PREVENTION EFFORTS FOR SOCIAL ENGINEERING ATTACKS FROM ROGUE ACCESS POINT (CASE STUDY : TEMOO CAFÉ)

Wirda Fitriani[1]*, Musthafa Zufar Bahri [2], Nova Mayasari [3]
Universitas Pembangunan Panca Budi

Keywords:
social engineering, *rogue access point, prevention, attack*.

***Correspondence Address:**
wirda@pancabudi.ac.id

Abstract: An access point is a network device containing a transceiver and antenna for transmitting and receiving signals to and from remote clients. One device that can endanger a network is the presence of a Rogue Access Point (RAP). One technique used by rogue access point owners to obtain their target is by using Social Engineering techniques. This attack can camouflage itself and is therefore categorized as a dangerous attack. This attack can monitor network traffic and steal sensitive data from victims, which can ultimately be misused.
The prevention efforts of social engineering attacks from rogue access points through two methods: creating educational posters and using a rogue access point detection tool. Posters are used to help everyone to prevent themselves from such attacks, while the rogue access point detection tool is used to monitor the presence of these rogue access points. This tool works only to monitor and does not address the issue directly and technically. The cafe management has a role in directly addressing the existence of these rogue access points.

INTRODUCTION

The advancement of digital communication technology has made communication between humans more easily accessible and instant. One example is the internet network that can be easily accessed through Wireless Local Area Network (WLAN). An access point is a network device containing a transceiver and antenna for transmitting and receiving signals to and from remote clients. The function of an access point is to send and receive data, acting as a data buffer between Wireless LAN (WLAN) (Taruk, Budiman, & Safril, 2021). Access points are often placed in public spaces such as airports, shopping centers, hospitals, and cafes to provide internet connectivity. One device that can endanger a network is the presence of a rogue access point (RAP), but this requires user interaction to occur if client devices are not automatically set to connect (Witemyre, Abegaz, Payne, & Mady, 2018). Rogue access point attacks are considered dangerous,

with potential victims being spied on by hackers, allowing sensitive data to be stolen and misused. Therefore, prevention of such attacks is crucial. One technique used by rogue access point owners to obtain their targets is through Social Engineering techniques.

Social engineering attacks are one of the most dangerous threats in the world. On a global scale, cybersecurity analyst company Cyence stated that the United States is the country most targeted by social engineering attacks. One such company affected by this was Equifax, which was hacked for several months, and sensitive customer data was breached and stolen in 2018. This company is a consumer credit reporting and monitoring agency that collects individual and business consumer data to track their credit history (Salahdine & Kaabouch, 2019).

In this research, the author aims to create prevention efforts for Social Engineering, specifically from rogue access points. This prevention is divided into two parts: user prevention and service provider prevention. To help users prevent themselves from becoming victims of social engineering attacks from Rogue Access Points (RAP), the author creates educational posters in the service provider environment. The poster will inform about the dangers of illegal WiFi or SSID and provide information to users about the actual cafe SSID, so users do not connect to the wrong SSID.

As for prevention efforts from the service provider side, the author uses a NodeMCU ESP8266 microcontroller that is slightly modified to detect rogue access point attacks. This tool uses the Telegram application as a notification sender if there is an attack on the WiFi of the service provider's location, allowing the service provider to monitor WiFi network security without requiring a special network administrator. To run it, this tool must be connected to the WiFi that will be protected. After connecting to the WiFi, users can access the tool's settings by entering the tool's IP address in a browser.

The tool works by scanning previously stored SSIDs, and if there is an SSID that resembles or starts with the stored SSID name, the tool will detect this SSID as an unknown SSID and send a notification to the Telegram application. After the attack is detected, the service provider will follow up according to existing procedures.

RESEARCH METHODS

As mention in introduction, there are two methods to create prevention efforts that divided into two parts, namely prevention from the user side and from the service

provider side.

1. Poster Design

Prevention efforts for users are the most effective way to prevent social engineering attacks because these attacks exploit human ignorance (users). Hackers use this method when there are no longer any system vulnerabilities, and the only way to proceed is by manipulating users to carry out their actions. To prevent this, users must understand and be aware of digital security. Efforts to increase user knowledge and awareness about digital security, specifically WiFi network security, are done through educational posters that will be displayed at the service provider's location. These posters contain education about the dangers of connecting to the wrong or fake WiFi network, and in other posters, the correct cafe WiFi SSID name will be informed to prevent users from connecting incorrectly.

a. Poster Design Layout

The educational poster to be created consists of two different designs and will be made using the Canva design application. The design size used is 210mm x 297mm (A4). The poster design layout is as follows :

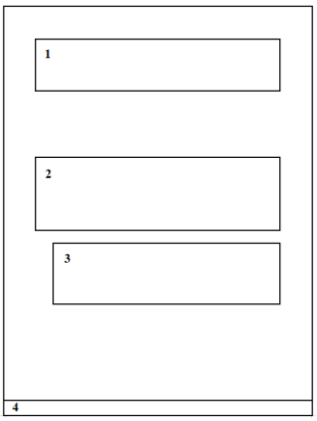

Figure 1. Poster Design Layout for Education

Figure 1 is the poster design layout that will be created to advise users to know that connecting to the wrong or unknown WiFi can make the connected device vulnerable to hacking. In section number 1, the text "WARNING!" will be created with a red background to attract the reader's attention. Sections number 2 and 3 will have the text "*Terhubung ke Wifi Tak Dikenal* " and "*Membuatmu Rentan Diretas*". Section number 4 will have the text "*Pastikan Kamu Terhubung Ke Wifi Yang Benar*". With this poster, users will be aware of digital security and will not be careless in using it.

b. Poster Design Layout for Information

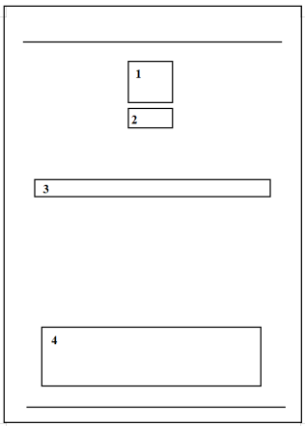

Figure 2. Poster Design Layout of Information

Figure 2 presents a design layout aimed at informing users of the correct provider WiFi SSID. The provider's WiFi SSID will be written between sections 3 and 4 on the poster. Section 1 will be filled with a WiFi symbol image, and section 2 will contain the word 'WiFi' to clarify the poster's purpose. Section 4 will have the text "*Jangan salah pilih. Wifi yang Benar hanya yang tertera di atas*".

2. Design and Development of the Device

To prevent social engineering attacks by service providers, a fake access point detection tool is used. This tool will scan for nearby WiFi names within a 20-meter radius and send a notification to a Telegram application if any WiFi name resembles the service provider's WiFi.

a. Block Diagram

Before designing and building this tool, it's easier to create a block diagram to get a general overview. The block diagram for this fake access point detection tool can be seen in Figure 3.

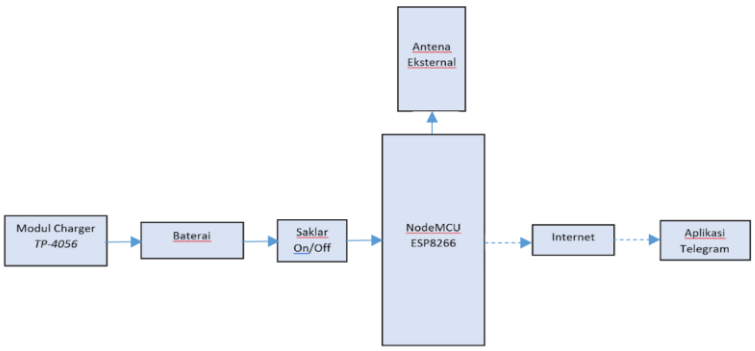

Figure 3. Block diagram of the rogue access point detection tool

The rogue access point detection tool is designed using a NodeMCU ESP8266 microcontroller as the detector. The NodeMCU will scan for unknown WiFis and mark them as attacker WiFis. The Telegram application is used to monitor the device. Once the NodeMCU successfully marks a suspicious WiFi, the result will be sent to a Telegram bot that can be accessed using a smartphone. To maximize the functionality and mobility of this device, several other tools are added, including a TP-4056 charger module, a 18650 2500mAh Li-ion battery, an on/off switch, an additional antenna, and a 5cm x 7cm project box.

b. NodeMCU Design

The NodeMCU is the core component of this device. Its primary role is to scan for WiFi names within a 20-meter radius and report the results via the Telegram application. Initially, the NodeMCU is programmed to store the names of the WiFis it will protect. Subsequently, the NodeMCU will continuously scan for suspicious WiFis within its range. The program is written using the Lua scripting language to fulfill its function. The NodeMCU circuit can be seen in the following image:

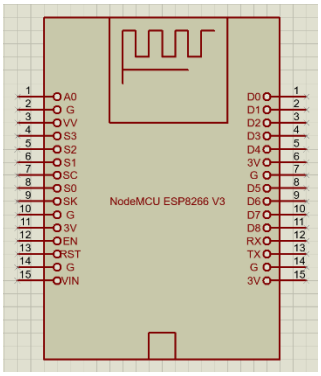

Figure 4. Node MCU Circuit

c. TP-4056 Charger Module

The TP-4056 charger module is used to recharge the device's battery using a micro USB cable. This module has red and blue LED indicators. When charging and current is flowing in, the red LED will light up. When charging is complete, the blue LED will light up. The circuit diagram of the TP-4056 charger module can be seen in Figure 5.

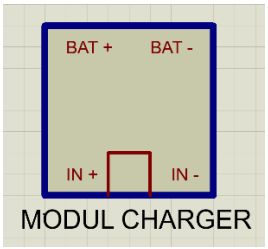

Figure 5. Charger Module Circuit

d. On/Off Switch

An on/off switch is a component that can interrupt and connect an electrical current. The switch used in this project is the KCD1-11 model, which has two pins. By using a switch, it simplifies the operation of this device, especially in turning it on and off easily. The switch circuit diagram can be seen in Figure 6.

Figure 6. Switch Circuit

e. External Antenna

An external antenna is an optional component because the NodeMCU can already send signals to other devices wirelessly. An external antenna is used to extend the signal range, which is useful for the main function of this device. The external antenna used in this device has a coverage range of approximately 20 meters with a signal strength of 5dBi. The antenna circuit diagram can be seen in Figure 3.8.

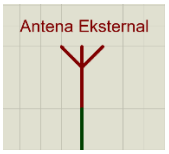

Figure 7. External Antenna Circuit

f. The Circuit

The design of the rogue access point detection tool using the NodeMCU ESP8266 begins with creating a circuit design of all the components that will be connected to the NodeMCU ESP8266 and other additional components. After that, the main and supporting components are assembled according to the previously created circuit design so that they are connected to each other and can function according to their purpose.

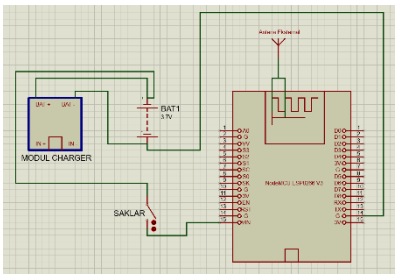

Figure 8. The Circuit.

RESULTS AND DISCUSSION

This section details the implementation phase of the social engineering prevention plan, utilizing posters as an information medium and a rogue access point detection tool, along with its testing.

1. Poster Implementation

Poster implementation is the first step in preventing social engineering attacks from fake access points and aims to educate cafe customers. Posters are placed in strategic locations within the cafe, such as the bar and the entrance. With these posters, customers will be continuously educated about digital security, especially WiFi security.

The implemented posters will be printed on A4-sized art paper using art paper or polymer ink. Clear print results will influence cafe customers to read the poster. The printing process and materials used greatly affect the print results, so it is recommended to use the previously mentioned materials for optimal results.

The printed posters will be placed in A4-sized photo frames to make them more durable and visually appealing when displayed in the cafe. Images of the posters in frames can be seen in Figures 9 and 10.

Figure 9. Education Poster in Frame

Figure 10. Information Poster in Frame

Placing posters in strategic locations within the service provider's premises aims to make them easily visible to users. This method can directly educate users at the potential location of attacks, thus preventing attacks from occurring.

2. Testing

The preparation on the wifipumpkin3 tool has been completed, and testing on the device can now be carried out. Testing the fake access point detection tool is done as similarly as possible to the possible ways hackers can carry out their actions. The testing of the fake access point detection tool will be carried out three times on different SSIDs.

In the test, the provider as a cafe SSID to be used is "TEMO COFFEE" and the fake SSID is "TEMO COFFEE A". The test begins by turning on the device first, and the device's information will be sent via a Telegram bot as shown in Figure 11.

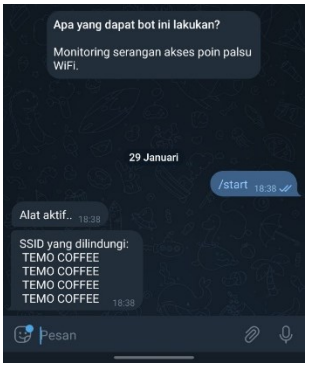

Figure 11. Telegram Bot Displaying Device Activation Information in the test

After the device is turned on, the WiFi adapter is then installed on the device. Then, a fake SSID is created by running wifipumpkin3 first, then activating the tool by typing "start" in the terminal as shown in Figure 12.

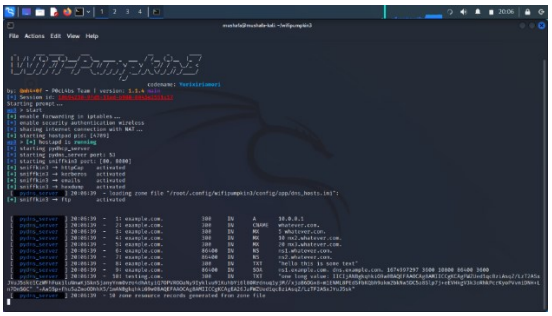

Figure 12. Wifipumpkin Activated Display

The fake SSID has been successfully created and is listed in the device's WiFi list, and the fake SSID can be accessed as shown in Figure 13. After the fake SSID is visible in the available WiFi list, the fake access point detection tool immediately detects it as an attack and sends a danger status via the Telegram bot as shown in Figure 14.

Figure 13. WiFi List Display

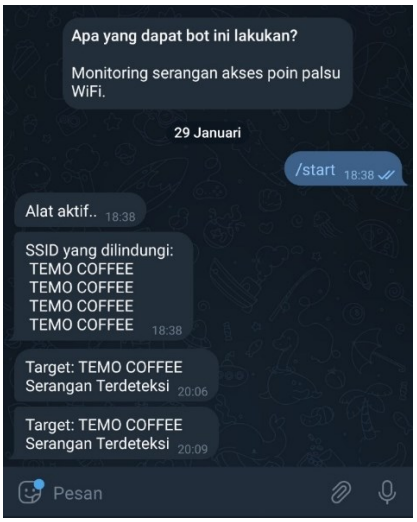

Figure 14. Status Display on Telegram

3. Discussion

The way this fake access point detection tool works is by first storing the SSID it wants to protect. Then, the device will scan to find SSIDs that are identical to the cafe's

SSID or have the same prefix as the cafe's SSID, as shown in Table 1.

Table 1. Example of How the Device Works

No.	SSID CAFE	Other SSID	STATUS
1	*TEMO COFFEE*	*TEMO COFFEE* **A**	Rogue Access Point Detected
2	*TEMO COFFEE A*	*TEMO COFFEE A* **B**	Rogue Access Point Detected
3	*TEMO COFFEE A*	**TEMO COFFEE B**	Clear

In Table 1, at point one, the cafe's WiFi has an SSID "TEMO COFFEE" and there is a fake SSID that is initially similar to the cafe's SSID but with an added letter "A" to become "TEMO COFFEE A" to deceive customers. The device will detect the fake access point and send its status information to Telegram. Similarly, in Table 1 point 2, the cafe's WiFi has an SSID "TEMO COFFEE A" and there is another SSID that is initially similar to the cafe's SSID but with an added letter "B" to become "TEMO COFFEE A B". In Table 1 point three, the device does not detect any attacks because the prefix of the other SSID is not similar to the cafe's SSID. This method can be used if the cafe has more than one SSID. However, this method may be exploited by hackers. If that happens, the informational posters that have been installed around the cafe will help customers to know which WiFi SSIDs are actually owned by the cafe, so that customers are not tricked by hackers.

CONCLUSION

Based on the design, testing, and discussion of the tool, the author obtained the following conclusions from this research regarding the implementation of social engineering attack prevention from fake access points at Temo Coffee. The results of this study present that the previously designed tool can detect rogue access points and send the information to Telegram. Posters and the tools are both needed and have their own advantages in preventing social engineering attacks from fake access points. Posters serve as a means of providing educational information to cafe customers to prevent customers from becoming victims of social engineering from fake access points. While the tool aims to monitor for fake access points.

REFERENCE

Chamim. (2012). Mikrokontroler Belajar Code Vision AVR Mulai Dari Nol

Dahoud, A. Al, & Fezari, M. (2018). NodeMCU V3 For Fast IoT Application Development. Notes, October, 5.

Nugroho, A. A. (2012). Implementasi Aplikasi Berbasis Web Sebagai Sistem Pendeteksi Rogue Access Point Dengan Wired-Side Solution.

Salahdine, F., & Kaabouch, N. (2019). Social engineering attacks: A survey. . *Future Internet*.

Sowah, R. A., Ofori-Amanfo, K. B., Mills, G. A., & Koumadi, K. M. (2019). Detection and prevention of man-in-the-middle spoofing attacks in MANETs using predictive techniques in Artificial Neural Networks (ANN). Journal of Computer Networks and Communications, 2019. https://doi.org/10.1155/2019/4683982

Taruk, M., Budiman, E., & Safril, M. (2021). Kinerja Perangkat Access Point Menggunakan Metode Coverage Visualization. *Jurnal Rekayasa Teknologi Informasi (JURTI)*. doi:https://doi.org/10.30872/jurti.v5i1.7069

Witemyre, S., Abegaz, T., Payne, B., & Mady, A. N. (2018). Hijacking Wireless Communications using WiFi Pineapple NANO as a Rogue Access Point. *Proceedings of the 2018 Conference on Cybersecurity Education, Research and Practice.*