Analysis of Deauthentication Attack on IEEE 802.11 Connectivity Based on IoT Technology Using External Penetration Test

Yogi Kristiyanto[1*] and Ernastuti[2]
[1]Management Information System Department, Gunadarma University
Depok 16424, Indonesia
[2]Computer Science Department, Faculty of Computer Science and Information Engineering, Gunadarma University
Depok 16424, Indonesia
Email: [1]yogi.kristiyanto@gmail.com, [2]ernas@staff.gunadarma.ac.id

***Abstract*—The research aims to know the level of security of WiFi connectivity against deauthentication attacks on Internet of Things (IoT)-based devices. It is done through testing using an external penetration test method. The external penetration test simulates a real external attack without information about the target system and network given. The process starts from accessing the device through Internet or WiFi by the test target. At the same time, the attacker performs Denial-of-Service (DoS) attacks on WiFi. The attacker uses Arduino ESP8266 NodeMCU WiFi with Lua programming. To record WiFi activities, the researchers use CommView for WiFi V. 7.0, and the target is Internet Protocol (IP) camera device. The result shows that the communication of the test target with the gateway is lost, but the Media Access Control (MAC) of the test target is still registered at the gateway. Deauthentication attacks cause communication paralysis, and several changes occur, such as an increase in data rate, and change in frequency channel, Distribution System (DS) status, retry bits in frame management, and the sequence number.**

***Index Terms*—Deauthentication Attack, Internet of Things (IoT), External Penetration Test**

I. Introduction

INTERNET of Things (IoT) is a new paradigm that includes smart object networks. Those are embedded sensors using the Internet [1]. Most IoT and IoT network devices depend on wireless technology. The choice of wireless technology is closely related to the success of IoT networks. IoT devices consist mainly of three layers. There are application layer, network layer, and perception layer. In the perception layer, IoT devices have a strong relationship with sensors, Radio-Frequency Identification (RFID), Wireless Sensor Networks (WSN) such as WiFi [2]. WiFi systems are widely used in homes, factories, offices, and many public places as Internet access points, and the starting point for many Internet gateways that will be needed to complete IoT coverage. WiFi is the obvious choice for IoT connectivity because its coverage in buildings is almost everywhere now. However, it is not always the right choice in the category of reliability and security. The IEEE 802.11 protocol is still classified as vulnerable as these security gaps affect the work of IoT technology [3].

IEEE 802.11 networks or WiFi connectivity use radio waves to send information wirelessly over a LAN. Its reach can be extended by expanding WiFi coverage. The IoT model that appears "smart" by connecting sensors via WiFi to cloud services and managing them and data traffic. Then, this service offers a portal for analytic and smartphone-based user controls. IoT sensors must be configured to connect it to WiFi using three parameters. Those are network discovery, authentication, and device identity [4].

The fast development of the IEEE 802.11 networks has become the main target of attackers. They attack for various reasons, ranging from simple entertainment to cyber-terrorist attacks or making a profit. It is possible mainly because of wireless transmission media. It is proven to be far more vulnerable than traditional wired networks [5].

The type of Denial-of-Service (DoS) attack on WiFi can cause communication paralysis between connected devices. The process of this attack occurs in the authentication. It is done by sending broadcast addresses and changing broadcast addresses on targets attacked. In this case, the devices are connected through WiFi. This

Received: Mar. 17, 2020; received in revised form: May 05, 2020; accepted: May 05, 2020; available online: May 18, 2020.
*Corresponding Author

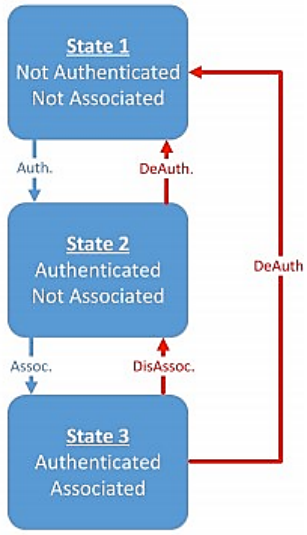

Fig. 1. Authentication state machine [8].

Fig. 2. Penetration test phases [11].

attack is called deauthentication. The absence of secure authentication also uncovers the devices to many other security threats that may lead to malicious attacks such as DoS attacks [6]. DoS attacks on WiFi are mainly caused by frame management authentication, association, deauthentication, and forged disassociation. In general, DoS attacks on WiFi can be classified into two categories, one of which refers to attacks the target. They are authentication blocking attacks and association flooding attacks [7].

Deauthentication is the most common form of the IEEE 802.11 DoS protocol. Previously, authentication requests a connection. After successful authentication consisting of two acknowledged authentication frames, the client station will request the association. Association response frames follow frame request association. Each frame is also recognized. The next step depends on the type of security used on WiFi and determines how intrusive the deauthentication attack is. Then, all Layer 2 management frames are broadcasted in plain text so that the closest device can find the network and request a connection. Many security problems arise from this lack of protection. If an attacker captures this plaintext management frame, she/he can fake a package that seems to come from the victim [8]. This process can be seen in Fig. 1.

All packets transmitted over IEEE 802.11 network have homogeneous headers. Those help the attacker to guess the first eight bytes of the headers [9]. The IEEE 802.11 encryption schemes do not encrypt the management and control frames, making them vulnerable to spoong attacks. The deauthentication frame is a management frame. It is sent in plain-text which guarantees faster processing and low computation for the Access Point (AP). However, spoofing plain-text frames are trivial. As deauthentication frames are sent in plain-text, AP cannot verify the authenticity of these frames. As a result, the AP processes spoofed the deauthentication frame(s) [10].

Based on the background, the research aims to know the level of security of IEEE 802.11 or WiFi connectivity against deauthentication attacks on IoT-based devices. It is done through testing using an external penetration test method. The results are expected to provide information for mitigating deauthentication attacks using the external penetration test.

II. Research Method

The penetration test is a method for actively evaluating and assessing network security or information systems. It is done by simulating attacks from the attacker's perspective. It is used by an attacker to gain unauthorized access to the organization's network system and take unwanted actions [12]. The external penetration test is also known as the black box penetration test. It tries to simulate a real external attack without information about the target system and network given to the examiner. The phases of a penetration test can be seen in Fig. 2.

With information on penetration test phase and penetration test tools, it aims to simulate a deauthentication attack on an IP camera that can be accessed via the Internet. In this case, it is called a target and gateway. The test is carried out on WiFi connectivity using attacker tools. During the test period, the data are recorded by using network analyzer and packet sniffing software.

A. Penetration Test Phase

First, in the planning phase, it needs a clear definition and scope to what extent that external penetration test is carried out. Moreover, it requires preparations in the form of information and actions to be taken during the external penetration test. The plan must also be made for test scenarios. The data are collected and used as an information, and the scenario is made in this phase. With the scenario created, it is expected that the testing is not outside the problem boundary.

Second, it is discovery. In this phase, it aims to find information related to test targets. This phase is the beginning of the recording stage as the data collected is used as material for testing at the attack stage. In this case, it is done by using software network analyzer and packet sniffer tools. The process is referred to as fingerprint, which performs active and passive scans of WiFi signals in the area without entering the WiFi network.

Third, the current attack process uses comparison parameters before being attacked and after being attacked. Fourth, there is reporting. The last stage of the penetration test is useful as a reference point for defining preventive actions and mitigation activities to address identified vulnerabilities. The results of the test are reported into a digestible report for reading.

B. Penetration Test Tools

The tools used are:

1) Network analyzer and packet sniffer software: it is software for analyzing network performance such as Commview.
2) Attacker tools: it is an IoT-based simulation device for deauthentication attacks using the ESP8266 module, NodeMCU tools, and Lua programming.
3) Gateway: it is a network device that contains a transceiver and antenna for transmitting and receiving signals to and from remote clients using standard IEEE 802.11 WiFi connectivity while also providing internet access to clients.
4) Computer: Intel Core-i5, DDRIII 4GB, 500 GB HDD, Windows 7 64 Bit.
5) Target: The device used is an IP (Internet Protocol) camera. It is connected to a gateway that can be accessed from the local network or the Internet over WiFi connectivity.

C. External Penetration Test

It is necessary to have a scope and definition of to what extent external penetration tests are carried out. The preparations in the form of information and actions must be done. This created scenario is to simulate a deauthentication attack on a device with IEEE 802.11 (WiFi) connectivity. The process of this scenario aims to record all activities when the attack process occurs using tools that have been prepared.

TABLE I
EXTERNAL PENETRATION TEST SCENARIO.

Use Case Name	Deauthentication Attack Simulation
Actor	Test target, attacker
Description	The test target accesses the device through the Internet or WiFi media. In the same process, the attacker uses DoS attack on the WiFi.
Purpose	It is to prove DoS attack on the test target so that the test target cannot access the WiFi and Internet
Start State	The access of test target via WiFi and the Internet is connected
End State	The access of test target via WiFi and the Internet is disconnected

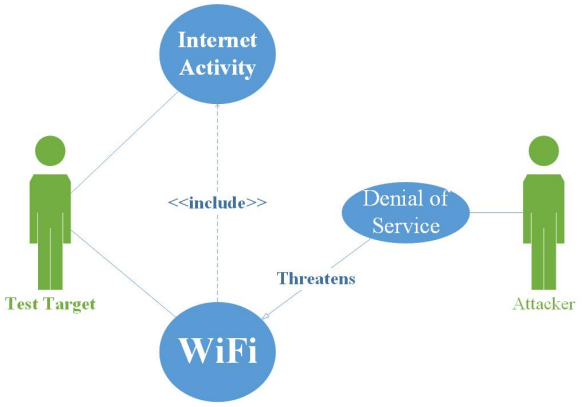

Fig. 3. Unified Modeling Languange (UML) diagram external penetration test scenarios.

Table I explains that the actors involved are test target as victim and attacker as perpetrator. The process starts from accessing the device through Internet or WiFi by the test target. At the same time, the attacker performs DoS attack on WiFi. The scenario is done to see the DoS attack on the target so that the test targets cannot access the Internet. The initial condition is connected, while the final condition is disconnected.

The carried out scenario is to understand and achieve the objectives of the external test penetration results.UML diagram is needed to find out the process and network diagram to clarify how the scenario will be run along with penetration test tools needs. It can be seen in Fig. 3. For more details, the flow of attacks is in Fig. 4.

When the test target tries to access an IP Camera, it cannot be accessed because the attacker has disconnected the WiFi connectivity. The attacker uses Arduino ESP8266 NodeMCU WiFi with Lua programming. The program script will execute the deauthenti-

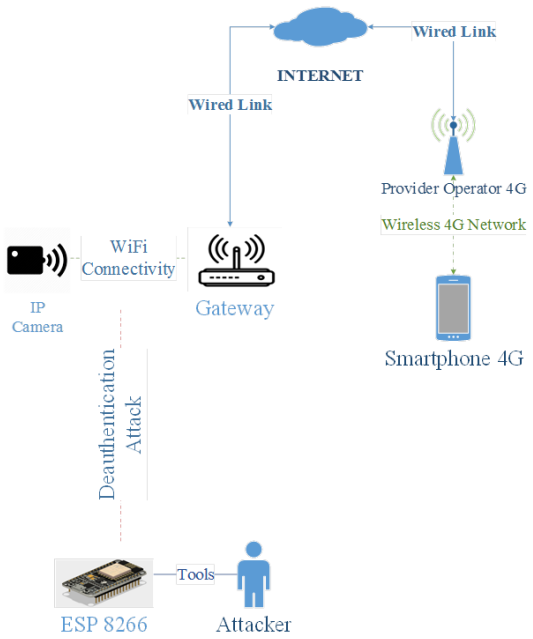

Fig. 4. Network diagram of deauthentication attack simulation with external test penetration.

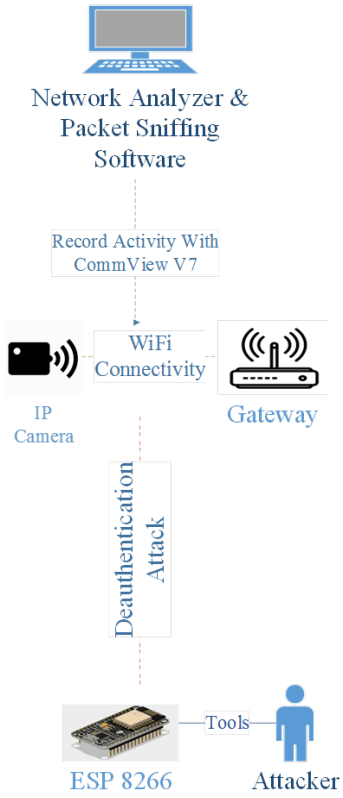

Fig. 5. Network diagram of the recording process during the external penetration test.

cation attack method on the target. The device works by connecting the ESP8266 NodeMCU WiFi device via a gadget (notebook, mobile, and others), and calling the device's web server application [13]. Then, it scans the available Service Set Identifier (SSID), after finding the target to be attacked. Next, the deauthentication attack can be made. The programming script nowadays can be found on the Internet as deauther script.

Some parameters are needed to record the process during the test. First, it is the target or the media tested. Second, Basic Service Set Identifier (BSSID) is used to identify and enter the WiFi network. Third, it is Stands for Station (STA). It is a term for clients that are connected to WiFi network. Fourth, there are before and after attack status. Those are the status of the target before and after the attack. Fifth, the estimated time is the time of the attack carried out from the connected to the disconnected condition.

To record WiFi activities that are running, the researchers use CommView for WiFi V.7.0 from TamoSoft. The features provided are capturing every packet on the air to display important information such as access point and station's list per-node and per-channel statistics, signal strength, list of packages and network connections, protocol distribution graphs, and others. For more details, how the data is taken during the external penetration testing process is in Fig. 5.

III. Results and Discussion

There are several impacts of an attack that occurs from a deauthentication attack on the test target. First, the communication of the test target with the gateway is lost. Second, the Media Access Control (MAC) address of the test target is still registered at the gateway. However, when the test target tries to connect to the gateway again, it cannot be done. Third, the test target is trying to find the same SSID (Service Set Identifier) so that it can be connected again with the gateway.

The proof of vulnerable IEEE 802.11 connectivity on IoT devices is revealed by using an external penetration test. The results of the test obtain the reports. It is in the form of data that can be used as information to provide conclusions at the end of the discussion.

A. Attack and Results

Before the attack, the attacker needs to scan the test target first. This process is called fingerprinting. It performs active and passive scans of WiFi signals in the area without entering into the WiFi network.

As seen in Fig. 6, the results of the fingerprint process are the target information in the form of MAC

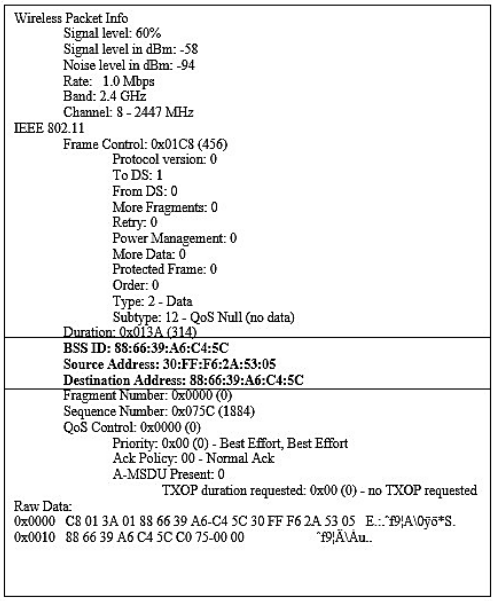

Fig. 6. Fingerprint results on the target.

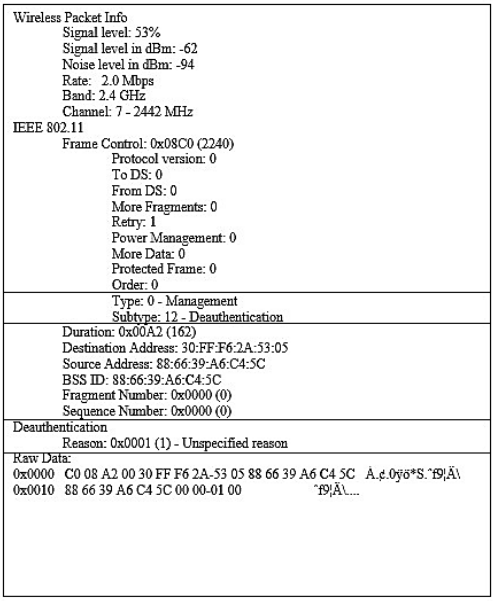

Fig. 7. The status of deauthentication.

address, namely 30: FF: F6: 2A: 53: 05 and 88: 66: 39: A6: C4: 5C. It can also be informed that the status is connected that there are transactions between source address (30: FF: F6: 2A: 53: 05) and destination address (88: 66: 39: A6: C4: 5C) in the information. This information can be used as a basis for conducting deauthentication attacks due to the availability of the MAC address. The information shows there is a transaction between BSSID 88: 66: 39: A6: C4: 5C and STA 30: FF: F6: 2A: 53: 05 so that it can obtain connected status.

Figure 7 shows the deaunthetication attack result. The information from the STA shows the status of deauthentication from BSSID. It can be seen that these changes are in frame control, which is significant from Type: 2 Data and Subtype: 12 - Quality of Service (QoS) to Type: 0 - Management, and Subtype: 12 - Deauthentication. Moreover, Table II shows the changes that occur in the data rate, channel, to-Distribution System (DS) and from-DS, retry bits, type, subtype, duration, BSSID, source address, destination address, and sequence number.

The current attack process uses the parameter comparison of results before and after being attacked. From the results of the test, the researchers find an initial and final condition on the status before and after being attacked. Thus, it can give information about the failure of the IEEE 802.11 connectivity.

There is an increase in data rate from 1 Mbps to 2 Mbps because the packet is sent to IEEE 802.11 WiFi connectivity on the source address and destination

TABLE II
THE STATE CONDITION.

State Condition	Start	End
Data Rate	1 Mbps	2 Mbps
Channel	5–2432 Mhz	7–2442 Mhz
To-DS bits	1	0
From-DS bits	0	0
Retry bits	0	1
Type	2 - Data	0 - Management
Subtype	12 - QoS Null (No Data)	12 - Deauthentication
Duration	314ms	162ms
BSSID	88:66:39:A6:C4:5C	88:66:39:A6:C4:5C
Source Address	30:FF:F6:2A:53:05	88:66:39:A6:C4:5C
Destination Address	88:66:39:A6:C4:5C	30:FF:F6:2A:53:05
Sequence Number	1672	0

address. Then, there is a change of channel from 5–2432 Mhz to 7–2442 Mhz. This change proves that there is frequency interference given by the attacker. Moreover, the status of the to-DS (number 1 bits) and from-DS (0) in the initial state condition indicates that the target has been authenticated and connected to the BSSID. Meanwhile, the final state condition to-DS and from-DS gives a number of 0 bits. It shows that the target is still available in the BSSID, but the status is management - deauthentication. This change also affects the type and sub-type fields, as well as the source address and destination address fields. In Retry bits, the number 0 indicates that the frame is not retransmission, while the number 1 is a retransmission.

Then, the sequence number in the initial state condition is 1672 as the transmission number between the transmitter and receiver. The final status becomes 0, and the number of the transmission starts from the

beginning or resets. Thus, it can be seen that the target is not transmitting to the source address and destination address.

B. Mitigation

Based on the review of the state condition change process [8], the researchers find at the time of the attack occurs, the frame management process found in 802.11 MAC headers serves as a setting for communication between STA and Access Point (AP). Due to these weaknesses originating from the failure of the transmission system, the development of the system is needed. The IEEE 802.11 frame is updated to close the gap, but the results of the previous test frame fail to overcome deauthentication attacks [7].

IEEE 802.11 management is managed at the Physical and Data Link layers. The MAC header process is at the Data Link layer. The communication between devices in IEEE 802.11 requires an identifier. The MAC function is an identification between devices to exchange data transactions, and the process is in the management of the MAC control. With a deauthentication attack, the attacker sends a data signal by forcibly changing the initial state condition. Thus, the target cannot be connected to the gateway. It means it has status from connected to disconnected.

It needs to be improvements in the IEEE 802.11 frame management. It regulates communication between STA and AP so that it is not easy to interfere with deauthentication attacks, which are long-term solutions. For short-term solutions, it is recommended that AP has more than one MAC address or AP for STA as a back-up when the attack occurs.

IV. Conclusion

The research aims to analyze the level of security of IEEE 802.11 or WiFi connectivity against deauthentication attacks on IoT-based devices. It is done by using an external penetration test method. Deauthentication attacks cause communication paralysis between devices connected. Several changes occur. Those are an increase in data rate, change in frequency channel, change in DS status, changes to retry bits in frame management, and the sequence number starting from the start. It needs improvements in the IEEE 802.11 frame management. Therefore, future researchers should analyze a solution to deal with this attack due to the increasing number of WiFi connectivity usage.

References

[1] R. M. Andrade, R. M. Carvalho, I. L. de Araújo, K. M. Oliveira, and M. E. Maia, "What changes from ubiquitous computing to Internet of Things in interaction evaluation?" in *International Conference on Distributed, Ambient, and Pervasive Interactions*. Vancouver, BC, Canada: Springer, July 9–14, 2017, pp. 3–21.

[2] A. Efe, E. Aksöz, N. Hanecioğlu, and Ş. N. Yalman, "Smart security of IoT against DDOS attacks," *International Journal of Innovative Engineering Applications*, vol. 2, no. 2, pp. 35–43, 2018.

[3] E. Oriwoh and G. Williams, "Internet of Things: The argument for smart forensics," in *Handbook of research on digital crime, cyberspace security, and information assurance*. USA: IGI Global, 2015, pp. 407–423.

[4] P. Thornycroft. (2016) Wi-Fi access for the Internet of Things can be complicated. [Online]. Available: https://bit.ly/3cv2UqI

[5] M. Bogdanoski, P. Latkoski, and A. Risteski, "Analysis of the impact of AuthRF and AssRF attacks on IEEE 802.11e-based access point," *Mobile Networks and Applications*, vol. 22, no. 5, pp. 834–843, 2017.

[6] M. A. Razzaq, S. H. Gill, M. A. Qureshi, and S. Ullah, "Security issues in the Internet of Things (IoT): A comprehensive study," *International Journal of Advanced Computer Science and Applications (IJACSA)*, vol. 8, no. 6, pp. 383–388, 2017.

[7] C. Liu and J. Qiu, "Performance study of 802.11 w for preventing DoS attacks on wireless local area networks," *Wireless Personal Communications*, vol. 95, no. 2, pp. 1031–1053, 2017.

[8] J. Milliken, V. Selis, K. M. Yap, and A. Marshall, "Impact of metric selection on wireless deauthentication DoS attack performance," *IEEE Wireless Communications Letters*, vol. 2, no. 5, pp. 571–574, 2013.

[9] H. A. Abdul-Ghani, D. Konstantas, and M. Mahyoub, "A comprehensive IoT attacks survey based on a building-blocked reference model," *(IJACSA) International Journal of Advanced Computer Science and Applications*, vol. 9, no. 3, pp. 355–373, 2018.

[10] T. Khalil, "IoT security against DdoS attacks using machine learning algorithms," *International Journal of Scientific and Research Publications*, vol. 7, no. 6, pp. 739–741, 2017.

[11] M. Alamanni, *Kali Linux wireless penetration testing essentials*. UK: Packt Publishing, 2015.

[12] Course Technology Cengage learning, *Penetration testing procedures & methodologies*. USA: Nelson Education, Ltd., 2011.

[13] H. Ikasamo. (2018) ESP8266/ESP32 connect WiFi made easy. [Online]. Available: https://www.hackster.io/hieromon-ikasamo/esp8266-esp32-connect-wifi-made-easy-d75f45