

AUTOMATION FRAMEWORK FOR ROGUE ACCESS POINT MITIGATION IN IEEE 802.1X-BASED WLAN

¹NINKI HERMADUANTI, ²IMAM RIADI

¹Department of Informatics Engineering, Islamic University of Indonesia, Yogyakarta, Indonesia

²Department of Information System, Ahmad Dahlan University, Yogyakarta, Indonesia

E-mail: ¹ninki.hermaduant@gmail.com, ²imam.riadi@is.uad.ac.id

ABSTRACT

Wi-Fi hotspot is a product of wireless network technology than can be easily found in public places such as airport, café, or shopping mall. Besides offering ease in connection, the use of wireless network technology is also raises security issue because it lies in an open or public area. There needs to be a mechanism that can control access to the wireless network to protect it from attacker or intruder. Port-based authentication system or known as IEEE 802.1X standard is a framework that provides access control to the network. But still it is possible for the attack to occur in wireless network environment protected by IEEE 802.1X, i.e. rogue Access Point (rogue AP). A rogue AP can act like authorized Access Point (authorized AP), deceiving wireless users. Therefore, it is necessary to do mitigation steps including detection and elimination of rogue AP. In this research, live forensics method is used to detect the rogue AP. Output of this research is a framework for mitigating rogue AP in an IEEE 802.1X-based Wireless Local Area Network (WLAN). This framework can also be used as a basic for doing automation process to mitigate rogue AP, helping the network administrators to minimize their manual tasks for handling the rogue AP.

Keywords: *Framework, Rogue, Access Point, Forensics, IEEE 802.1X*

1. INTRODUCTION

Internet wireless as a product of wireless network technology now are often used. Besides offering ease in connection, the use of wireless network technology is also caused some security issues and should be considered because it is located in open public area [1].

The security issues sparked the mechanism to control access to the network in order to protect it from intruders. IEEE 802.1X is known as port-based authentication system, a framework that provides access control to the network that verifies client's information such as username and password. If the information is valid, then the client is allowed to access the network [2]. At first, IEEE 802.1X was only designed to meet the needs of security on wired networks with coverage Local Area Network (IEEE 802 LAN), but as the development of technology, IEEE 802.1X was also developed to meet the security needs of the wireless network with coverage of Wireless Local Area Network (IEEE 802.11 LAN) or referred to as WLAN [3]. Encryption which is used in IEEE 802.1X-based WLAN is WPA-Enterprise [4] or WPA2-Enterprise using RADIUS (*Remote Authentication Dial-In User Service*) server as an

authentication server to authenticate the client to the network using a username and password [5].

Application of IEEE 802.1X standard is intended to provide device authentication mechanism used by the client to the WLAN. However, although the IEEE 802.1X standard has been applied, it is still possible for the attack to occur. There are various attacks that can be performed on WLAN, including IEEE 802.1X-based WLAN. Among them are war driving [6], Denial of Service (DoS) attack [7], and rogue Access Point (rogue AP) as a rogue authenticator that masquerades as an authorized Access Point, which is dangerous, given the rogue AP can be used to obtain client data and gain access to the network [2].

The number of attacks that might occur in wireless networks that one of them is a rogue AP, making the need to do mitigation for rogue AP case, which means doing activities to lower impacts or risks that may arise due to the existence of rogue AP. The nature of rogue AP masquerading as authenticator device [2], making it difficult to distinguish it from the legitimate one, so the first step in mitigating the rogue AP case is to detect the presence of rogue AP [8]. Detection of rogue AP as part of the mitigation steps can be done with live forensics analysis approach, a forensic method to



gather information, analyze and present them using a variety of forensic tools while the system is still running [9]. Live forensics can also be done in case there is intrusion on the system or network to secure volatile evidence on the running system during the process of investigation [10].

Detection of rogue AP in this research is adopted from several studies that have been done before, namely:

1. Comparison of SSID, signal strength, and IP address [11].
2. RAPD algorithm by sniffing traffic and comparing the result with authorized AP data [12].
3. Comparison of various parameters, such as SSID, MAC address, authentication type, channel, frequency, and signal. If a lot of the same parameters, it can be concluded that the Access Point is a rogue AP [13].

Previous studies have not been done in IEEE 802.1X-based WLAN environment, but this research uses IEEE 802.1X-based WLAN as the object. Adoption of rogue AP detection method of the three studies previously mentioned will be developed with the additional parameter of protocol used in IEEE 802.1X-based WLAN. The main contribution in this research is the enhancement of rogue AP detection using parameter of protocol used in IEEE 802.1X-based WLAN.

Therefore, the topic raised in this research is rogue AP mitigation in IEEE 802.1X-based WLAN, including Authorized AP Data Population step, Rogue AP Detection step and Rogue AP Elimination step. Expected output in this research is a mitigation framework for rogue AP case in IEEE 802.1X-based WLAN. This framework can be used as a basis to automate processes in mitigating the rogue AP case. Automation is done with the aim to help network administrators minimize manual tasks carried in mitigation process of rogue AP case in IEEE 802.1X-based WLAN.

The remaining sections are structured as follows: Section 2 presents the basic theory of live forensics, IEEE 802.1X, and rogue AP. Section 3 discusses methodology used in this research. Section 4 explains the result of this research. Finally, Section 5 gives a conclusion to the whole research and the further work.

2. BASIC THEORY

2.1 Live Forensics

Live forensics is conducted by collecting data when the system exposed to attack is still running.

Forensic data gathered through a live system can provide the evidence that cannot be obtained from the static disk image. The data collected is a representation of a dynamic system and is unlikely to be reproduced the next time [14].

Live forensics can bring out some concerns, such as this method should not modify the target system in order to go undetected by the intruder, the target system to be investigated should not normally be shut down or restarted for a long period of time, other than that the whole procedure of live forensics should not affect normal services running on the target system [15].

Although there are some concerns with live forensics, when conducting an investigation on the network, this method can be used to obtain as much information about the activities going on in the network. Investigators can put up a packet sniffer to capture traffic running on the network and analyze them [16]. Tools such as NetworkMiner, tcpflow, Wireshark and NetSleuth can be used in the live forensics in network environment [9].

2.2 IEEE 802.1X

2.2.1 IEEE 802.1X Components

Three components are necessary to form a 802.1X authentication mechanism on the network. These components are as follows [2]:

1. Supplicant (Client)
User's devices which need to be authenticated before accessing the network, such as laptops or IP phones.
2. Authenticator
Network devices that work at Layer 2, such as Ethernet switches in a wired network or Access Point in a wireless network. Authenticator acts as a gateway between the supplicant and the network to be accessed by the supplicant.
3. Authenticator Server
The server that handles supplicant authentication. RADIUS server is often used in the implementation of IEEE 802.1X-based network, so it is known in the networking industry as a standard for authentication server.

2.2.2 IEEE 802.1X Protocol

EAP (Extensible Authentication Protocol) is a protocol commonly used for user authentication in IEEE 802.1X-based network [17]. However, EAP is actually more correct to say as a framework of communication between the client and the server, and the protocols used in the communication can be selected from the available protocols in the EAP framework itself. The client and the server must use

the same protocol for authentication and communication [18].

Some of the existing protocols within the EAP framework, also known as the EAP methods that commonly used to communicate within the IEEE 802.1X-based network are as follows [18]:

1. EAP-MD5
MD5 protocol exists on the client side converts client password into an MD5 hash and forwards it to the server. The server that receives MD5 hash of client password will compare it with the MD5 hash value that has been stored on the server. The comparison will determine whether or not the client can log in.
2. EAP-LEAP
LEAP (Lightweight Extensible Authentication Protocol) is a protocol developed by Cisco to address the weaknesses in WEP.
3. EAP-TLS
TLS (Transport Layer Security) works under the Digital Certificate.
4. EAP-TTLS
TTLS (Tunnel Transport Layer Security) was developed to overcome the weaknesses in TLS that require Digital Certificates for client and server. TTLS requires only Digital Certificate for server.
5. EAP-PEAP
PEAP (Protected Extensible Authentication Protocol) is also referred to as EAP inside EAP. PEAP uses a server certificate to check the validity of the server. When PEAP client validates the server by server certificate, it then forms a secure tunnel. Client validation process can begin with whichever EAP Method. And this EAP Method is protected by TLS.

Figure 1 shows the relation between EAP protocol and IEEE 802.1X components.

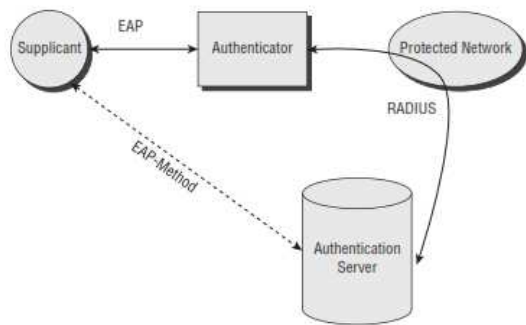


Figure 1: EAP and IEEE 802.1X Component [2]

2.3 Rogue AP

Rogue AP generally refers to unauthorized Access Point [19]. The existence of rogue AP can

be a serious threat in the organization's network, because it has the potential to open access for unauthorized parties who may intend to steal confidential information or even perform DoS attack [20]. Rogue AP can be a wireless Access Point that allows an intruder to do man in the middle attack [21]. Wireless media used by WLAN communication can allow eavesdropping attack to find out the wireless data communication occurs in WLAN [22]. Rogue AP can be configured similar to the authorized AP. This causes evil twin attack. Attacker can find out the relevant information about a legitimate AP through knowledge or reconnaissance [23]. When user connects to a rogue AP, the intruder can monitor and capture user's network traffic [24].

Figure 2 shows the possible attacks caused by rogue AP existence in an organization's network.

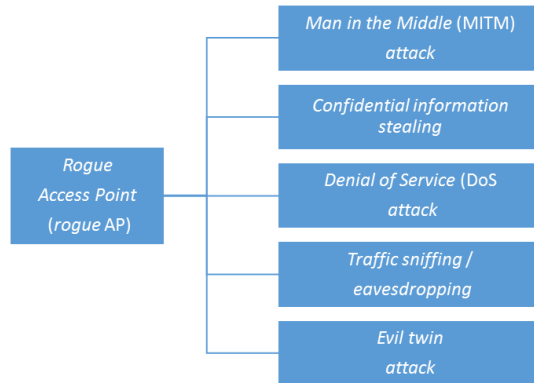


Figure 2: Attacks Caused by Rogue Access Point

3. METHODOLOGY

Mitigation of rogue AP case in IEEE 802.1X-based WLAN comprising the steps of the Authorized AP Data Population, Rogue AP Detection and Rogue AP Elimination. Authorized AP Data Population step is conducted only if there are authorized AP changes in the network. Rogue AP Detection step is conducted using live forensics. Rogue AP Elimination step is conducted for rogue AP containment. Framework for rogue AP mitigation is developed based on rogue AP mitigation steps mentioned. This framework will serve as the basis for implementing automation of rogue AP mitigation in IEEE 802.1X-based WLAN.

3.1 Authorized AP Data Population

Authorized AP Data Population is conducted if there is a change in the network in order to update authorized AP data properly. If there is a freshly

installed authorized AP, then the authorized AP data will be added. Conversely, if there is an authorized AP removed from the network, then the data will be deleted.

3.2 Rogue AP Detection

Rogue AP Detection is conducted using live forensics where system is still running. Rogue AP Detection step consists of several processes:

1. Capture

Has two subprocesses, namely Access Point scanning and wireless traffic capture. Access Point scanning aims to determine the existence of Access Point broadcasting SSID. The desired information is SSID name, Access Point MAC address, the channel used, signal strength (power), and encryption type used by the SSID. While the wireless traffic capture aims to determine whether there is an EAP used by SSID and EAP type used, if any. For this purpose, the delivery of EAP packet must be triggered in order to capture the EAP packet.

2. Note

Records the parameters required in Rogue AP Detection step. Data extraction is conducted from the result of Access Point scanning subprocess in the Capture process to get several parameters, such as SSID name, MAC address, channel, power, and encryption type used by SSID. In addition, parameter of EAP type will be needed and this can be obtained from the result of wireless traffic capture analysis in the Analyze process. All of these parameters will be recorded into a table in a file, which has SSID, BSSID (MAC Address), Channel, Power, Encryption and EAP Type column.

3. Analyze

Analyzes a wireless traffic capture file obtained from the Capture process to determine the EAP type used. The parameter of EAP type is then recorded through the Note process.

4. Report

Produces Access Point data after the Capture, Note and Analyze processes conducted. The Report process also determines which Access Point is rogue AP. Comparison needs to be done between Access Point data gathered from detection step and authorized AP data gathered in population step. At first, Access Point data gathered from the detection step are categorized as unauthorized AP. Then the rogue AP data will be determined through rules of comparison as shown in Figure 3:

- a. Rogue AP's SSID name is the same as authorized AP's SSID name.
- b. Rogue AP's MAC address is different from authorized AP's MAC address.
- c. Rogue AP's channel can be the same as or different from authorized AP's channel. Access Point usually configured to use channel 1, 6 or 11 to avoid interference [25].
- d. Signal strength (power) transmitted by rogue AP is in good range do basic connectivity with minimum signal -80 dBm [26].
- e. Rogue AP's encryption type is the same as authorized AP's encryption type.
- f. Rogue AP's EAP type is the same as authorized AP's EAP type.

Access Point will be categorized as a neighbor AP if not all of the rules are met.

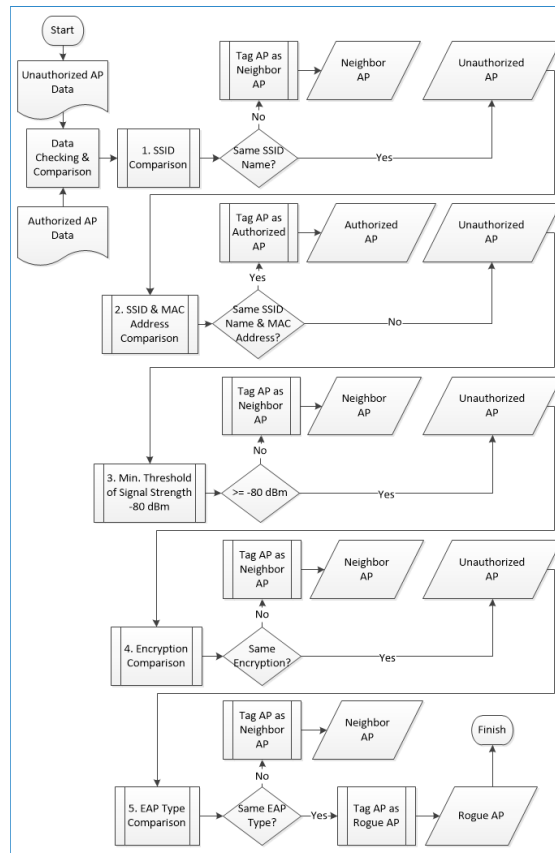


Figure 3: Unauthorized AP and Authorized AP Data Comparison Flowchart

From the steps described previously, namely the Authorized AP Data Population step and Rogue AP Detection step, the process and subprocesses involved can be presented as shown in Figure 4.



Figure 4: Authorized AP Data Population Step and Rogue AP Detection Step

3.3 Rogue AP Elimination

Rogue AP elimination step includes monitoring process whether a client connected to the rogue AP and rogue AP containment process. Assuming that the rogue AP has been detected, then the steps of elimination can be described as follows:

1. Examination of whether or not a client is connected to a rogue AP, conducted by capturing rogue AP traffic using parameters of MAC address and channel.
2. Rogue AP containment aiming to disable rogue AP so it cannot serve the client request to make a connection. Containment is done through a deauthentication process. The goals are:
 - a. To disconnect the client from the rogue AP.
 - b. To send DoS packets to disable rogue AP's service.
3. Examination of whether there is still client connected to a rogue AP.

4. RESULT

4.1 Rogue AP Case Simulation

Case simulation will be run by setting up a software-based rogue AP using Hostapd-WPE and FreeRADIUS-WPE tools. Although based on software, it is still necessary to use hardware, such as wireless card or wireless adapter to broadcast SSID and monitor wireless traffic passing by. Figure 5 shows the topology run in this research.

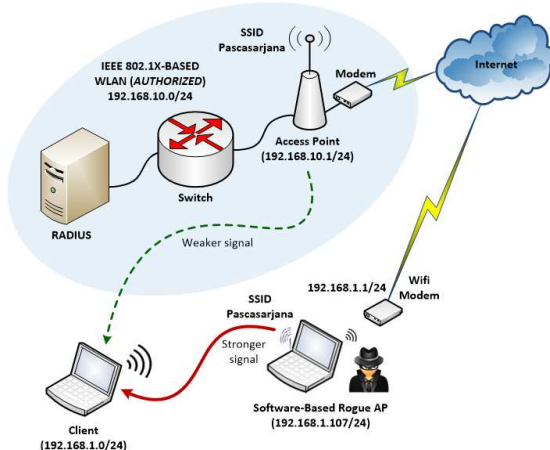


Figure 5: Network Topology for Rogue AP Simulation

This research uses EAP-PEAP (Protected Extensible Authentication Protocol). The reason EAP-PEAP selected in this research is because EAP-PEAP only requires a certificate from the server side [27], so it can avoid the issues associated with the installation of digital certificate on each client [28]. EAP-PEAP is also a password-based EAP, which is easier to manage [27], as well as more suitable for the case simulation in this research where rogue AP can be used to obtain username and challenge/response of client password, then a program can crack it and obtain the password in clear text format.

Figure 6 shows username and challenge/response of client password obtained from rogue AP. Meanwhile, Figure 7 shows challenge/response of client password cracked using Asleap tool.

```

root@blackhat:/home/master
root@blackhat:~/home/master# tail -f /usr/local/var/log/radius/freeradius-server-wpe.log
response: 88:02:34:19:02:bb:3e:e6:3f:69:6c:f1:4b:e2:98:26:5c:30:9a:3b:85
:98:95:b5
john NETNTLM: ninkyhade:$NETNTLM$65eac87425166cfd98802341902bb3ee63f696c
f14be298265c309a3bb59895b5
mschap: Mon Aug 1 11:26:37 2016
username: didan
challenge: bc:8b:66:97:c9:cc:95:05
response: d0:d5:96:81:1c:23:4e:93:59:b2:cd:25:93:01:9a:e7:2a:b1:e3:47:09
:8f:dc:ac
john NETNTLM: didan:$NETNTLM$bc8b6697c9cc95058d0d596811c234e9359b2cd2593
019ae72ab1e347098fdcac
    
```

Figure 6: Username and Challenge/Response of Client's Password Obtained from Rogue AP

```

root@blackhat:/home/master
username: didan
challenge: bc:8b:66:97:c9:cc:95:05
response: d0:d5:96:81:1c:23:4e:93:59:b2:cd:25:93:01:9a:e7:2a:b1:e3:47:09
:8f:dc:ac
john NETNTLM: didan:$NETNTLM$bc8b6697c9cc95058d0d596811c234e9359b2cd2593
019ae72ab1e347098fdcac
^C
root@blackhat:~/home/master# asleap didan -C bc:8b:66:97:c9:cc:95:05 -R d0:d5:96:
81:1c:23:4e:93:59:b2:cd:25:93:01:9a:e7:2a:b1:e3:47:09:8f:dc:ac -W rockyou.txt
asleap 2.2 - actively recover LEAP/PPTP passwords. <jwright@hasborg.com>
Using wordlist mode with "rockyou.txt".
hash bytes:      586c
NT hash:         8846f7eaaa8fb117ad06bdd830b7596c
password:        password
    
```

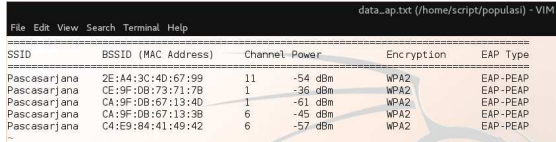
Figure 7: Cracking Challenge/Response of Client's Password Using Asleap Tool

4.2 Mitigation of Rogue AP Case

Given the dangers of rogue AP's threat, the rogue AP mitigation measures needs to be done, either manually or automatically in order to know the

difference. Mitigation includes the steps of Authorized AP Data Population, Rogue AP Detection in IEEE 802.1X-based WLAN with live forensics and Rogue AP Elimination.

As mentioned before, Authorized AP Data Population step is conducted only if there is a change in the network. It is performed using the Generate Access Point Data phase which produces authorized AP data as presented in Figure 8.



SSID	BSSID (MAC Address)	Channel	Power	Encryption	EAP Type
Pascasarjana	2E:A4:3C:4D:67:99	11	-54 dBm	WPA2	EAP-PEAP
Pascasarjana	CE:9F:0B:73:71:7B	1	-36 dBm	WPA2	EAP-PEAP
Pascasarjana	CA:9F:0B:67:13:4D	1	-61 dBm	WPA2	EAP-PEAP
Pascasarjana	CA:9F:0B:67:13:3B	6	-49 dBm	WPA2	EAP-PEAP
Pascasarjana	C4:E9:84:41:49:42	6	-57 dBm	WPA2	EAP-PEAP

Figure 8: Authorized AP Data Obtained from Generate AP Data Phase in Authorized AP Data Population Step

The Rogue AP Detection step also uses Generate Access Point Data Phase. The difference is the Generate Access Point Data phase in Authorized

AP Data Population step produces authorized AP data, while the Generate Access Point Data phase in Rogue AP Detection step produces unauthorized AP data, shown in Figure 9.



SSID	BSSID (MAC Address)	Channel	Power	Encryption	EAP Type
Pascasarjana	68:E3:27:08:5D:2F	1	-32 dBm	WPA2	EAP-PEAP
PLEMBURAN26	78:E8:86:D5:E7:24	11	-23 dBm	WPA	None
Pascasarjana	C4:E9:84:41:49:42	6	-47 dBm	WPA2	EAP-PEAP
hotspot	00:23:69:35:89:9C	6	-82 F6	WPA	None

Figure 9: Unauthorized AP Data Obtained from Generate AP Data Phase in Rogue AP Detection Step

The differences between processes involved in Generate Access Point Data phase in Authorized AP Data Population step and Generate Access Point Data phase in Rogue AP Detection step both manually and automatically are presented in Table 1.

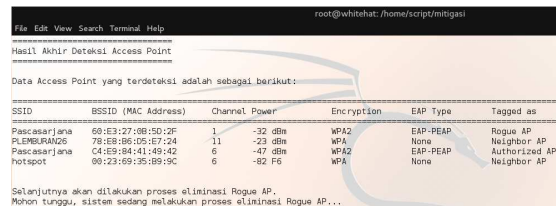
Table 1: The Differences Between Generate AP Data Phase in Authorized AP Data Population Step and Rogue AP Detection Step

Process	Authorized AP Data Population Step		Rogue AP Detection Step	
	Manual	Automation	Manual	Automation
Capture	AP Scanning	AP Scanning	AP Scanning	AP Scanning
Note	Data Extraction from AP Scanning Result	Data Extraction from AP Scanning Result	Data Extraction from AP Scanning Result	Data Extraction from AP Scanning Result
Note	Recording of Data Extraction Result	-	Recording of Data Extraction Result	-
Capture	Wireless Traffic Capture	Wireless Traffic Capture	Wireless Traffic Capture	Wireless Traffic Capture
Analyze	Analysis of Wireless Traffic Capture File	Analysis of Wireless Traffic Capture File	Analysis of Wireless Traffic Capture File	Analysis of Wireless Traffic Capture File
Note	Recording of Data Analysis Result	Recording of Data Extraction & Data Analysis Result	Recording of Data Analysis Result	Recording of Data Extraction & Data Analysis Result
Report	Authorized AP Data	Authorized AP Data	Unauthorized AP Data	Unauthorized AP Data

The next step after Generate Access Point Data phase produces unauthorized AP data is the Report process with subprocess of data comparison between unauthorized AP and authorized AP in order to determine which Access Point is the rogue AP. The rules used in data comparison are mentioned in Section 3.2 and showed by Figure 3.

Parameters for comparison used in this research are SSID, MAC address, signal strength, encryption type, and EAP type. IP address [11] as in Layer 3 (Network) is excluded because detection of rogue AP is conducted in Layer 2 (Data Link). Channel and frequency [13] are also excluded because whatever channel and frequency used, rogue AP can still run. These findings simplify the use of parameters in data comparison and with only one additional parameter, namely EAP type because

rogue AP simulation is conducted in IEEE 802.1X-based WLAN environment.



SSID	BSSID (MAC Address)	Channel	Power	Encryption	EAP Type	Tagged as
Pascasarjana	68:E3:27:08:5D:2F	1	-32 dBm	WPA2	EAP-PEAP	Rogue AP
PLEMBURAN26	78:E8:86:D5:E7:24	11	-23 dBm	WPA	None	Neighbor AP
Pascasarjana	C4:E9:84:41:49:42	6	-47 dBm	WPA2	EAP-PEAP	Authorized AP
hotspot	00:23:69:35:89:9C	6	-82 F6	WPA	None	Neighbor AP

Figure 10: Final Result of Unauthorized AP and Authorized AP Data Comparison

Figure 10 shows the final result of data comparison subprocess, which determine the rogue AP. The next step after Rogue AP Detection step is Rogue AP Elimination step. First, Rogue AP

monitoring must be conducted using Airmo-ng tool with parameters of MAC address and channel to determine whether or not there is a client connected to the rogue AP, as shown in Figure 11.

```

root@whitehat: /home/script/mitigasi
File Edit View Search Terminal Help
CH 1 ]] Elapsed: 12 s ]] 2016-08-11 14:23
BSSID PWR RXQ Beacons #Data, #s CH MB ENC CIPHER AUTH ESSID
60:E3:27:08:50:2F -28 100 118 6 0 1 11 WPA2_CCMP MGT Pascasarjana
BSSID STATION PWR Rate Lost Frames Probe
60:E3:27:08:50:2F E0:B9:BA:32:04:60 -42 11 -11 0 4
Rogue AP MAC Address Rogue AP's Client MAC Address
    
```

Figure 11: Rogue AP Monitoring Process Before Conducting Containment Process

Next is rogue AP containment by sending deauthentication packets using Aireplay-ng tool with MAC address parameter to disconnect client from rogue AP and to disable rogue AP so it cannot serve the client connection requests to the rogue AP, as shown in Figure 12. Then do the monitoring process again using Airmo-ng tool to check whether or not there is still a client connected to the rogue AP, as shown in Figure 13.

```

root@whitehat: /home/script/mitigasi
File Edit View Search Terminal Help
root@whitehat: /home/script/mitigasi# aireplay-ng -0 50 -a 60:E3:27:08:50:2F -wlan1mon
14:39:48 Waiting for beacon frame (BSSID: 60:E3:27:08:50:2F) on channel 1
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
14:39:48 Sending DeAuth to broadcast -- BSSID: [60:E3:27:08:50:2F]
14:39:49 Sending DeAuth to broadcast -- BSSID: [60:E3:27:08:50:2F]
14:39:49 Sending DeAuth to broadcast -- BSSID: [60:E3:27:08:50:2F]
14:39:50 Sending DeAuth to broadcast -- BSSID: [60:E3:27:08:50:2F]
14:39:50 Sending DeAuth to broadcast -- BSSID: [60:E3:27:08:50:2F]
14:39:51 Sending DeAuth to broadcast -- BSSID: [60:E3:27:08:50:2F]
14:39:51 Sending DeAuth to broadcast -- BSSID: [60:E3:27:08:50:2F]
14:39:52 Sending DeAuth to broadcast -- BSSID: [60:E3:27:08:50:2F]
14:39:52 Sending DeAuth to broadcast -- BSSID: [60:E3:27:08:50:2F]
14:39:53 Sending DeAuth to broadcast -- BSSID: [60:E3:27:08:50:2F]
14:39:53 Sending DeAuth to broadcast -- BSSID: [60:E3:27:08:50:2F]
14:39:54 Sending DeAuth to broadcast -- BSSID: [60:E3:27:08:50:2F]
    
```

Figure 12: Rogue AP Containment Process by Sending Deauthentication Packet

```

root@whitehat: /home/script/mitigasi
File Edit View Search Terminal Help
CH 1 ]] Elapsed: 12 s ]] 2016-08-11 14:45
BSSID PWR RXQ Beacons #Data, #s CH MB ENC CIPHER AUTH ESSID
60:E3:27:08:50:2F -21 100 124 0 0 1 11 WPA2_CCMP MGT Pascasarjana
BSSID STATION PWR Rate Lost Frames Probe
    
```

Figure 13: Rogue AP Monitoring Process After Conducting Containment Process

4.3 Rogue AP Mitigation Framework

Rogue AP mitigation framework can be developed following a case simulation and rogue AP mitigation. Framework for manually conducting rogue AP mitigation can be seen in Figure 14, whereas framework for automatically conducting rogue AP mitigation is shown in Figure 15.



Figure 14: Automation Framework for Rogue AP Mitigation



Figure 15: Automation Framework for Rogue AP Mitigation

5. CONCLUSION

Automation framework for rogue AP mitigation is developed after learning how to conduct rogue AP mitigation manually. This automation framework uses three steps. One, Authorized AP Data Population step using Generate Access Point Data phase that produces authorized AP data. Two, Rogue AP Detection step using live forensics which includes the processes of Capture (Access Point scanning), Note (data extraction of Access Point scanning result), Capture (wireless traffic capture including EAP packet trigger), Analyze (analyze wireless traffic capture file), Note (recording of data extraction and analysis results) and Report (rogue AP data). And three, Rogue AP Elimination step through the monitoring and containment of rogue AP.

The automation framework can serve as a basis in building a script that can automate the steps of rogue AP mitigation. In this research, rogue AP in IEEE 802.1X-based WLAN is proved to be detected and eliminated. However, this framework does not cover detection of rogue AP using MAC spoofing. Furthermore, improvement with detection of rogue AP using MAC spoofing will be made in future work.

REFERENCES:

- [1] A. Faqih, A. F. Rochim, and R. R. Isnanto, "Hotspot Management System Based on Time Quota and Data Packet", 2012. [Online]. Available <http://eprints.undip.ac.id/32541/>.
- [2] J. Geier, *Implementing 802.1X Security Solutions for Wired and Wireless Networks*, Indianapolis: Wiley Publishing, Inc., 2008.
- [3] I. Networks, "Introduction to 802.1X for Wireless LANs (Vol. 1)", 2006. [Online]. Available http://www.interlinknetworks.com/whitepapers/Intro_802_1X_for_Wireless_LAN.pdf.
- [4] S. Sukhija and S. Gupta, "Wireless Network Security Protocols: A Comparative Study", *International Journal of Emerging Technology and Advanced Engineering*, Vol. 2, No. 1, 2012, pp. 357–364.
- [5] C. Hoffman, "WPA2, WEP, and Friends: What's the Best Way to Encrypt Your Wi-Fi?", 2013. [Online]. Available <http://www.makeuseof.com/tag/wpa2-wep-and-friends-whats-the-best-way-to-encrypt-your-wi-fi/>. [Accessed: November 16, 2015].



- [6] L. Jacob, D. Hutchinson, and J. Abawajy, "Wi-Fi Security: Wireless with Confidence", *Proceedings of the 4th Australian Security and Intelligence Conference*, 2011, pp. 88–96.
- [7] O. Ozan, "Denial of Service Attacks on 802.1X Security Protocol", Naval Postgraduate School, Monterey (California), 2004. [Online]. Available <http://www.dtic.mil/dtic/tr/fulltext/u2/a422412.pdf>.
- [8] I. H. Saruhan, "Detecting and Preventing Rogue Devices on the Network", 2007. [Online]. Available <https://www.sans.org/reading-room/whitepapers/detection/detecting-preventing-rogue-devices-network-1866>.
- [9] M. Rafique and M. N. A. Khan, "Exploring Static and Live Digital Forensics: Methods, Practices and Tools", *International Journal of Scientific and Engineering Research*, Vol. 4, No. 10, 2013, pp. 1048–1056.
- [10] J. T. Luttgens, M. Pepe, and K. Mandia, *Incident Response & Computer Forensics (3rd ed.)*, McGraw-Hill Education, 2014.
- [11] S. Jagtap and K. N. Honwadkar, "Rogue Access Point Detection in WLAN by Analyzing Network Traffic and Behavior", *International Journal of Computer Applications*, Vol. 1, No. 22, 2010, pp. 27–29.
- [12] S. Thakur and A. Bodhe, "RAPD Algorithm: Detection of Rogue Access Point in Wireless Network", *International Journal of Emerging Technology and Advanced Engineering*, Vol. 3, No. 6, 2013, pp. 85–89.
- [13] A. A. Chougule, S. B. Vanjale, and P. B. Mane, "Detection and Prevention of Rogue Access Point in the 802.11 Using Various Parameters", *International Journal of Advanced Research in Computer Science and Software Engineering*, Vol. 5, No. 5, 2015, pp. 1723–1727.
- [14] F. Adelstein, "Diagnosing Your System without Killing It First", *Communications of the ACM*, Vol. 49, No. 2, 2006, pp. 63–66.
- [15] Y. Cheng, X. Fu, X. Du, B. Luo, and M. Guizani, "A Lightweight Live Memory Forensic Approach Based on Hardware Virtualization", Elsevier, 2016, doi: 10.1016/j.ins.2016.07.019.
- [16] A. Reyes, K. O'shea, J. Steele, J. R. Hansen, B. R. Jean, and T. Ralph, "Incident Response: Live Forensics and Investigations", *Cyber Crime Investigations*, Elsevier, 2007, pp. 89–109.
- [17] J. C. Chen and Y. P. Wang, "Extensible Authentication Protocol (EAP) and IEEE 802.1X: Tutorial and Empirical Experience", *IEEE Communications Magazine*, Vol. 43, No. 12, 2005, pp. 26–32.
- [18] U. Kumar, P. Kumar, and S. Gambhir, "Analysis and Literature Review of IEEE 802.1X (Authentication) Protocols", *International Journal of Engineering and Advanced Technology*, Vol. 3, No. 5, 2014, pp. 163–168.
- [19] P. G. Sasane and S.K. Pathan, "Detecting and Eliminating Rogue Access Points in IEEE-802.11 WLAN - A Multi-Agent Sourcing Methodology", *International Journal of Sciences: Basic and Applied Research*, Vol. 3, No. 1, 2011, pp. 9–15.
- [20] G. Shivaraj, M. Song, and S. Shetty, "A Hidden Markov Model Based Approach to Detect Rogue Access Points", *IEEE Military Communications Conference*, 2008, pp. 1–7.
- [21] S. Shetty, M. Song, and L. Ma, "Rogue Access Point Detection by Analyzing Network Traffic Characteristics", *IEEE Military Communications Conference*, 2007, pp. 1–7.
- [22] S. Jadhav, S. Vanjale, and P. B. Mane, "Detecting Fake Access Point into Wireless Network Using Clock Skews as Fingerprinting Technique", *International Journal of Advanced Research in Computer Science and Software Engineering*, Vol. 4, No. 7, 2014, pp. 26–31.
- [23] V. V. Nanavare and V. R. Ghorpade, "A Survey on Evil Twin Access Point Detection Technique", *International Journal of Innovative Research in Computer and Communication Engineering*, Vol. 4, No. 3, 2016, pp. 4381–4386.
- [24] S. Nikbakhsh, A. B. A. Manaf, M. Zamani, and M. Janbeglou, "A Novel Approach for Rogue Access Point Detection on the Client-Side", *26th International Conference on Advanced Information Networking and Applications Workshops*, 2012, pp. 684–687.
- [25] Metageek, "Why Channels 1, 6 and 11?". [Online]. Available <http://www.metageek.com/training/resources/why-channels-1-6-11.html>. [Accessed: July 12, 2016].
- [26] Metageek, "Understanding RSSI". [Online]. Available <http://www.metageek.com/training/resources/understanding-rssi.html>. [Accessed: July 12, 2016].



- [27] K. Sankar, A. Balinsky, D. Miller, and S. Sundaralingam, "EAP Authentication Protocols for WLANs", 2005. [Online]. Available
<http://www.ciscopress.com/articles/article.asp?p=369223&seqNum=2>. [Accessed: June 12, 2016].
- [28] Cisco, "Cisco Protected Extensible Authentication Protocol, 2016. [Online]. Available
http://www.cisco.com/c/en/us/products/collateral/wireless/aironet-1200-series/prod_qas0900aecd801764fa.html. [Accessed: June 12, 2016].