

Wi-Fi Security Using WEKA

¹Khaing Khaing Wai

¹*Faculty of Computer Systems and Technologies
University of Computer Studies, Yangon, Myanmar
khaingkhaingwai@ucsy.edu.mm*

ABSTRACT

Wi-Fi is a vital piece of day by day life. Billions of people the world over depend upon Wi-Fi in their homes and organizations, to shop, bank, facilitate life, and remain related. Wireless connectivity devices, for example, phones, Laptops and PCs are by and large progressively utilized by University students to get to learning assets nearby systems and the Internet. Most of the phones offer security shows for relationship with a Wi-Fi router. This paper presents a layout of Wi-Fi security and suggestions as indicated by Wi-Fi organization.

Keywords: SSID, Wi-Fi, Wireless Security Protocols, WEP, WPA, WPA2-PSK

1 Introduction

Wireless Internet gets to headway is basically powerfully passed on in both office and open conditions, compared to by Internet clients at home. The web has been progressively given to sift through devices through remote relentlessness (Wi-Fi) frameworks, to be express to the IEEE 802.11 measures. Advances in phone improvements have given telephones proportionate if not more obvious handiness than standard work an area PCs for the utilization of use like web program, media player, Wi-Fi openness, and some more. As the development of versatile turn of events and online life produces affiliations need to give more ideas to Wi-Fi security issues so as to keep the fundamental assaults from programmers that can incite time and money related difficulties in framework fix, inaccessibility of significant associations. Any device that relationship up to the system winds up being a touch of the structure for the affiliation time range. A less secure device will introduce a clear course for a developer to dispatch an assault. In the event that preventive measures are not taken, by at that point, it will take a break for the assailants to dispatch assaults on sorting out assets through the related telephone. In this paper, we will discover how safely the cell phone gather as one with the free Wi-Fi routers. The effects of this evaluation will permit ITC organizations, mastermind officials, and customers, additionally of other for all intents and purposes indistinguishable systems plan better security structures to counter current risks that may make by techniques for phone relationship in Wi-Fi structures. In segment 2, we will examine the various kinds of security conventions utilized in Wi-Fi engaged telephones, the segment 3, we quickly talk about the Wi-Fi organizations/administrations, in segment 4, the proposed system, in segment 5, data information and analysis, at last, conclusions in segment 6.

2 Wireless Security Protocols

Wireless security shows give affirmation endeavors from a phone. The security shows are Wired Equivalent Privacy, Wi-Fi Protected Access, and Wi-Fi Protected Access 2 [1]. Security is a worry as attackers utilize different sorts of hacking programming and method to barge in on security. This security show utilized different estimations to ensure the transmission of data from direct A toward point B.

A. Wired Equivalent Privacy

Wired Equivalent Privacy (WEP) is a security protocol, appeared in the IEEE Wireless Fidelity standard, 802.11b [1], that is wanted to wireless local area network (WLAN) with a degree of security and protection essentially vague based on what is generally expected of a wired LAN. A LAN is by and large ensured by physical security mechanisms (controlled access to a structure, for instance) that are viable for a controlled physical condition, at any rate, might be lacking for WLANs since radio waves are less confined by the dividers containing the system. WEP would like to create relative confirmation to that offered by the wired system's physical security tries by scrambling data transmitted over the WLAN. Information encryption [3] ensures the uncovered remote relationship among customers and segments; when this measure has been taken, other runs of the mill LAN security mechanisms, for example, secret key insurance, from start to finish encryption, virtual private frameworks, and verification can be set up to guarantee confirmation.

B. Wi-Fi Protected Access

Wi-Fi Protected Access (WPA) is a remote security standard to guarantee PCs identified with a Wi-Fi affiliation. Its motivation is to address true deficiencies inside the past framework, the WEP standard. WPA gives customers an undeniably significant level of confirmation that their information will stay ensured by utilizing the Temporal Key Integrity Protocol (TKIP) for information encryption. 802.1x verification has been natural in this protocol to improve client approval. WPA and WPA2 are simultaneous security standards. WPA watched out for a greater bit of the IEEE 802.11i standard, and the WPA2 accreditation accomplished full consistence. All things considered, WPA2 will not work with some more network cards, thusly the essential for simultaneous security standards. WPA utilizes the two different techniques, to be specific WPA-PSK (CCMP), and WPA-PSK (TKIP). Wi-Fi Protected Access joined a 128-bits (TKIP) which adequately makes another key for every datum pack; WEP essentially had a progressively small 40-bits encryption key which was fixed and ought to be physically entered on wireless access focuses (APs)[1]. TKIP was proposed to be utilized with progressively arranged WEP gadgets, with fortified firmware. Notwithstanding, stars found a security stream in TKIP concerning shortcomings in recovering the keystream of information packs; it could just encode "short" (128 bytes) information bundles. This caused TKIP to be dislodged with CCMP (now and again called "AES-CCMP") encryption appear in WPA2, which gives extra security [1], [2].

C. Wi-Fi Protected Access Version 2-Pre-Shared Key

Wi-Fi Protected Access 2 (WPA2), considering IEEE 802.11i, is another wireless security protocol wherein just embraced clients can get to a wireless gadget, with highlights supporting more grounded cryptography (for example Advanced Encryption Standard or AES), more grounded confirmation control (for example Extensible Authentication Protocol or EAP), key association, replay assault affirmation, and information integrity. WPA2-PSK protocol is that the most uncommon Wi-Fi encryption standard which is

executed to overhaul the security of WPA. WPA2 utilizes the 802.11i standard part which contains information encryption computation. WPA2 likewise uses the two combination procedures, to be specific WPA2-PSK (CCMP), and WPA2-PSK (CCMP/TKIP). The validation strategy utilized right now either CCMP or TKIP. Notwithstanding, as by greatness of WPA, in WPA2-PSK just CCMP ought to be the decision of execution, as it utilizes AES [1], [6]. Today, by a long shot the majority of the wireless has a WPA2 security highlight for interfacing with another Wi-Fi gadget. This security protocol was sorted out with a definitive target that product engineers feel that its difficult to break the encryption. A control for using WPA2 is the handling speed. A few supervisors notice that utilizing WPA2 requires logically momentous equipment to view to most remarkable structure execution for significantly used frameworks. The issue was as to using the wireless access point (WAP) or router [5]. The chances of a product designer to agitate into WPA2 security using standard hardware are nil.

3 Wi-Fi Services

Growth within the quantity of customers permitted the grounds to offer free Wi-Fi administration to the customers. This Wi-Fi licenses certain applications to run, for instance, the customers can find the opportunity to look through locales, and email. Then again, certain applications will not be feasible, for example, Facebook, what is the application, Viber, and other prompting applications. The free Wi-Fi awards customers to get the web through their telephones and PCs. Customers need to enter manual delegates to find the opportunity to access their phones. They would then have the alternative to interface with the free Wi-Fi inside the grounds.

4 Proposed Methodology

At first, Acrylic Wi-Fi Professional programming is utilized to collect the information from the live Free-Wi-Fi router. This thing is the best Wi-Fi analyzer which encourages the structure overseer to see a way and Wi-Fi channels, sellers, and security protocol every shipper utilizes [6]. Also, the gathered information is entered in Weka programming to make an expressive assessment of important properties of SSID name, Security, and Vendor. The SSID Device name trademark records the SSID (Service Set Identifier) name of the gadgets that have made the affiliation. The security characteristic records the kind of security used by all of the partner devices. The seller shows the hardware merchant to an access point. The Vendor quality records the gadget seller names.

5 Data Collection and Analysis

Figure 1 shows an area of the screen of Acrylic Wi-Fi Professional programming in its live condition. It shows the 802.11 standards (b, g, just as n) models, most uncommon speed in Mbps, security, Wi-Fi Protected Setup (WPS) accessibility, and Vendor for each device in the affiliation.

SSID	802.11	WEP	WPA	WPA2	WPS	Vendor
10YHw	b, g, n		PSK-TKIP/CCMP	PSK-CCMP	1.0	Shenzhen C-Data Technology Co. Ltd.
10YHw	b, g, n		PSK-TKIP/CCMP	PSK-CCMP	1.0	Shenzhen C-Data Technology Co. Ltd.
10YHw	b, g, n		PSK-TKIP/CCMP	PSK-CCMP	1.0	Shenzhen C-Data Technology Co. Ltd.
V21C	b, g, n		PSK-TKIP/CCMP	PSK-CCMP		DASAN CO. LTD.
MyanmarNet	b, g, n		MGT-TKIP/CCMP	MGT-TKIP/CCMP		TP-LINK TECHNOLOGIES CO. LTD.
GSNTWIF-ABCD	b, g, n		PSK-CCMP	PSK-CCMP		Shenzhen Century Kinyang Technology Co.
Yvaw Play Along	b, g, n		PSK-CCMP	PSK-CCMP	1.0	DASAN Network Solutions
MV1747E371	g	Open				
Chico	b, g, n		PSK-CCMP	PSK-CCMP		
MyanmarNet	b, g, n		MGT-TKIP/CCMP	MGT-TKIP/CCMP		
MyanmarNet	g, n		MGT-CCMP	MGT-CCMP		Ruckus Wireless
VICaCam_8078d	b, g, n			PSK-CCMP	1.0	Shanghai Xiang Technology Co. Ltd.
MyanmarNet	b, g, n		MGT-TKIP/CCMP	MGT-TKIP/CCMP		
10YHw	b, g, n		PSK-TKIP/CCMP	PSK-CCMP		

Figure 1. Portion of Acrylic Wi-Fi Professional

As appeared in Figure 2, the Acrylic dataset contains 5 properties of SSID, Vendor, and Security (WEP, WPA, WPA2). An entirety of 23 records (events) is accessible for assessment purposes.

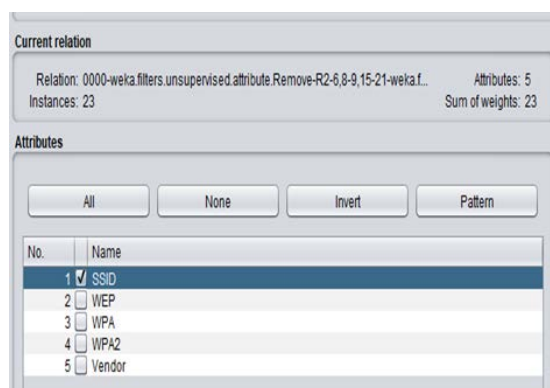


Figure 2. Acrylic Data for Analysis

The SSID of devices that are in a relationship in Figure 3. There are 20 unmistakable SSIDs which addresses just 83% of affiliations. There is an open entryway this SSID was imparted by a relative gadget. Regardless, there is likewise the open entryway that SSID was conveyed from different devices. This default SSID is changed by the device proprietors to keep up a key good way from confusion.

A comparative fundamental merchant of the partner devices is Xiaomi, Oppo, Shenzhen, and Dasan as showed up in Figure 4. These have been perceived as having a spot with device name Android AP. TP-LINK, Shanghai, LG are other dynamic WAPs. This data on Vendor sufficiency by clients can help the ICT benefits in getting ready for network updates and expansions that are material to this greater part classification of the client base. Best practices and organizations from this seller and gadget name can likewise be wrangled later on for this social event for their client perseverance to Xiaomi and it's Android AP Wi-Fi (telephone).

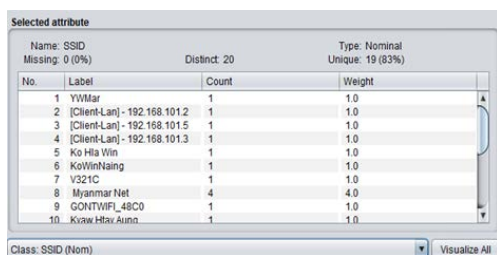


Figure 3. Weka Analysis of Device Names

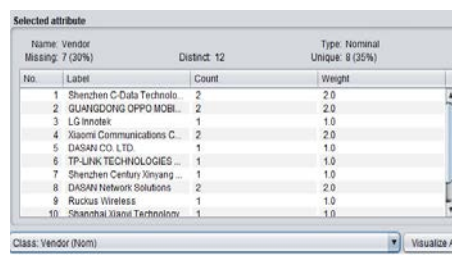


Figure 4. Weka Analysis of Vendors

Figure 5 shows that 18 out of the 32 devices related to utilizing WPA2-PSK security, which is the best security accessible now. An immense segment of this best security identifies with Device Name Android AP and Vendor Xiaomi. 12 others used on any occasion WPA, while 2 devices utilized WEP for the network. While 2 is an unassuming number, it should be seen that a solitary tricky area for the software engineer section can make significant harm sort out assets. From Figure 1 it will, by and large, be seen that WEP is

configured on Shenzhen devices. These devices are WAPs configured and controlled by IT Services. It is progressively canny to uproot these devices if the most indispensable security is inaccessible on these devices.



Figure 5. Weka Analysis of Security (WEP, WPA & WPA2)

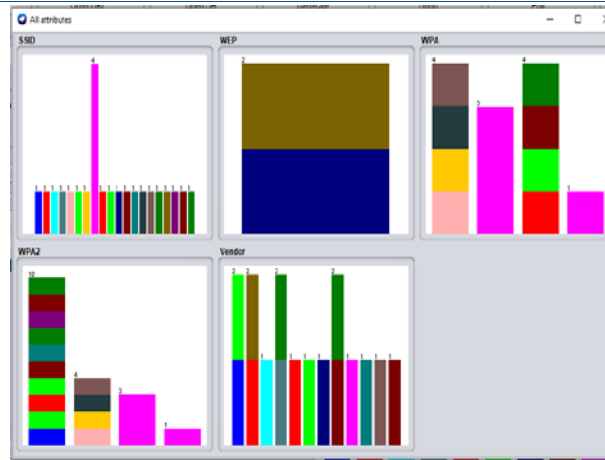


Figure 6. Weka Analysis of Device Names, Vendors & Security (WEP, WPA & WPA2)

In the first spot, we recognize the best security, WPA2-PSK ought to be need number one in organizing issues. The IT Services ought to at first configure its WAPs for WPA2-PSK. It needs to likewise warily screen what sort of telephone or Laptop or PC is a partner with its WAPs. While the free programming mechanical assembly Acrylic Wi-fi Professional was utilized right now, the uncommon decision is to utilize Kali Linux, a Debian-decided Linux appointment which is normal for bleeding-edge bad behavior scene assessment and infiltration testing. Second, give Wi-Fi accessibility free or notwithstanding just by techniques for WPA2-PSK configured settings and devices. Better in spite of everything register the customers and plan their devices at IT Services. We prescribe changing the SSID to customer confirmation numbers and allowing just these to build up the affiliation. This will permit IT Services to consider to effectively who is on the structure at a given time. Additionally, along these lines network issues as indicated by specific customers can be directed on an individual explanation. Third, the customer needs to enter a solid secret word in configuring his/her WPA2-PSK telephone. Forward, if the telephone or PC wishes to set up an affiliation utilizing WEP security, it ought to be denied access for security reasons. Next, sellers ought to configure the most brought security up in their wireless devices as is regularly done, ideally WPA2-PSK. Finally, the merchants need to underline on the security part of their wireless gadgets and make care through their customer documentation of their things.

6 Conclusion

Wi-Fi does not ensure about and can be ambushed by programmers in view of relaxed up security arrangements in a little WAPs. In any case, the positives are that a prevailing piece of customers is interfacing with WAPs utilizing the most raised WPA2-PSK security show through the most recent android telephones. This gives new chances to IT Services to misuse this example.

REFERENCES

- [1] A. Sari and M. Karay, "Comparative Analysis of Wireless Security Protocols: WEP vs WPA", International Journal of Communications, Network and System Sciences, vol. 8, no. 12, pp. 483-491, 2015
- [2] Differencebetween.net, "Difference Between WPA and WPA2 | Difference Between", Differencebetween.net, 2017. [Online]. Available: <http://www.differencebetween.net/technology/difference-wpa-and-wpa2/>. [Accessed: 06-Jun-2017].

- [3] R.Schenk, "Wireless LAN Deployment and Security Basics". PCMAG, 2017. [Online]. Available: <http://www.pcmag.com/article2/0,2817,1157727,00.asp>. [Accessed: 05-Jun-2017].
- [4] Wi-Fiplanet.com, "802.11 WEP: Concepts and Vulnerability", Wifiplanet.com, 2017. [Online]. Available: <http://www.wifiplant.com.tutorials/article.php/1368661/80211-WEP-Concepts-and-Vulnerability.htm>. [Accessed: 05-Jun-2017].
- [5] Whirlpool, "Encryption –WEP and WPA", Whirlpool.net.au. 2017. [Online]. Available: http://whirlpool.net.au/wiki/wlanh_103. [Accessed: 31-May-2017].
- [6] Acrylicwifi.com, "Wi-Fi analyzer –Acrylic Wi-Fi professional for windows", Acrylic Wi-Fi, 2017. [Online]. Available: <https://www.acrylicwifi.com/en/wlan-software/wifi-analyzeer-acrylic-professional/>. [Accessed: 31-May-2017].
- [7] <https://www.wi-fi.org/discover-wi-fi/security>
- [8] <https://www.cyberpunk.rs/wireless-security-protocols-wep-wpa-wpa2-and-wpa3>