Borneo International Journal eISSN 2636-9826; Vol. 6 (3); 2023; 152-156
Published by *Majmuah Enterprise*
www.majmuah.com

Improving User Trust of Public Wireless Access Point using Wireless Devices Identification Information

ADI AFFANDI BIN AHMAD
School of Computing, Universiti Utara Malaysia (UUM),06010 UUM Sintok, Kedah Darul Aman, MALAYSIA
Email: adi@uum.edu.my | Tel: +60175874692 |

Received: September 23, 2023
Accepted: September 29, 2023
Online Published: September 30, 2023

Abstract

Public Wireless Access Point (AP) is a wireless access point accessible to the public. Connecting to the Internet through Public Wireless Access Point does not require users to authenticate (Open Authentication). There are also organizations using the authentication method for users to access their public AP. Passwords are shared or displayed at an easy-to-see place. Some organizations use open authentication, but users need to authenticate through the captive portal provided. There are many security threats faced by users when using Public Wireless Access Point. These security threats cause users to put a Public AP at a low level of trust. Identifying the Public AP identity that is used or connected to, may improve the user trust of the Public AP. This paper tries to explore the use of Netsh Commands for Wireless Local Area Network (WLAN) in Windows Operating System to obtain complete information on the Wireless Access Points around the area. The Organizationally Unique Identifier (OUI) found on the MAC Address of the Access Point is compared to the latest list of OUI issued by Institute of Electrical and Electronics Engineers (IEEE) to identify Access Point manufacturer. Authentication methods and encryption techniques used by the AP can also improve the level of trust of users to the AP.

Keywords: Wireless Access Point (AP), Authentication, Wireless Security Threats, Public Wireless AP, User Trust, Device Identification

1. Introduction

Business networks today are evolving to support people who are on the move. People are connected using multiple devices, including computers, laptops, tablets, and smart phones. This is the vision of mobility where people can take their connection to the network along with them on the road. According to Hintze, Hintze, Findling, & Mayrhofer, (2017), mobile devices that is commonly used today like smartphones and tablets have become an indispensable part of people's lives. Their study show that smartphones are used almost thrice as often as tablet devices. There are many different infrastructures (wired LAN, service provider networks) that make this type of mobility possible, but in a business environment, the most important is the wireless LAN (WLAN). The wireless network according to Gierłowski & Nowicki (2007) has reached a stage where it is appropriate in a business environment to support the business applications used including the mission-critical applications. Wireless networks are classified into two categories namely structured (infrastructure mode) and structureless (ad-hoc mode) based on architecture (Ahmed & Abbas, 2015) (Neetesh & Narendra, 2012). A common wireless data implementation is enabling devices to connect wirelessly via a LAN. In general, a wireless LAN requires the following network devices:

- Wireless Access Point (AP)
- Computing Devices with Wireless NIC adapters

This type of wireless data implementation according to IEEE (2016) and Keceli, Inan, & Ender (2007) is known as an infrastructure basic service set (BSS). This paper is organised as follows: in Section 2, we discuss the concepts of Infrastructure BSS and it continue in section 3, where we focus on Wireless Access Point, Authentication methods and Security Threats. The methodology used will be discuss in Section 4. Section 5 shows the results of the study and discussion of the results.

2. Infrastructure Basic Service Set (BSS)

The basic building block of a Wireless Local Area Network (LAN) architecture define by IEEE (2016) is known as basic service set (BSS). Wireless stations (STA) are the basic devices that communicate inside this basic service set. Unlike devices in wired LAN that usually remain at one location, Wireless STAs are usually fixed, portable or mobile. A portable STA is one that is moved from location to location, but that is used only while at a fixed location. Mobile STAs actually

access the LAN while in motion. Stations in BSS communicates with each other. Data transfers from one station to another is by transmitting radio signals or wireless medium (WM). The collection of all possible directional transmissions by a member STA defines the coverage area. This area is called the Basic Service Area (BSA). An infrastructure BSS form a component of an extended form of network that is built with multiple BSSs. The architectural component used to interconnect infrastructure BSSs is the Distribution system (DS). Wireless access point (AP) in an entity inside an infrastructure BSS that contains one station (STA) and provides access to the distribution services, via the wireless medium (WM) for associated STAs. An AP comprises a STA and a distribution system access function (DSAF).

Figure 1 shows the relationship between BSS Infrastructure components such as Wireless Stations (STA), Access Point (AP), Distribution system (DS) and distribution system medium (DSM) in creating a IEEE 802.11 Architecture.

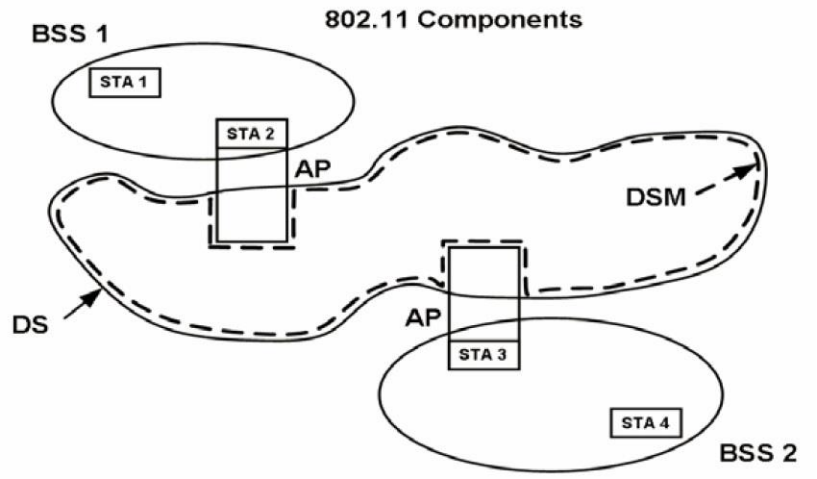

Figure 1: Infrastructure BSS, Source: IEEE (2016)

3. Wireless Access Point, Authentication and Security

When we enable (switch on) the Wi-Fi Adapter found on our computing device, we will find that there are many Wireless Access Point or Service Set Identifier (SSID) nearby. The owner of the network normally assigned a meaningful name for the SSIDs so that users can easily find the relevant network through their devices (Seneviratne, Jiang, Cunche, & Seneviratne, 2015). There are 2 types of Access Point in the list of available Access Points that are Open Access Point and Secure Access Point. There is also an access point owner who puts their AP in a hidden network. Users cannot see this AP type in the list of available APs. The AP owner hides their AP name from the list of available APs by setting up their APs to not broadcast its SSIDs. The owner of this hidden AP usually puts their AP in a private network. Access is only allowed to users who know the SSID of the AP. Enterprise network owners, using enterprise-level APs can separate their private wireless networks from public access by creating a public wireless access point.

Public Wireless Access Point (AP) is a wireless access point accessible to the public. Connecting to the Internet through Public Wireless Access Point does not require users to authenticate or also known as Open Authentication. There are also organizations using the authentication method for user to access their public AP. Passwords are shared or displayed at an easy-to-see place, typically employing pre-shared keys using WEP or WPA-PSK. Some organizations using open authentication, but users need to authenticate through the captive portal provided (Soewito & Hirzi, 2014).

There are many security threats faced by users when using Public Wireless Access Point. These security threats cause users to put a Public AP at a low level of trust. US-CERT (2008), Mardiana & Wan Haslina (2013) and Tzvi, Andriy & Artem (2015) have listed some of the threats faced by public AP users, including: Evil Twin Attacks, Wireless Sniffing, Peer-to-Peer Connections, Unauthorized Computer Access, Shoulder Surfing, Third-Party Data Gathering and Malicious Access Points or Rogue Access Points. Public wireless networks very rarely provide a way in which the wireless access point (AP) can be authenticated to the user. According to Kindberg, Mitchell, Grimmett, Bevan, & O'Neill, (2009), public AP that used pre-shared keys using WEP or WPA-PSK offer some level of protection against passive eavesdropping. Users will be exposed to a rogue AP set up by an attacker (Nikki & Imam, 2016). This rogue AP may offer a captive portal which appears identical to that provided by the location's legitimate AP and may accept the same pre-shared key for link layer encryption.

The authentication methods listed above are usually used to authenticate the users of the wireless network. In our study, we try to authenticate or identify the identity of the public access point. Identifying the Public AP identity that is used or connected to, may improve the user trust of the Public AP. Next section of this paper tries to explore the use of Netsh Commands for Wireless Local Area Network (WLAN) in Windows Operating System to obtain a complete information on the Wireless Access Points around the area.

4. Methodology

The main objective of this study is to identify the identity of the public access point in the area studied. This research method is conducted in 3 stages: choosing the appropriate location to conduct the study, using the appropriate tool to obtain complete information on wireless access points and identifying the access point manufacturer by comparing the OUI information which is part of the MAC address obtained in stage 2 with the OUI list issued by the IEEE.

4.1 Location selection

The location selected to conduct the study is at School of Computing (SOC), Universiti Utara Malaysia. Within the area, there are lecture halls, administrative offices, and lecturer rooms. The study was conducted in 3 different places, Lecture Hall 4 (DKG4), SOC Foyer and lecturer room at Level 3 (Room no. 3125). These three places are far apart from each other.

4.2 Software / tool selection

This study tries to explore the tool that is already available in Microsoft Windows Operating System known as Network Shell (netsh) Commands for Wireless Local Area Network (WLAN) (Microsoft, 2023). Using Network shell (netsh) command-line utility, we can configure and display the status and information of various network communications components including wireless access points.

4.3 Manufacturer Identification

The manufacturer of the wireless access point can be identified by comparing the OUI information which is part of the MAC address obtained in stage 2 with the OUI list issued by the IEEE.

5. Results and discussion

Table 1, 2 and 3 shows the list of Wireless Access Points available in 3 locations around the School of Computing namely Lecture Hall 4 (DKG4), SOC Foyer and lecturer room at Level 3 (Room no. 3125).

Table 1: Wireless AP visible at Lecture Hall 4 (DKG4)

SSID Name	Authentication	Encryption	BSSID MAC Address
UUMWiFi_Guest	Open	None	24:01:c7:ac:f2:73
			24:01:c7:b8:6f:52
			f0:7f:06:d7:dc:e3
			94:b4:0f:52:73:c1
			00:24:6c:25:21:d3
			f0:7f:06:9d:bf:83
NorlizaK	WPA2-Personal	CCMP	ac:af:b9:46:b2:96
ConferenceRoom	WPA2-Personal	CCMP	2c:56:dc:8a:70:94
UUMWiFi	WPA2-Enterprise	CCMP	00:24:6c:25:21:d1

Table 2: Wireless AP visible at School of Computing (SOC) Foyer

SSID Name	Authentication	Encryption	BSSID MAC Address
UUMWiFi_Guest	Open	None	24:01:c7:b8:8f:82
			00:26:99:a2:9b:82
			78:ba:f9:ca:b7:92
			00:26:99:a2:a7:22
			24:01:c7:ac:f4:d2

Table 3: Wireless AP visible at lecturer room at Level 3 (Room no. 3125)

SSID Name	Authentication	Encryption	BSSID MAC Address
Human_Centred Computing Group	Open	None	6c:19:8f:58:9b:0c
UUMWiFi_Guest	Open	None	24:01:c7:b8:7b:12
			00:1a:1e:fb:ff:23
UUMWiFi	WPA2-Enterprise	CCMP	00:1a:1e:fb:ff:21

The Organizationally Unique Identifier (OUI) found on the MAC Address of the Access Point is then compared to the latest list of OUI issued by IEEE (2023) to identify Access Point manufacturer. Table 4 shows the OUI and the Assignee (vendor, manufacturer, or other organization assigned with that OUI).

Table 4: Shows the OUI and the Assignee

OUI	The Assignee	SSID
24:01:c7	Cisco Systems, Inc	UUMWiFi_Guest
f0:7f:06	Cisco Systems, Inc	UUMWiFi_Guest
94:b4:0f	Aruba Networks	UUMWiFi_Guest
00:24:6c	Aruba Networks	UUMWiFi_Guest, UUMWiFi
ac:af:b9	Samsung Electronics Co.,Ltd	NorlizaK
2c:56:dc	ASUSTek COMPUTER INC.	ConferenceRoom
00:26:99	Cisco Systems, Inc	UUMWiFi_Guest
78:ba:f9	Cisco Systems, Inc	UUMWiFi_Guest
6c:19:8f	D-Link International	Human_Centred Computing Group
00:1a:1e	Aruba Networks	UUMWiFi_Guest, UUMWiFi

The identified MAC or OUI is listed in the Publicly Registered MA-L (company name & address on the public listing). APs manufactured by companies listed in Privately Registered MA-L (company name and address NOT on the public listing) cannot be identified. The results from the study, based on the authentication method used, there were 2 public access points in the study area namely UUMWiFi_Guest and Human_Centred Computing Group. UUMWiFi_Guest uses APs manufactured by Cisco Systems, Inc and Aruba Networks. Both companies are network equipment manufacturers. Large organizations usually use all APs from one or two similar companies. If there is an AP using the organization's SSID but issued by a different manufacturer, or such manufacturer cannot be identified, this is probably a sign that the AP is not valid. Human_Centred Computing Group uses AP manufactured by D-Link International. This company is a network equipment manufacturer but not just only producing AP, this company also produces network interface card (NIC) and other equipments. There are also 2 APs using WPA2-Personal as authentication methods, NorlizaK and ConferenceRoom. NorlizaK uses AP manufactured by Samsung Electronics Co.,Ltd. This company is a manufacturer of mobile phones. ConferenceRoom uses AP manufactured by ASUSTek COMPUTER INC. This company is a manufacturer of computing equipment.

6. Conclusions

This paper tries to explore the use of Netsh Commands for Wireless Local Area Network (WLAN) in Windows Operating System to obtain complete information on the Wireless Access Points around the area. There are many other methods that can be used to obtain information about wireless access points. In this study, we compare Organizationally Unique Identifier (OUI) found on the MAC Address of the Access Point with the latest list of OUI issued by Institute of Electrical and Electronics Engineers (IEEE) to identify Access Point manufacturer. The MAC address obtained cannot be verified since there are software and tools that can change the MAC address of a device. However, this study can help identify APs identity in general. Identifying the Public AP identity that is used or connected to, may improve the user trust of the Public AP.

References

Ahmed, M., & Abbas, S. (2015). Energy Efficient Wireless Networking and Computing Infrastructure. International Journal of Natural and Engineering Sciences, 60-64.

Gierłowski, K., & Nowicki, K. (2007). Wireless Networks as an Infrastructure. Network-Based Information Systems: First International Conference, NBiS 2007 (pp. 49-58). Regensburg: Springer Berlin Heidelberg.

Hintze, D., Hintze, P., Findling, R. D., & Mayrhofer, R. (2017). A Large-Scale, Long-Term Analysis of Mobile Device Usage Characteristics. Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies, 1-21.

IEEE. (2016). Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications (IEEE Std 802.11™-2016). New York: IEEE.

IEEE. (2023). IEEE OUI. Retrieved from IEEE OUI: https://standards-oui.ieee.org/

Kecili, F., Inanc, I., & Ender, A. (2007). Fairness Provision in the IEEE 802.11 e Infrastructure Basic Service Set.

Kindberg, T., Mitchell, J., Grimmett, J., Bevan, C., & O'Neill, E. (2009). Authenticating Public Wireless Networks with Physical Evidence. 2009 International Conference on Wireless and Mobile Computing, Networking and Communications, 394-399.

Mardiana, M., & Wan Haslina, H. (2013). Wireless Networks: Developments, Threats and Countermeasures. International Journal of Digital Information and Wireless Communications (IJDIWC), 125-140.

Microsoft. (2023). Network shell (netsh). Retrieved from Microsoft Learn: https://learn.microsoft.com/en-us/windows-server/networking/technologies/netsh/netsh

Neetesh, S., & Narendra, C. (2012). Message Security in Wireless Networks: Infrastructure based vs. Infrastructureless Networks. 2012 IEEE International Students Conference on Engineering and Systems (SCES 2012), (pp. 915-920). Allahabad.

Nikki, H., & Imam, R. (2016). Automation Framework for Rogue Access Point Mitigation In IEEE 802.1x-Based WLAN. Journal of Theoretical and Applied Information Technology, 287-296.

Seneviratne, S., Jiang, F., Cunche, M., & Seneviratne, A. (2015). SSIDs in the wild: Extracting semantic information from WiFi SSIDs. 2015 IEEE 40th Conference on Local Computer Networks (LCN) (pp. 494-497). Florida: IEEE.

Soewito, B., & Hirzi. (2014). Building secure wireless access point based on certificate authentication and firewall captive portal. The European Physical Journal Conferences.

Tzvi , K., Andriy , O., & Artem , K. (2015). Is it safe to use public Wi-Fi networks? Retrieved from Computerworld: http://cdn.computerworld.com.au/article/571791/it-safe-use-public-wi-fi-networks/

US-CERT. (2008). Cybersecurity & Infrastructure Security Agency (CISA). Retrieved from https://www.cisa.gov/sites/default/files/publications/Wireless-Security.pdf