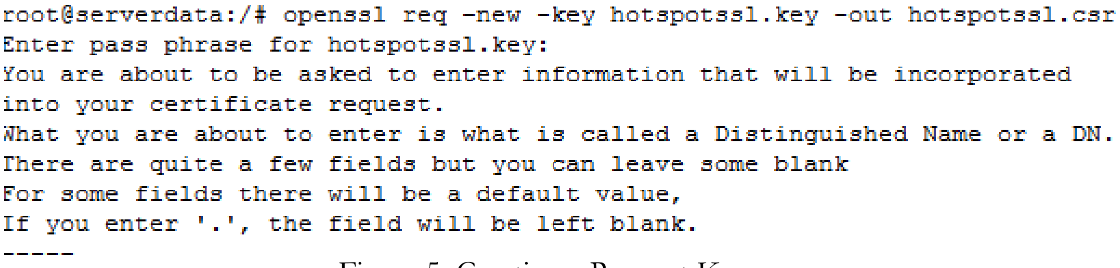
Figure 3. Importing the Certificate File

Open the Mozilla or Google Chrome browser, and the Mikrotik hotspot login display will automatically appear using the Secure Socket Layer facility. This is evident in the login URL, which is https://192.168.1.1. Then, fill in the hotspot user and password.



```
root@serverdata:/# openssl genrsa -des3 -out hotspotssl.key 1024
Generating RSA private key, 1024 bit long modulus
...................................................++++++
.........++++++
e is 65537 (0x10001)
Enter pass phrase for hotspotssl.key:
Verifying - Enter pass phrase for hotspotssl.key:
```

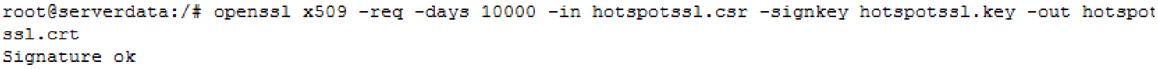
Figure 4. Mikrotik Hotspot Login Display



```
root@serverdata:/# openssl req -new -key hotspotssl.key -out hotspotssl.csr
Enter pass phrase for hotspotssl.key:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
```

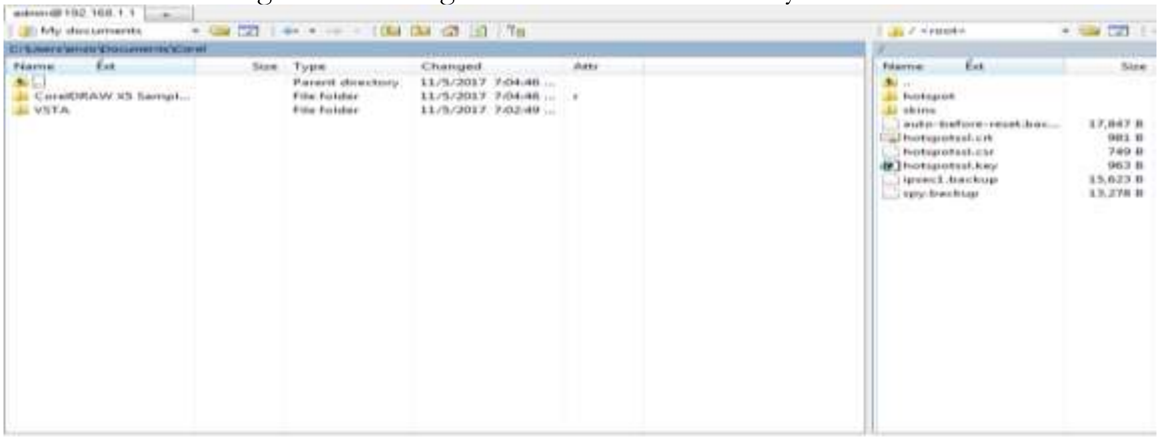
Figure 5. Creating a Request Key

The command for SSL operations using req -X.509 is a Certificate Signing Request (CSR) or a self-signed X.509 certificate. The parameter -days 10000 specifies the validity period of the certificate, which is 10,000 days (approximately 3 years). The option -keyout determines the name of the output file for the private key that is generated, while the option -out specifies the name of the output file for the certificate that is created



```
root@serverdata:/# openssl x509 -req -days 10000 -in hotspotssl.csr -signkey hotspotssl.key -out hotspot
ssl.crt
Signature ok
```

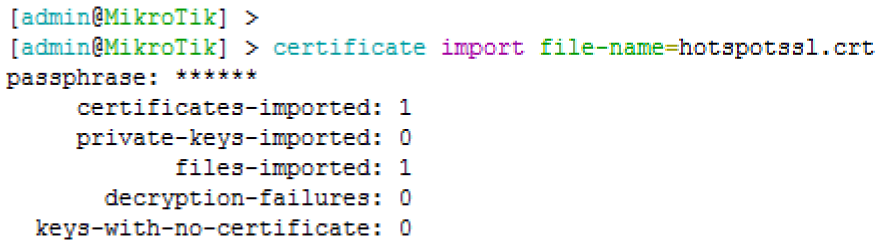
Figure 6. Creating a Certificate File and a Key File



Name	Ext	Size	Type	Changed	Attr
..			Parent directory	11/5/2017 7:04:46 ...	
CorelDRAW X5 Sampl...			File folder	11/5/2017 7:04:46 ...	r
VSTA			File folder	11/5/2017 7:02:49 ...	

Name	Ext	Size
..		
hotspot		
skins		
auto-before-reset.bac...		17,847 B
hotspotssl.crt		981 B
hotspotssl.csr		749 B
hotspotssl.key		963 B
ipsec1.backup		15,623 B
spy.backup		13,278 B

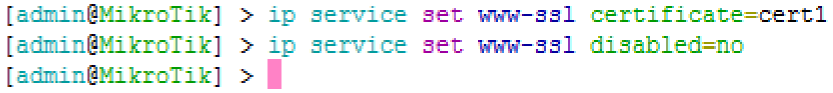
Figure 7. Uploading Certificate and Security Key to Mikrotik Hotspot



```
[admin@MikroTik] >
[admin@MikroTik] > certificate import file-name=hotspotssl.crt
passphrase: ******
     certificates-imported: 1
      private-keys-imported: 0
             files-imported: 1
        decryption-failures: 0
  keys-with-no-certificate: 0
```

Figure 8. Importing a Certificate File

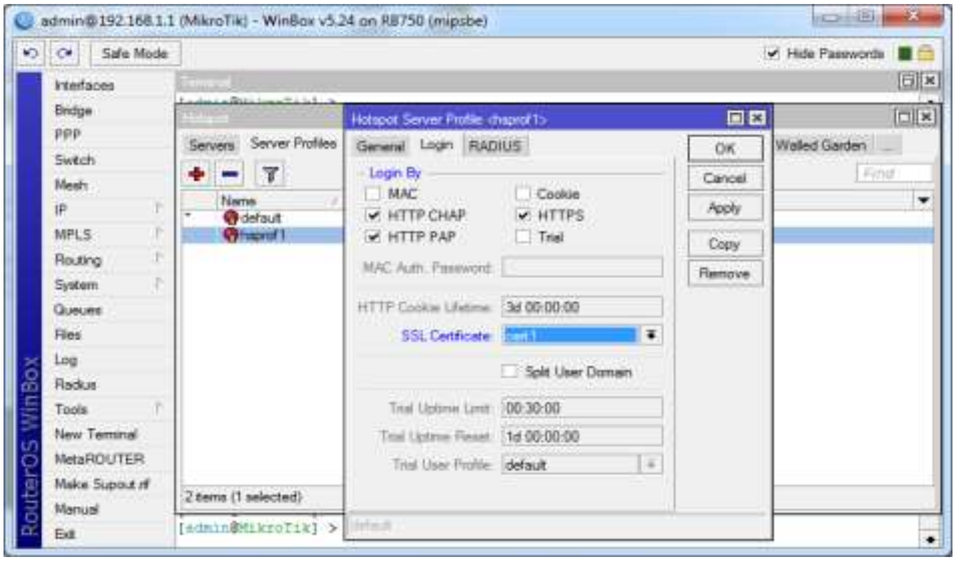
Then, install the key file that has been created on the Mikrotik router using the certificate import command. Next, enable the www-ssl service so that the Mikrotik server supports SSL. After that, configure the system to use the certificate file that was previously generated.



```
[admin@MikroTik] > ip service set www-ssl certificate=cert1
[admin@MikroTik] > ip service set www-ssl disabled=no
[admin@MikroTik] >
```

Figure 9. Enabling the SSL Service Using a Certificate

The figure below shows the configuration of the www-ssl service in the Winbox application.



admin@192.168.1.1 (MikroTik) - WinBox v5.24 on RB750 (mipsbe)

Hotspot Server Profile <hsprof1>

Login By
☐ MAC ☐ Cookie
☑ HTTP CHAP ☑ HTTPS
☑ HTTP PAP ☐ Trial

MAC Auth. Password:
HTTP Cookie Lifetime: 3d 00:00:00
SSL Certificate: cert1
☐ Split User Domain
Trial Uptime Limit: 00:30:00
Trial Uptime Reset: 1d 00:00:00
Trial User Profile: default

2 items (1 selected)

Figure 10. Enabling the SSL Service Using a Certificate

Open the Mozilla Firefox or Google Chrome browser. The login page for the Mikrotik hotspot will automatically appear using the Secure Socket Layer (SSL) facility. This is evident from the login URL, namely https://192.168.1.1. Then, enter the hotspot username and password.

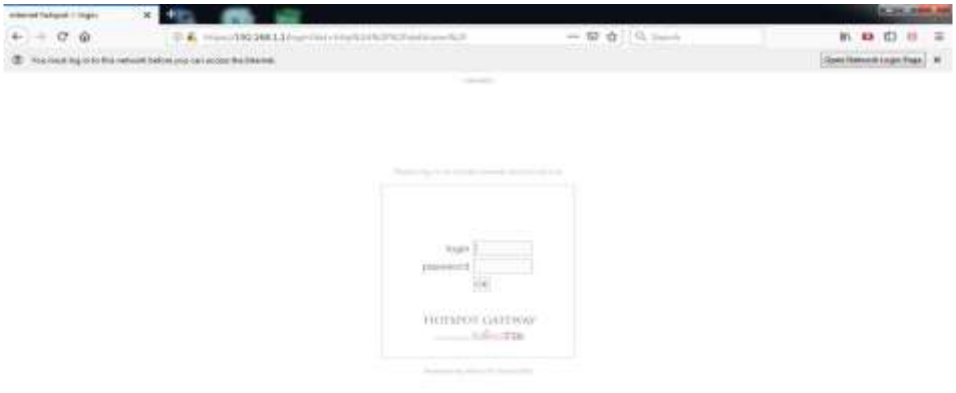


Figure 10. Mikrotik Hotspot Login Page

Discussion

The SSL protocol authenticates the server to the client using public key cryptography and digital certificates. To activate SSL on the Mikrotik login page, it is necessary to install an SSL certificate that matches the server and the Mikrotik hotspot login web page. After SSL is installed, the Mikrotik hotspot login URL, which was previously http://, becomes https://. Figures 4.10 and 4.11 (not visible in the provided pages) show the capture results using the Wireshark application. The result obtained is that the IP address acquired by the hotspot client is 192.168.1.5. It can then be seen that the SSL-type data packet is performing the handshake protocol, namely client hello. After performing the Client Hello handshake, the packet continues with Server Hello, then the certificate is sent. Network data packets that have used SSL imply the encryption of all data transferred between the server and the client.

Conclusion and Recommendations

The conclusions obtained from this study are as follows: It provides ease and security of internet access through the wireless hotspot network for employees and staff within the PTPN 7 Musi Landas Plantation Office environment. The results of the attack test to obtain the login user and password in the wireless network security testing using the Secure Socket Layer (SSL) method lead to the conclusion that this security system can function well and is difficult to penetrate.

References

Kock, Ned, David Avison, and Julien Malaurent. (2017). "Positivist Information Systems Action Research: Methodological Issues." Journal of Management Information Systems.

Jamaluddin, Hasbullah, Suaeb, N. F. (2018). Analisis Keamanan Website Terhadap Sniffing Process Pada Jaringan Nirkabel Menggunakan Aplikasi Wireshark (Studi Kasus Simak Unismuh).

Bayu, Imam. (2017). Analisa Keamanan Jaringan WLAN dengan Metode Penetration Testing. Teknik Informatika Universitas halu Oleo Kendari, 3, (3), 68-78.

Pratama, N. A., Triyono, J., & Iswahyudi, C. (2019). Implementasi Secure Socket Layer Pada Real-Time Video Surveillance Menggunakan Zoneminder dan Apache Webserver. 7(1), 20-28.

Tedyyana, A. (2020). Implementasi Secure Socket Layer Pada Aplikasi Computer Assisted Test Komisi Pemilihan Umum Bengkalis. Digital Zone: Jurnal Teknologi Informasi dan Komunikasi, 11 (1), 71-80.

Kock, Ned. (2017). Information systems Action Research An Applied View Of emerging Concepts and Methods. Texas A & M International University. USA.

Andica, Intan Yuli. (2017). Performa Kinerja Web Server Berbasis Ubuntu Linux Dan Turnkey Linux. Jurnal Penelitian Ilmu Komputer, Sistem Embedded Dan Logic, Vol. 5.

W. Agustiara, A. Pratama, S. Junaidi, K. Padang, and S. Barat, "Analisis Keamanan Protokol Secure Socket Layer Terhadap Serangan Paket Sniffing Pada Website Portal," vol. 6, no. 1, 2022.

Muzakir, A., & Ulfa, M. (2019). Analisis Kinerja Packet Filtering Berbasis Mikrotik Routerboard Pada Sistem Keamanan Jaringan. Simetris Jurnal Teknik Mesin, Elektro dan Ilmu Komputer, 10 (1), 15-20.

Zam, Efvy. (2016). Buku Sakti Wireless Hacking. Jakarta: PT. Elexmedia Komputindo.