UNAUTHORIZED ACCESS POINTS (ROGUE AP) IN WIRELESS NETWORK CONTROL SYSTEM

Saulius Juškevičius, Dangis Rimkus
Kaunas University of Technology, Kaunas, Lithuania

Abstract. In this paper wireless network security issues are analyzed, especially with unauthorized access points and man in the middle attacks. Propose solution how to protect wireless network using open source hardware and software. Also describe more detailed implementation of control system.

Keywords: access point, rogue AP, wireless network, openWRT, LuCI, open source.

Introduction

Wireless local area network (WLAN) is becoming more and more popular wireless technology, especially IEEE 802.11 standard. This technology is used in various locations such as homes, cafes, large companies, and other public places. The ease of access to this common technology gives rise to security and privacy issues. Due to the principle of operation of this technology, the openness of broadcasting, several attacks are possible. One of them is the attack of an unauthorized access point (Rogue AP). An unauthorized access point could be described as an access point that was not installed by the WLAN administrator. (Shen X., 2006)

A hacker can build an access point with the same service set identifier (SSID) as the actual access point and can force users to connect to an unauthorized access point. In this way, a hacker can collect private information from users and perform a man-in-the-middle attack. When trying to hide in the network and avoid being caught, hackers copy the Media Access Control (MAC) address of the real access point and replace it, thus mimicking the actual access point as shown in Fig. 1. Such an attack is not difficult to organize. And internet is full of tutorials for such attacks. Since the vast majority of user devices do not have access point authentication and verification mechanisms, it is impossible for them to distinguish between an actual, and an unauthorized access point. Therefore, there is a need for technology or detection method to detect and neutralize unauthorized access points.

The solutions for detecting existing unauthorized access points include three aspects: user-side, wired-side and wireless-side detection. The basis of user-side detection methods is statistical analysis and algorithms for finding anomalies. This solution is simple and inexpensive for the user, but additional software is needed on the user's device. For these reasons, the user-side detection method is difficult to apply widely. Another method is wired detection and the unauthorized access point needs to be connected to the network, thus transferring data to the Internet. This method monitors the network and searches for data that can travel through an unauthorized access point. However, it is physically difficult to connect an access point to a foreign network, and it is easier to monitor the wireless network. For this reason, wireless detection is the most important solution. The principle of operation is the collection of technical information of all visible access points, one of which is the value of the Received Signal Strength Indication (RSSI), after reading this value from several devices at different locations, it is possible to construct a signal strength indicator vector and determine the physical position of the unauthorized access point. Also, the information gathered can be used to restrict users' access to an unauthorized access point by sending deauthentication packets to the unauthorized access point MAC address. (Gonzales H., 2010)

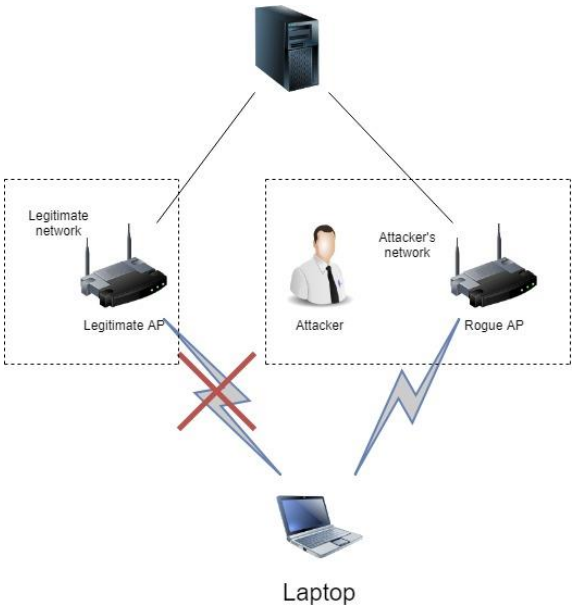

Figure 1. Man in The Middle attack using rogue AP

Risks of Rogue AP

With current information technology (IT) industry evolution unauthorized access points can be hidden and hard to find. And the risk comes from using unauthorized access points for "man in the middle" attacks to collect, eavesdrop and trick users in giving their private information. The attacker secretly relays and alters the communication between two parties and lets the attacker to intercept all incoming and outgoing messages between the parties. There are different ways for the attacker to get information about the victim. Such attacks are like Secure Socket Layer (SSL) hijacking, eavesdropping, Domain Name System (DNS) spoofing and stolen browser cookies. Each attack uses different approach to get information. SSL hijacking makes user connect to unsecured Hypertext Transfer Protocol (HTTP) server making all sent information unencrypted. Eavesdropping is when attacker creates legitimately sounding network name and when user connects to it attacker can monitor user's activity. DNS spoofing forces users to fake websites and forcing users to enter login credentials. Attacker can hijack cookies from browsers and since all browsing information is stored in them attacker can gain access to your passwords, addresses and other sensitive information. Apart from these type of attacks there are others of which purpose is the same to collect sensitive information.

Proposed solution

In this document a system solution will be proposed with these functions:

1. Locating and/or blocking rogue access points and not disturbing legitimate networks correct functioning from stopping clients and the legitimate administrator from connecting to legitimate access points and their network.
2. Implement wireless network control system and all its functions using open source software and hardware.

The control system would consist of router, at least 3 access points and control system software.

The following are the components of control system:

1. Access Point: The access point will have two operating modes, normal mode, and monitoring mode. Subsequent mode monitors the environment and collects information about surrounding access points. Most business-level hardware has such functionality. In this case, both modes will be able to operate simultaneously, as separate adapters will be used for each mode. For example, Raspberry Pi 3B has its own integrated wireless network adapter, and a second USB wireless network adapter operating in monitoring mode.
2. Auxiliary Wireless Network Adapter: In this case, it would be a USB wireless network adapter plugged into the Raspberry Pi 3B connector that would be in monitor mode.
3. Router: The unauthorized access point control system will work on the router and all the information will be stored in it.

Detecting unauthorized access point

Unauthorized access point detection starts with access point environment monitoring and gathering and storing information like shown in Fig.2.

The order of this process would look like this:

1. Collects frames around access points and clients using an auxiliary wireless adapter on the access point.
2. The collected wireless network information is stored in the router's memory.
3. Both of these steps are repeated until the network is checked through all wireless channels.

All information collected is displayed on the control system page. It is also possible to assign categories to all access points. When new access points are detected which are not categorized, a message is sent to the administrator.

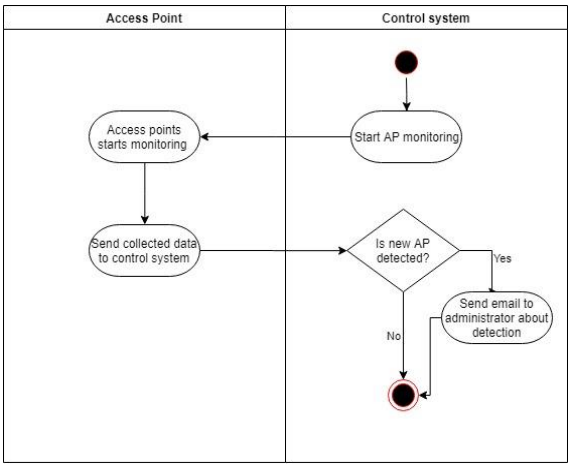

Figure 2. AP detection activity diagram

Localization of unauthorized access point

When the needed information is collected, the administrator sees all access points on the control system page. The administrator can select an access point and see more detailed information about it. Also with an environmental map and at least 3

access points, you can roughly locate the location of the selected access point on the map by the existing access points. The process is shown in Fig. 4.

This process is shown as follows:

1. The administrator determines the positions of the existing three access points on the map.
2. Selects access point which to locate.
3. The trilateration method determines the approximate position according to the calculated distances (circle radius) of received RSSI values. At least 3 legitimate access points are needed locate rogue AP since it is trilateration method's operating principle Fig. 3.

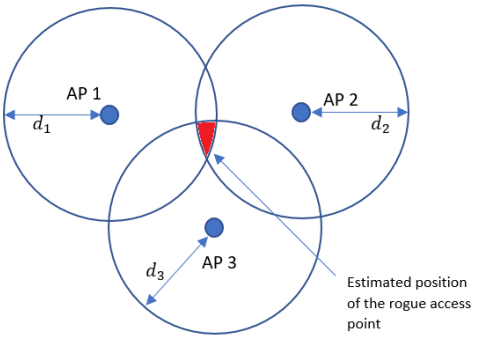

Figure 3. Example of 2D localization using Trilateration

After that administrator can physically locate the access point and take care of it. (Le T. at al., 2012), (An Xie, & Ouyang, 2018).

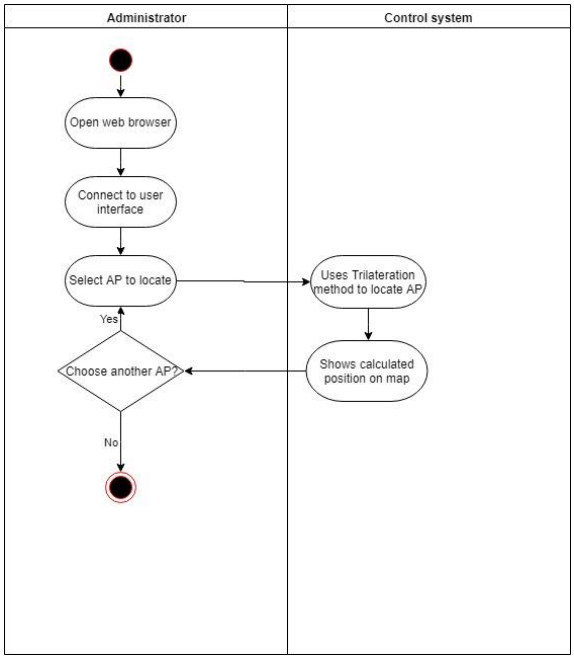

Figure 4. AP localization activity diagram

Block unauthorized access point

If administrator fails to physically remove an unauthorized access point or for other reasons. This access point can be blocked, more precisely by sending the deauthentication packet to the MAC address of that access point so that all clients disconnect and cannot reconnect to it. Fig 5. Also it is possible to send multiple packets to different targeted rogue access points by generating packets from gathered access points list.

This process is shown as follows:

1. An administrator chooses an unauthorized access point to block.
2. Access points send the generated deauthentication packet to prevent the operation of an unauthorized access point.

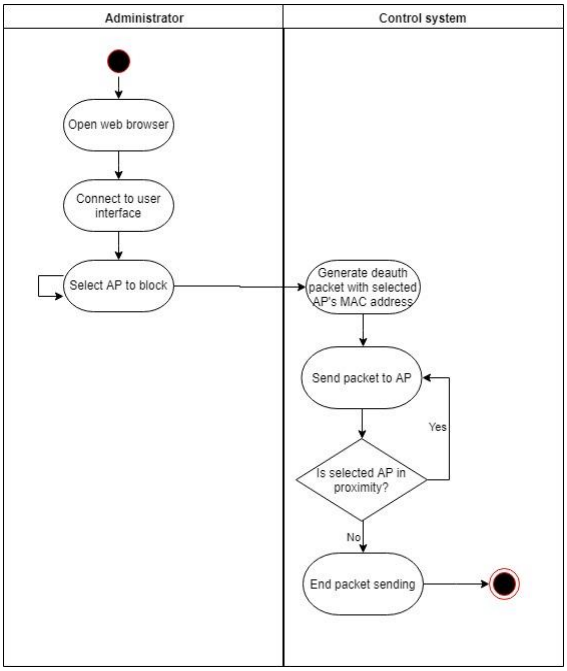

Figure 5. Rogue AP blocking activity diagram

Implementation using open source hardware and software

The implementation of this article's proposed solution could be done on the open source hardware and software. The aim of this implementation to help people track their wireless network for low cost in comparison with enterprise level hardware and software.

The chosen hardware is Raspberry Pi 3 B+ because of its capabilities like integrated Wireless Local Area Network (WLAN) module, internal memory, processing power and for software was chosen OpenWRT firmware because of its licensing you can freely modify it not like DD-WRT or

Tomato. They are open source but modification is not allowed without authors agreement.

For the user interface the default OpenWRT's LuCI web interface is sufficient for this implementation and it makes configuration more user-friendly. The web user interface uses the Lua programming language and splits up the interface into logical parts like models, views and controllers, uses object-oriented libraries and templating. It has evolved from an MVC-Web framework. The Lua code is parsed with CBI parser into HTML form for the user to view. Also user interface uses uHTTPd webserver to communicate with user and vice versa. And at the base of system is OpenWRT firmware as shown in Fig. 6.

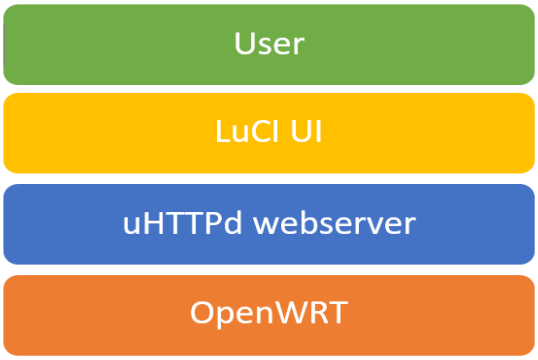

Figure 6 LuCI architecture

Despite that there some restrictions. First of all we have failed to find a Lua library for generating deauthentication packets. Solution for that is to use Python "impacket" library for working with packets and generating them. Another obstacle is user's interaction with map of building. To bypass that Javascript integration into Lua files is needed. (Openwrt., 2019)

Conclusions

The ease of setting up a rogue access point makes it a serious security problem. Authors suggested open source hardware and software makes it affordable for small offices, small businesses or personal use. Control system is most fitting small to medium size businesses because such businesses tend to use opens source software and hardware for their network because not like large companies they cannot afford expensive network control systems. This implementation makes it valuable for future wireless security development on open source firmware because no existing solution was found.

References

1. Shen, X., Lin, C., Sun, Y., Pan, J., Langendoerfer, P., & Cao, Z. (2006). Wireless network security. Wireless Communications and Mobile Computing, 6(3), 269-271.
2. Gonzales, H., Bauer, Lindqvist, Mccoy, & Sicker. (2010). Practical Defenses for Evil Twin Attacks in 802.11. 2010 IEEE Global Telecommunications Conference GLOBECOM 2010, 1-6.
3. Le, T., Ren Ping Liu, & Hedley. (2012). Rogue access point detection and localization. 2012 IEEE 23rd International Symposium on Personal, Indoor and Mobile Radio Communications - (PIMRC), 2489-2493.
4. An, Xie, & Ouyang. (2018). Reliable sensor location for object positioning and surveillance via trilateration. Transportation Research Part B, 117, 956-970.
5. Openwrt. (2019, February 28). Openwrt/openwrt. Retrieved from https://github.com/openwrt/openwrt

About the authors

Saulius Juškevičius
Student at Department of Applied Informatics, Kaunas University of Technology, Kaunas, Lithuania
E-mail: saulius.juskevicius@ktu.edu

Dangis Rimkus
Lecturer at Department of Applied Informatics, Kaunas University of Technology, Kaunas, Lithuania
E-mail: dangis.rimkus@ktu.edu