EPJ Web of Conferences **68**, 00029 (2014)
DOI: 10.1051/epjconf/20146800029

Building secure wireless access point based on certificate authentication and firewall captive portal

B. Soewito[1], and Hirzi.[1]

[1] Bina Nusantara Graduate Programs, Bina Nusantara University (BINUS), Jakarta, Indonesia

Abstract. Wireless local area network or WLAN more vulnerability than wired network even though WLAN has many advantages over wired. Wireless networks use radio transmissions to carry data between end users and access point. Therefore, it is possible for someone to sit in your office building's lobby or parking lot or parking lot to eavesdrop on the wireless network communication. This paper discussed securing wires local area network used WPA2 Enterprise based PEAP MS-CHAP and Captive portal firewall. We also divided the network for employer and visitor to increase the level of security. Our experiment showed that the WLAN could be broken using the attacker tool such as airodump, aireply, and aircrack.

1 Introduction

Wireless communication is exchange of information between two or more devices that are not connected by an electrical conductor. A wireless local area network (WLAN) links two or more devices over a short distance using a wireless distribution method, usually providing a connection through an access point for internet access.

The use of technology spread-spectrum or Orthogonal Frequency-Division Multiplexing (OFDM) technologies may allow users to move around within a local coverage area, and still remain connected to the network [1], [2]. Using Wireless Local Area Network users can access internet without pulling the cable network.

WLAN can overcome the problem of lack of wired network, because it has the advantage, as follows:

- Mobility: WLAN users can gain access to internet at anywhere from one access point to another access point, without preparing cable or network infrastructure.
- Scalability: WLANs can be configured to different topology depending on the needs of the system. Configuration can be easily changed from peer-to-peer network until the number of users to full infrastructure networks with thousands of users.
- Installation and Simplicity: Wireless network is very simple to configure. Simplicity of installation is more cost effective, network setup and installation do not need to use of cables.
- Installation Flexibility: WLAN users can gain access to the network without preparing the cable infrastructure.

With an explosive increase of internet application and a further wireless security system requirement, the network administrator will face more difficult challenge in meeting the ever stringent security design. Securing a wireless network is even more important than securing a wired network for one simple reason: Accessing a wireless network does not require physical access to a network jack or cable, as does accessing a wired network. [3], [4]. Wireless networks use radio transmissions to carry data between end users and the network. Therefore, it is possible for someone to sit in your office building's lobby or parking lot to eavesdrop on wireless network communications.

The answer to this problem is to use strong encryption to protect data transmitted over a wireless network and to use authentication to each one who would like to use the wireless network. There are several security schemes that can be used, namely Hidden SSID, MAC Address Filtering, and WEP security protocols or WPA/WPA2-PSK. However, these schemes also have weaknesses and can be exploited.

In our proposed method to improve the wireless security, we used two level securities. First we used the integrated firewall with pfSense Captive Portal server as a user login portal. Second we implemented WPA2-enterprise which requires digital certificates for device recognition process with the authentication server based

database together with list of existing accounts in Active Directory.

2 Attacking on WLAN and Security

In WLAN, Communication and transferring data using media radio transmission which opened to all users [5], [6], [7]. This circumstance will attractive to people who want to use WLAN without permission. There are several purposes to connect to the WLAN without permission such: to get free internet access, to steal data, spying on the activities a person or company, to damage a company's system, etc.

Some of WLAN attack that are very easy to do and others are more complicated but the results is very dangerous. Below are some of examples of WLAN attacks.

1. Wireless Network Sniffing: Sniffing is eavesdropping activities or listening to any data packets passing the network. A sniffer is a program that intercepts (tap) and decode network traffic that is being transmitted to a medium [8], [9]. Easier to sniffing the wireless network. As it is known that the air medium to use your WLAN which means as far as the WLAN signal coverage, as far as it can also be done sniffing. Some of the activities associated with sniffing is Passive Sniffing, Detection of SSID, and Collecting MAC Address.
2. Wireless Man in the Middle Attack: Attacks Man-in-the-Middle trick done with the connection between your computer and the access point authorized users by entering another computer in between them as a provocation. The program used is also the same, except for their wireless devices. Through the program, the intruder is able to position itself in between the traffic data communication in wireless networks.
3. Brute Force Attack: an attack by performing tests on the access key by trying all possible password combinations, where most of the access point using a single key.
4. Session Hijacking: This attack was to steal session from a wireless user is already authenticated with access point [9], [10]. Attacker will send a wireless message to the user disassociate with him as if coming from the access point. Wireless users will think that the connection to the access point has been lost, but maintained that the access point is still connected to her wireless user. Then the attacker will use the MAC address and IP address to connect to the access point act as the user wireless [11].

To implement Wireless LAN security is to use a standard security protocol defined in IEEE 802.11 networks. The security protocol is WEP and WPA. In addition to securing the WLAN can also be applied along with the NPS Captive Portal and Active Directory as the authentication server.

3 Methodology

In this paper we introduce the technique to secure WLAN using WPA2 Enterprise, firewall captive portal, and certification techniques as shown in figure 1. The network topology in fig.1 is a regular network for medium office. In general, the medium office has three subnets in their office. So that we build the network topology that has three subnets and several servers.

3.1 Experiment tools

The devices that we used in our experiment are:

- Proxy:IBM-X3200, Pentium D 2.8 GHz, 2GB
- Active directory: IBM-X3400, Xeon E5506 2.1 GHz, 8GB
- Switch: Cisco-SRW2024, 24 ports
- Wireless Access Points: Linksys-WAP54G
- Laptop core i5, 4 GB

We also used software to evaluate the level security of our proposed architecture. We used Linux Backtrack version 5 with airodump-ng, airmon-ng, aireply-ng, aircrack, dan aireplay.

3.2 Performing attack

The first thing that we did in our experiment is to attack the network through WLAN with default security setting.

The following is the steps how to do the attack:

1. Identification and monitoring the existing WLAN or access point using airmon-ng and airodump-ng.
2. After knowing the existence of WLAN, the next action is to inject data packets to clients that are connected to the access point using aireplay-ng tool. With the injection of this package, the client will experience a de-authentication, so that it will force the client to do re-authentication.
3. In the re-authentication process, airodump-ng will capture the handshake process and save them into a file.
4. The handshake file has to decrypt using Aircrack-ng with Dictionary Attack techniques. The expected result is to know the password used to connect to the Access Point.
5. In addition to using Dictionary Attack, we also use a brute force technique. However, this technique took longer compare to dictionary attack.

3.3 Securing WLAN

Practically in securing WLAN, we have to divide SSID access point to three networks, namely voice data, internal user, and guest. In our work, we did not using IP-based voice communications; the voice data can be ignored. So, we focused on two SSID, the SSID for the internal user and guest. Users who connect to the internal SSID can access not only the Internet but also the internal network. While the user is connected to the guest SSID

cannot access to the internal network. In our work, we used two access points. Actually one access point SSID can have 2 pieces, but because there is no compatibility with pfSense server, then we used two access point to handle two SSID [12].

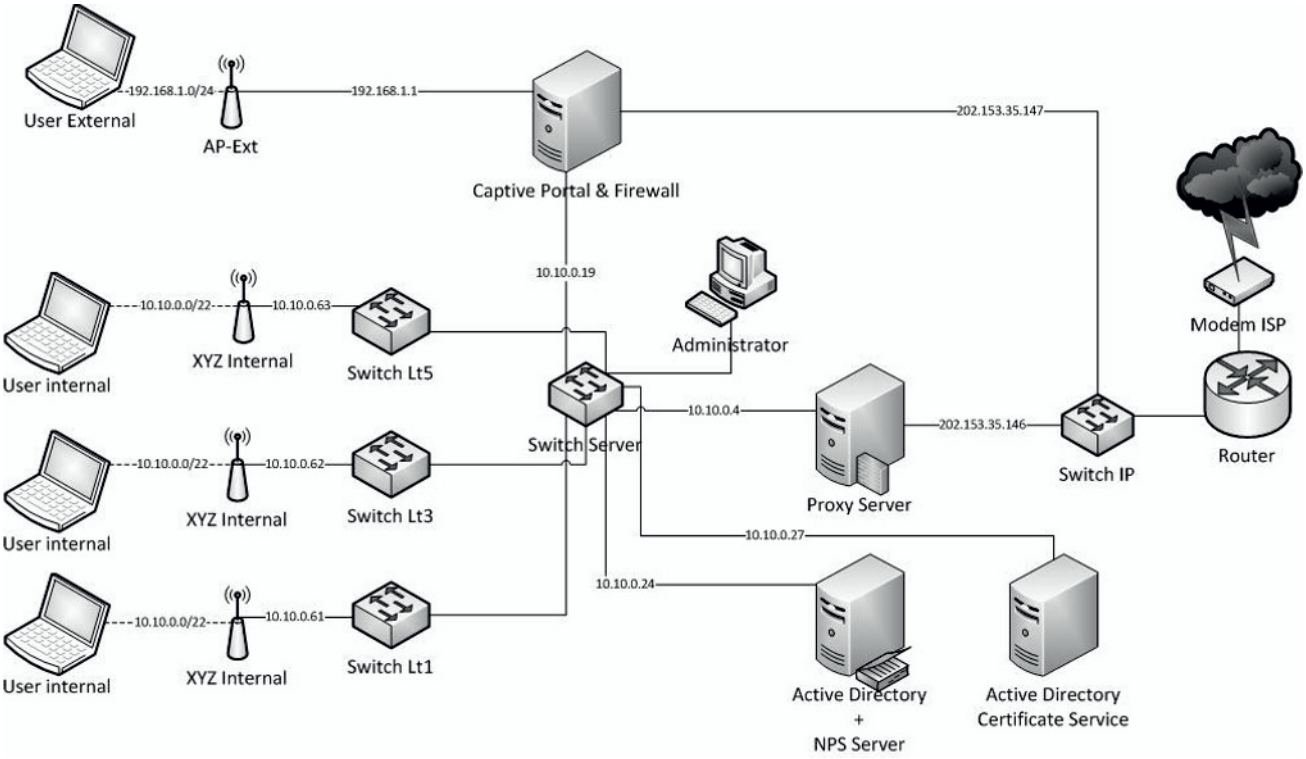

Fig. 1. Network Topology of our experiment.

Service (IAS), Network Policy Server (NPS Server), and used active directory technique [13], [14]. In our work, we proposed WLAN security used WPA2 enterprise base on PEAP-MS-CHAP and firewall captive portal. Protected Extensible Authentication Protocol (PEAP) is a member
of the family of Extensible Authentication Protocol (EAP) protocols. PEAP uses Transport Layer Security (TLS) to create an encrypted channel between an authenticating PEAP client, such as a wireless computer, and a PEAP authenticator, such as an Internet Authentication Service (IAS) or Remote Authentication Dial-In User Service (RADIUS) server. PEAP does not specify an authentication method, but provides additional security for other EAP authentication protocols, such as EAP-MS-CHAP v2, that can operate through the TLS encrypted channel provided by PEAP. PEAP is used as an authentication method for 802.1X wireless client computers, but is not supported for virtual private network (VPN) or other remote access clients.
We used NPS server as an interface from access point to active directory server. The purpose of active directory server is to save database for processing the authentication and create the certification on server as well as on client or user, so that only the users listed in active directory that can access internal SSID.

In our work, we used PEAP MSCHAP V2 that utilizes Active Directory Certificate Services to generate digital certificate installed on the NPS Server with the

3.3.1 Securing internal SSID

The most important in WLAN security is the process of authentication. There are several techniques in authentication process such as Internet Authentication intention that Wireless Client can be known by the NPS Server. To be more understood about the process of authentication, a flowchart of authentication process based on PEAP MSCHAP is shown in Fig. 2. PEAP MSCHAP V2 authentication process occurs in two phases. The first phase uses the protocol EAP to open channel TLS. The second phase uses the protocol EAP to do authentication mechanism of username and password who want to connect to the Wireless LAN through SSID Internal.

The steps of authentication between Wireless Client and Wireless access point that utilize NPS Server to perform processing packages are as follows:
1. Request Identity. The Wireless Client will request to connect to the wireless access point. Wireless Client sends EAP-start packet. Wireless access point then sends the request for the identity used packet EAP-Response/Identity
2. Authentication using a username and password. At this stage the Wireless access point will send the message Response / Identity to NPS server which is RADIUS Access Request form.
3. EAP-Request NPS Server. At this stage the NPS server will sends a RADIUS Access-Challenge message containing an EAP-Request message with the EAP type used in the TLS process. The request indicates that the TLS authentication process begins.
4. EAP-Response Wireless Client. Wireless Client will send an EAP Response. This is known as the hello packet delivery. Wireless access point will then forward the EAP

messages to NPS Server in the form of RADIUS access-request message.

Evaluating and analyzing the WLAN that has adopted our proposed technique is the same steps which we did in section 3.2. Basically the evaluation divided in to two parts: connection test and attacking WLAN.

3.3.2 Securing external SSID

In order to secure external SSID for guest, we used Captive portal firewall. At the time a user access the wireless access point, or when opening a website in the browser, visitor notification will appear to type in the username and password for authentication. It will be redirected to the Captive Portal login page. Users simply enter the username and password to gain access to the Internet network. Username is prepared is a guest. Once, the username and password recognized by the server, then the web page will be redirected back to the page that will be addressed in advance.

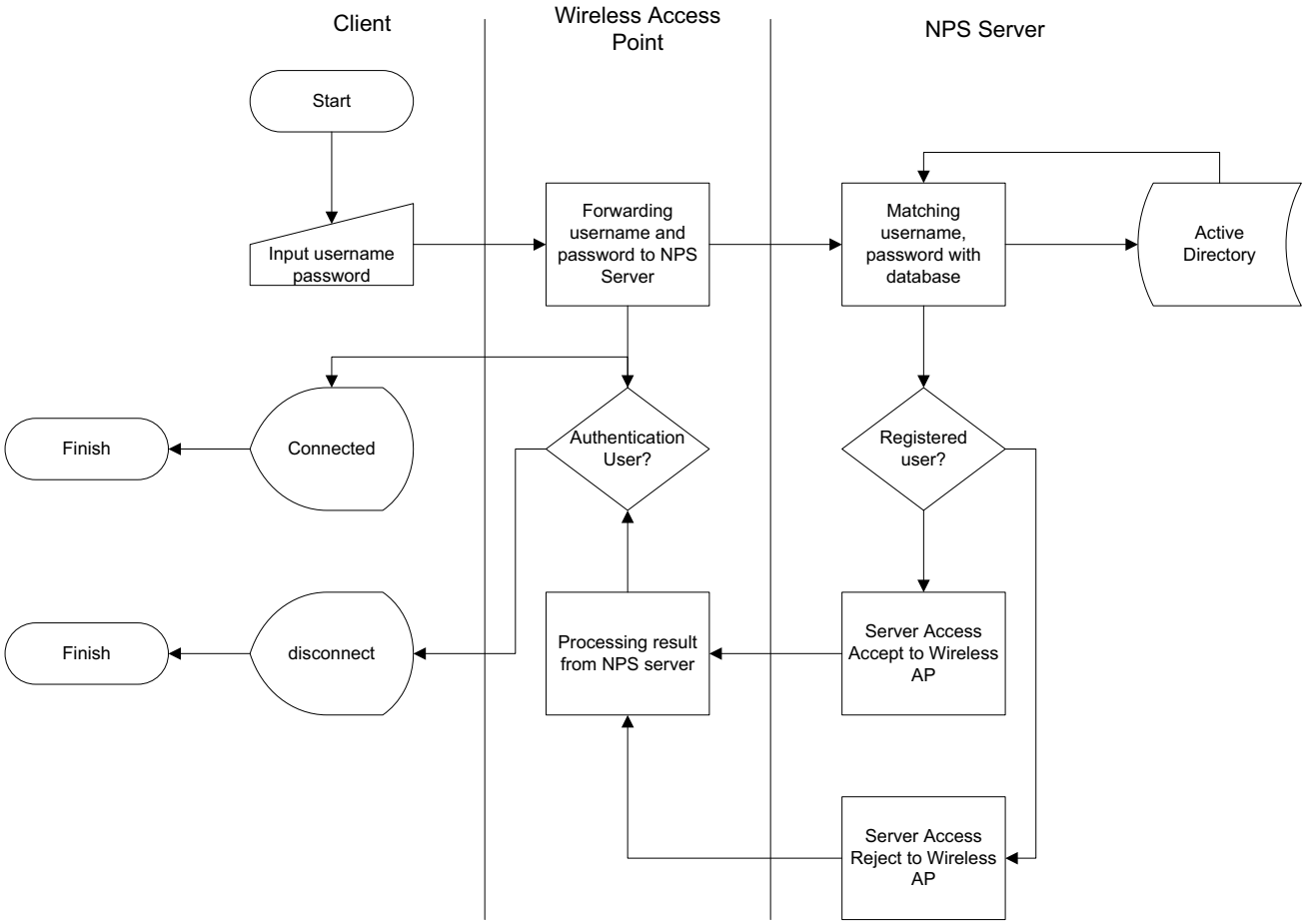

Fig 2. Flowchart process of authentication

To monitor guest connection, we used pfSense that can monitor user status who access to the network through Captive Portal. The pfSense can write the IP Address, user name, MAC Address, time when the guest start and finish connect to the network, etc.

4 Results and analysis

As we follow steps in section 3 to attempt attacks, it found that WLAN that used WPA2-PSK security is vulnerable to aircrack-ng. In our experiment, we need about nine minutes to break the password. We used aircrack-ng with airodump-ng and aireplay-ng. In this case we have to waiting for the client to perform authentication, WPA Handshake then the process would be easily captured by airodump-ng, then we performed Dictionary Attack using aircrack-ng. We can also use Aireply-ng to push client to do re-authentication.

The results of evaluating the proposed technique for SSID internal used the procedure as shown in section 3.2.

First, the experiment showed that the laptop that listed in active directory but does not have digital certificate could not join the WLAN. The NPS server rejected the requesting connection.

Second, the results of attacking test used the same tools in section 3.2: airodump-ng, aireplay-ng, and aircrack-ng as follow: Airodump-ng still can detect the internal SSID and other WLAN in the range. Aireplay-ng successfully do inject by sending the injection packet that cause the client has to do re-authentication. When client doing re-authentication, the Airodump-ng still can capture WPA handshake and save it in wpa2ent.cap. After we try to break this file for more than one hour we

found that the file is empty, do not content of authentication process. This was as we expect that the WLAN used the proposed topology in Fig.1 could not be broke. Because airodump-ng only captured handshake process between client and wireless access point. The process between client, RADIUS, and Active directory cannot be captured by Airodump-ng.

Table 1. Comparison WPA2-PSK, WPA2 Enterprise, and Captive Portal Firewall.

Comparison effectively attack			
Attacking tools	WPA2 PSK	PEAP MSCHAP V2	Captive Portal Firewall
Airodump-ng I	Yes	Yes	Yes
Airodump-ng II	Yes	No*	No*
Aireplay-ng	Yes	Yes	Yes
Aircrack-ng	Yes	No	No

In the table 1 above show that applying all attacking tool to attack WPA2 PSK can effectively run well. If one steps of attacking tools is not successful, then the process stops and attacking unsuccessful. WPA2 Enterprise with PEAP-MSCHAP proved that one of step is not successful. Airodump II could not run because the process of 4-way-handshaking could not capture username / password, backend Active Directory and digital certificates. This will caused the Aircrack-ng fails to do its job. The Captive Portal Firewall experiencing the same results. It means that the attack is unsuccessful.

Table 2. Time to attack using Aircrack-ng

Aircrack-ng			
Devices	WPA2 PSK	PEAP MSCHAP V2	Captive Portal Firewall
Laptop 1	00:08:56	01:34:45	~
Laptop 2	00:12:40	01:50:55	~
Laptop 3	00:18:24	02:25:58	~

Table 2 shows the time to attack using aircrack-ng. The time change proportional to the specifications of the laptop. The lower specification laptop attacker, then the longer it takes to solve the WPA2-PSK passwords. In the table 2, showed that device Laptop 1, took 8 minutes and 56 second to be cracked. But keep a special note for the implementation of PEAP MSCHAP V2 is even Aircracking-ng to work and do the cracking process as well as the results of time appears still not read the password (passphrase not found) because as noted earlier, the tools should be used before does not work successfully. So also with the Captive Portal Firewall, tools Aircrack-ng cannot work at all.

5 Conclusions

We concluded that the security of Wireless LAN in many places still used default setting which vulnerable to attack. They still use WPA2 PSK and there is no separation for internal and external users. WPA2 PSK does have weaknesses that can be exploited easily using a single laptop and Backtrack Linux operating system with only 4 steps. The test results show that the attack on security WLAN that used WPA2 PSK technique can be cracked easily in less than 9 minutes.

WPA2 Enterprise is used in our experiment use protection based PEAP MS-CHAP v2. PEAP MS-CHAP v2 provides mutual protection on the server and client using a digital certificate and additional protection with the username / password for each user in the Active Directory database backend.

Captive Portal Firewalls are used to prevent visitors connect to the internal network. it is blocked by the firewall. When the external user wants to use the Internet, will appear portal with the username and password. So even though visitor can be connected to the internet, but cannot go into internal network.

References

1. Singh, Amardeep et al. Classification of Security Attacks in 802.11 Wireless LAN and its Prevention. Journal of Computer Science and Applications. ISSN 2231-1270 Volume 3, Number 1.
2. Vibhuti, Shivaputrappa. (2005*). IEEE 802.11 WEP (Wired Equivalent Privacy) Concepts and Vulnerability*. San Jose State University, CA, USA CS265 Spring 2005, Retrieved (November 11, 2012) from *www.cs.sjsu.edu/~stamp/CS265/projects/Spr05/papers/WEP.pdf*
3. Anderson, Ross (2008). *Security Engineering, 2nd Edition*. Wiley.
4. Williams (2007). Information Security Concepts. Available at: http://www.rhwiii.info/pdfs/Introduction%20to%20basic%20security%20concepts.pdf (Sabtu, 22 Desember 2012)
5. Bhatia, Vhania et al (2012). Throughput and Vulnerability Analysis of an IEEE 802.11b Wireless LAN. International Journal of Computer Applications (0975 – 8887) Volume 52– No.3, August 2012, Retrieved (Desember 2, 2012), from *research.ijcaonline.org/volume52/number3/pxc3881509.pdf*
6. Simpson, Michael (2012). *Hands On Ethical Hacking and Network Defense*. Course Technology.
7. Herbiet, Guillaume-Jean and Nou, Gregory (2005). *Wireless Security Architecture for Campus Network*. [Electronic Version] available at *herbiet.gforge.uni.lu/files/wireless-security-cs6255.pdf (2012, November 11)*
8. Sankar, Krishna. et al (2004). *Cisco Wireless Lan Security, 1st Edition*. Cisco Press.

9. Microsoft (2010) *Wireless Access Deployment Overview* [Electronic Version]. available: http://technet.microsoft.com/en-us/library/ff919549%28v=ws.10%29.aspx (2013, Januari 23)
10. Kadlec, Jaroslav. et.al (2010). Implementation of an Advanced Authentication Method within Microsoft Active Directory Network Services. Sixth International Conference on Wireless and Mobile Communications IEEE. Retrieved (November 11, 2012), from http://ieeexplore.ieee.org
11. Johnson, Darren (2013). *Wireless Pre-Shared Key Cracking (WPA, WPA2) v1.0,* [electronic version]. Available: *http://www.og150.com/assets/Wireless%20Pre-Shared%20Key%20Cracking%20WPA,%20WPA2.pdf (2013, Mei 13)*
12. pfSense (2012) *pfSense FreeBSD*, [Electronic Version] Available: http://www.pfsense.org/index.php?option=com_frontpage&Itemid=1 (2012, Desember 22)
13. *Scheiner, Bruce. (2000) Attack Trees : Modeling Security Threats. Dr. Dobb's Journal,* [Electronic version]. Available : http://www.schneier.com/paper-attacktrees-ddj-ft.html (Jumat, 11 November 2012)
14. Sprengers, Martijn (2011). *GPU-based Password Cracking On the Security of Password Hashing Schemes regarding Advances in Graphics Processing Units,* [Electronic version] available : http://www.ru.nl/publish/pages/578936/thesis.pdf (2013, Januari 3)