PUBLISHED BY
JR
EDUCATION

Available online at http://ijite.jredu.id

IJITE

International Journal of Information Technology and Education (IJITE) 1(2), (March 2022) 60 - 71

International Journal of Information Technology and Education (IJITE)

http://ijite.jredu.id

Wireless Local Area Network Security through Protocol Wireless Protected Access

Sondy Kumajas[1], Julius Sasukul[2*], Alexander Siwi[2], Hellena Saruan[2]

Department of Information Technology and Communication, Universitas Negeri Manado, Indonesia

*Corresponding author: juliussasukul21@gmail.com

ARTICLE INFO

Article history:

Received: 19 November 2021; Received in revised form: 29 Desember 2021; Accepted: 18 March 2022;

Available online: 17 March 2022; Handling Editor: Fabiola Natasya Wauran

ABSTRACT

This study discusses the security analysis of Wireless Local Area Network (Wireless LAN) in the Community against external attacks on the Wireless Protected Access (WPA), Web Proxy, and Virtual Private Network (VPN) protocols, used to attack LAN. Three types of software are used as attackers, namely, Network Stumbler, Aircrack and Wireshark attackers. The software is used on the laptop at a distance of 5m to 25m from the Wireless LAN access point. From the experimental results, it can be seen that the fastest response time by the WPA Protocol was given by the Network Stumbler attacker, followed by Aircrack and Wireshark.

Keywords: security, Wireless Protected Access, Web Proxy, Virtual Private Network. LAN

INTRODUCTION

The development of communication technology is also supported by the increasing progress of infrastructure and technology. One of the developments in communication and

information technology is communication using wireless. This is marked by the development of the emergence of the network, because it has advantages over the following: Mobility, Scalability, Installation Speed and Simplicity, Installation Flexibility, Reduced cost of ownership. Information technology is not wireless technology that produces various conveniences also has an impact on internet service users, both industrial, educational and independent users. This development can also be wireless equipment that uses the standard Wireless Fidelity (WiFi) protocol based on the IEEE 802.11 standard. The increasingly widespread use of networks in the business world and the growing need for faster use of internet online services encourage people to take advantage of shared data and shared resources. With a Wireless Local Area Network (Wireless LAN) users can access information without looking for a place to plug in and can set up a network without pulling cables. Wireless LAN can overcome the problem of lack of wired felt directly by us with the many wireless hotspots available everywhere. Besides being able to help and give birth to various positive innovations, it also gives birth to a negative side, and this always happens, including the development of wireless.

To limit the widespread problems, the problems that will be discussed in this study are limited to the Wireless LAN security protocol infrastructure. The analysis was carried out through several studies of existing white papers and discourses as well as conducting experiments by attacking the Wireless LAN infrastructure. Wireless LAN security protocols used in this study are Wireless Protected Access (WPA), Web Proxy, and Virtual Private Network (VPN). By using 3 attacker tools, namely Network Stumbler, Aircrack, and Wireshark

The purpose of this study was to test the extent of the security capabilities of the WPA protocol, Web Proxy and Virtual Private Network (VPN), against attacks from Software Network Stumbler, Aircrack and Wireshark.

METHOD

The research focused on how to formulate existing problems and identified and formulated based on security aspects of the Wireless LAN protocol. Then develop a hypothesis as an answer or initial conclusion and a strategy to test whether the hypothesis is the answer to the existing problems.

Stages

In this study the author uses several stages, starting with:

1. Make a design using an infrastructure topology
2. Large addition of initialization vector size to prevent repetition of initialization vector values.
3. Changing the initialization vector selection method to prevent weak keys from occurring, as well as preventing possible replay attacks.
4. Change the encryption key for each packet sent (per packet key mixing).

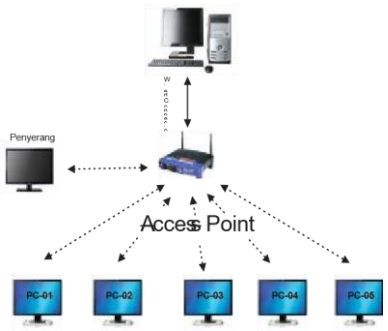


Figure 1 . Attack Trial

1. Better use of message integrity protocol to prevent message modification with 5 (five) wireless users connected to 1 (one) server through 1 (one) access point and 1 (one) attacker.
2. Tried attacks on Wireless LAN infrastructure using the WPA, Web Proxy and Virtual Private Network security protocols and access points with different signal strengths, namely at a distance of 5 meters, 10 meters, 15 meters, 20 meters, 25 meters.

Figure 2. Trial Position with the difference in distance between attackers

Data analysis

The data were analyzed using several stages of testing as follows:
1. Identify or monitor the configuration of hotspot presence using Network Stumbler 0.4.0 software.
2. Then deal with opening a wireless network connection.
3. Trying to crack the password on the access point used using the Aircrack-ng-0.9.3-win software.
4. The attack was measured for data sent, data received and data lost using Network Stumbler 0.4.0 software.

Testing of IP address manipulation attacks is carried out with 2 test methods:

Method 1:

1. Connect based on MAC Address and information
2. Get the IP Address and then open a Wireless connection session by logging into the Web Proxy and connecting to the server.
3. Eavesdropping on packets to obtain a valid MAC address using the Network Stumbler software and falsifying the attacker's MAC address and connecting with the access point based on the forged MAC address.

Method 2:
1. Connect with the access point based on the forged MAC Address and get the IP Address and the Wireless LAN connection is opened by logging into the Web Proxy.
2. Connect with the access point based on the fake MAC address and get the IP Address and cannot open a Wireless LAN connection session when logging in to the Web Proxy.

Expected results on the attacking side

The attack is successful if the IP Address of the wireless user and attacker is different (which is obtained from the server) and the attack fails if the IP Address of the wireless user and the attacker is the same (which is obtained from the server). If the attack fails then manually configure the IP address on one of the devices in order to get a different IP address.

RESULTS AND DISCUSSION

In designing the security model, assets Analysis Results with the WPA Protocol network at risk need to be considered such as weak points in the system with the WPA Protocol being able to overcome its security, or interference from the attacker, as well as the motivation of the attack for each potential weakness. Regarding this, it is very necessary to take the necessary security protection measures.

Table 1. Results of Attempted Attacks against the WPA Protocol

Distance (m)	Network Stumbler	Aircrack	Wireshark
	Response time rata2 (second)	Response time average (second)	Response time average (second)
5	0	320	3
10	0	930	6
15	0	1545	9
20	0	2140	12
25	0	2730	15

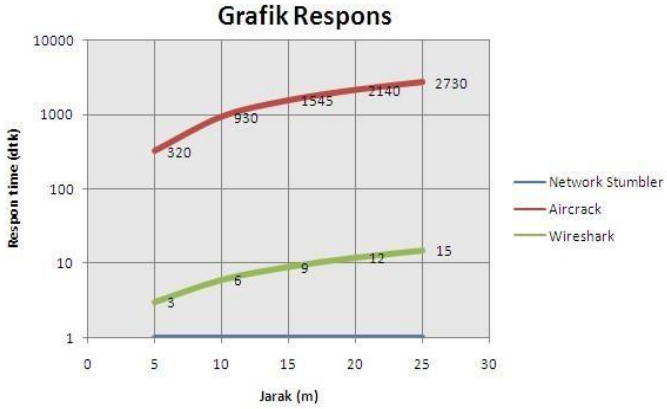


Figure 3. Graph of Response Time to the WPA Protocol.

From the Response Time graph, it can be seen that Network Stumbler is the fastest in detecting its security system, while Aircrack is the slowest. Then also carry out attacks on data retrieval sent by wireless users by using the WPA protocol to the server. And the result can be easily connected to the access point. And can also perform data retrieval so that the data received has weaknesses in data integrity and availability on the system. And the author tries to do an experiment to prove the weakness of the WPA protocol when applied to Wireless LAN, namely by attacking the encryption (Network Key or password) used by the access point.

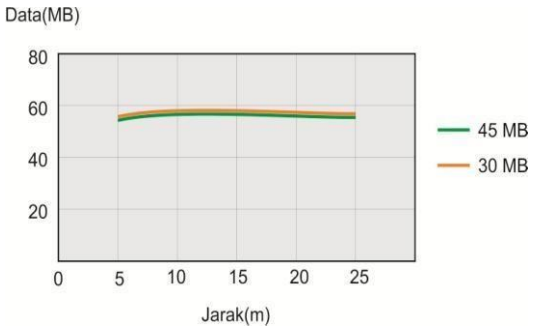


Figure 4. Number of Data Packets Received.

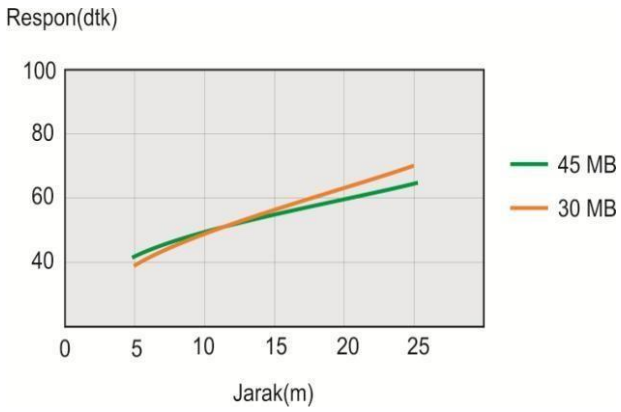


Figure 5. Response Time Data received on Server .

Analysis Results With Web Proxy Security

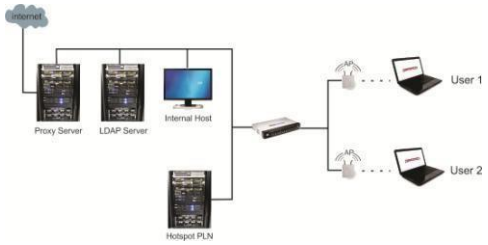


Figure 6. Wireless LAN Architecture

From the picture, the architecture of Wireless LAN and wired networks is part of an integrated network. Access control of devices that want to connect is done by using the MAC Address of the user stored in the LDAP (Lightweight Direction Access Protocol) server. The authentication process into the network is carried out through a Web Proxy that uses the Secure Socket Layer (SSL) protocol. SSL is a security protocol that works above layer 4 (four) OSI (transport layer), where all data that goes through this protocol will be encrypted.

After the user is authenticated, the user will get access rights to the internal wired network and to the internal (by using a proxy server). Wireless LAN users use a Web Proxy with SSL protocol in the authentication process, providing security protection against theft of wireless username and password information because the data is transmitted in encrypted form. The wireless user connection process can be seen in Figure 7.

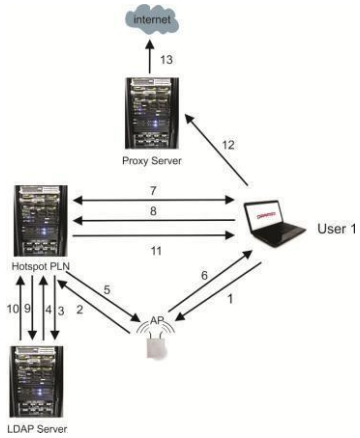


Figure 7. Wireless LAN Connection Process

Wireless connection process that occurs is as follows:

1. Wireless users perform the connection process with the access point using open system authentication (without using WEP).

2. Access point performs access control to connection requests from wireless users by querying hotspots based on MAC Address information owned by wireless users.

3. The query received by the hotspot is forwarded to the server to obtain information whether the MAC Address of the wireless user is a registered device.

4. The server confirms whether the MAC address is in the database or not.

5. The hotspot receives information from the server and then confirms the association process is accepted or not based on that information, that is, if the MAC address is registered, the association process is accepted and vice versa.

6. The access point confirms to the wireless user that the association process has been successful or not.

7. If the association process is successful, the following processes will be carried out (seventh process and so on).

8. After the wireless user gets an IP address, an authentication process is needed to ensure that the wireless user is a user who does have access rights. For that, the wireless user must enter information in the form of a wireless username and password via a Web Proxy that uses the SSL protocol. Where the data that is transmitted will be encrypted so as to prevent the possibility of attackers knowing the secret identity of the wireless user.

9. The server responds whether the authentication process is accepted or not by checking whether the wireless username and password combination is in the database directory.

10. These protocols provide transmitted plain text.

11. Strong authentication, encryption and integrity power. Other protocols exist. People do not use security at the top layer (application layer) such as the data link layer layer (such as WEP and HTTP, FTP and telnet are not WPA), because it transmits data from secure protocols because all data is "insecure" ” is still transmitted in plain text (clear WebProxy in the Community)

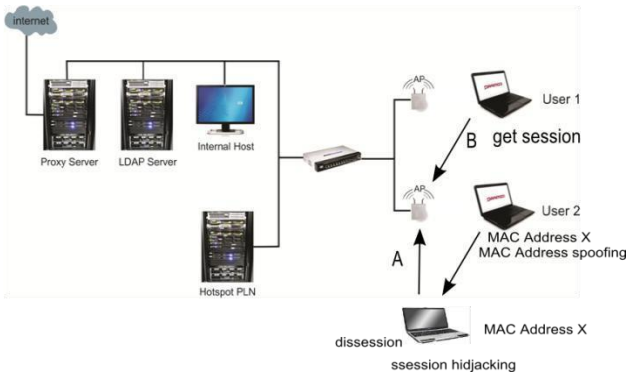


Figure 8. *Session Hijacking on Wireless LAN with Web Proxy*

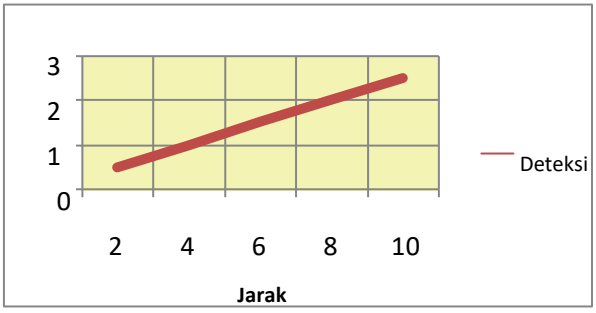


Figure 9. IP Address Detection attack experiment results

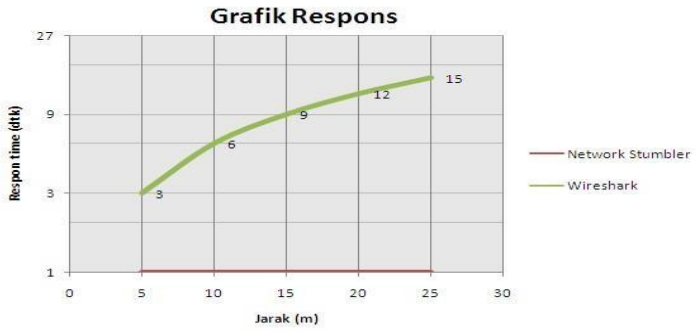


Figure 10. Graph of Response Time to Web Proxy Protocol

This means that the point of weakness in security can be exploited by attackers to intercept the data transmission and try to attack the authentication and access control of the system. From the Response Time graph, it can be seen that Network Stumbler is the fastest in detecting the security system, while Wireshark is the slowest.

On Society. The attack carried out is session hijacking, which is an attack carried out to steal a session from a wireless user who has been authenticated with an access point.

Attack on Virtual Private Network

Conducting experimental attacks on hotspots using Virtual Private Network security by trying to crack wireless usernames and passwords with different distances and trying to find connection sessions. From experiments conducted using aircrack software, the author can only identify or monitor the configuration of the presence of a hotspot without being able to solve the wireless username and find out the IP Address of the original wireless user, the password of the original wireless user without being able to change the wireless IP address.

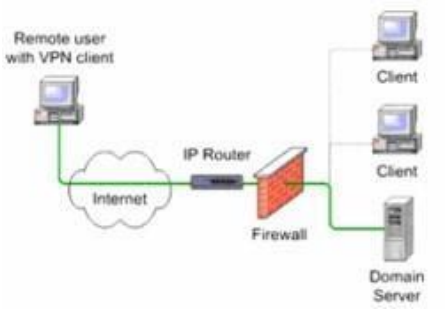
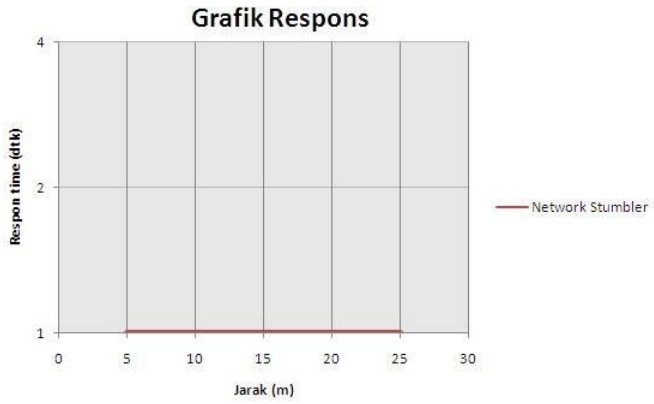


Figure 11. Security Network Structure with VPN

Table 2. Results of Attempted Attacks on VPN Protocols

Distance (m)	Network Stumbler	Aircrack	Wireshark
	Response time average (second)	Response time average (second)	Response time average (second)
5	0	Not successful	Not successful
10	0	Not successful	Not successful
15	0	Not successful	Not successful
20	0	Not successful	Not successful
25	0	Not successful	Not successful

Figure 12. Graph of Response Time to VPN Protocol.



CONCLUSION

From the results of research and experiments on Wireless LAN can be concluded as follows:

1. The use of security with the WPA protocol, Web Proxy and Virtual Private Network (VPN) does not provide security protection from Network Stumbler.
2. Using the WPA protocol, the average response time for Network Stumbler is faster than Wireshark, while the average Aircrack response time is 45 minutes for a distance of 25 m.

3. Using the protocol with Web Proxy, the average response time for Network Stumbler is faster than Wireshark, while Aircrack is not successful.
4. Using a protocol with a VPN, the average response time for Network Stumbler is faster, while the average response time for Wireshark and Aircrack is not successful.

REFERENCES

Acemoglu, D., Malekian, A., & Ozdaglar, A. (2016). Network security and contagion. *Journal of Economic Theory*, *166*, 536-585.

Kavianpour, A., & Anderson, M. C. (2017, June). An overview of wireless network security. In *2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud)* (pp. 306-309). IEEE.

Liu, G., Peng, B., & Zhong, X. (2020). A novel epidemic model for wireless rechargeable sensor network security. *Sensors*, *21*(1), 123.

Luong, N. C., Hoang, D. T., Wang, P., Niyato, D., & Han, Z. (2017). Applications of economic and pricing models for wireless network security: A survey. *IEEE Communications Surveys & Tutorials*, *19*(4), 2735-2767.

Muhammad, M., & Hasan, I. (2016). Analisa Dan Pengembangan Jaringan Wireless Berbasis Mikrotik Router Os V. 5.20 Di Sekolah Dasar Negeri 24 Palu. *Jurnal Elektronik Sistem Informasi dan Komputer*, *2*(1), 10-19.

Mulyanto, Y., Herfandi, H., & Kirana, R. C. (2022). ANALISIS KEAMANAN WIRELESS LOCAL AREA NETWORK (WLAN) TERHADAP SERANGAN BRUTE FORCE DENGAN METODE PENETRATION TESTING (Studi kasus: RS H. LMANAMBAI ABDULKADIR). *Jurnal Informatika Teknologi dan Sains*, *4*(1), 26-35.

Pawar, M. V., & Anuradha, J. (2015). Network security and types of attacks in network. *Procedia Computer Science*, *48*, 503-506.

Rathore, S., Sharma, P. K., Loia, V., Jeong, Y. S., & Park, J. H. (2017). Social network security: Issues, challenges, threats, and solutions. *Information sciences*, *421*, 43-69.

Rumalutur, S. (2014). Analisis Keamanan Jaringan Wireless LAN (WLAN) Pada PT. PLN (Persero) Wilayah P2B Area Sorong. *Jurnal Ilmiah Teknologi dan Rekayasa*, *19*(3).

Samsumar, L. D., & Gunawan, K. (2017). Analisis dan Evaluasi Tingkat Keamanan Jaringan Komputer Nirkabel (Wireless LAN); Studi Kasus di Kampus STMIK Mataram. *Jurnal Ilmiah Teknologi Infomasi Terapan*, *4*(1).

Sari, R. D., Supiyandi, A. P. U., Siahaan, M. M., & Ginting, R. B. (2017). A review of ip and mac address filtering in wireless network security. *Int. J. Sci. Res. Sci. Technol*, *3*(6), 470-473.

Sharma, P. K., Singh, S., & Park, J. H. (2018). OpCloudSec: Open cloud software defined wireless network security for the Internet of Things. *Computer Communications*, *122*, 1-8.

Suharmanto, A. Y., Lumenta, A. S., & Najoan, X. B. (2018). Analisa Keamanan Jaringan Wireless Di Universitas Sam Ratulangi. *Jurnal Teknik Informatika*, *13*(3).

Tayal, S., Gupta, N., Gupta, P., Goyal, D., & Goyal, M. (2017). A review paper on network security and cryptography. *Advances in Computational Sciences and Technology*, *10*(5), 763-770.

Zou, Y., Zhu, J., Wang, X., & Hanzo, L. (2016). A survey on wireless security: Technical challenges, recent advances, and future trends. *Proceedings of the IEEE*, *104*(9), 1727-1765.