International Journal of Computer (IJC)
ISSN 2307-4523 (Print & Online)
© Global Society of Scientific Research and Researchers
http://ijcjournal.org/

Enhanced Wi-Fi Security of University Premises Using MAC Address and Randomly Generated Password

Tanveer Ahmed[a], Md. Shafiqul Islam[b*]

[a,b]*Department of Computer Science and Engineering,*
Dhaka University of Engineering & Technology, Gazipur, Gazipur-1707, Bangladesh
[a]*Email: nobinweb@yahoo.com*
[b]*Email: msislam_80@yahoo.com*

Abstract

Many solutions are available for setting up wireless home networks to get internet connectivity working as quickly as possible. It is also quite risky as numerous security problems can result. Today's Wi-Fi networking products do not always help the situation as configuring their security features, and they can be time-consuming. In this paper, an improved security protocol is proposed for University premises, which is a combination of the process of MAC address filtering and random password generation. If the MAC address match, then the server will send a randomly generated password to the client. As a result, the whole network will face fewer intruders, and the security will be of top-notch. The proposed security solution was compared with the existing four security methods. The proposed solution has universality as the device and software needed for it is available all over the world.

Keywords: Wi-Fi; Security; MAC Address; Random Password.

1. Introduction

In the computer world, the ability of a system to manage, protect, distribute sensitive information means the security of the system. Data security was found several years before the advent of wireless communication due to humankind's need to send information (in war or peacetime) without disclosing its content to others. The first and most known machine, Enigma, was used by the German military to encrypt their messages in WWII. This machine was something similar to a simple typing machine with a scrambler unit to obfuscate the content of the messages [1,2]. Still from that time, many solutions to security threats have been introduced, and most of them were abandoned or replaced by better security standards.

----

* Corresponding author.

These ongoing changes promoted the security field to be a permanent hot topic. In the wireless world security threats were not known to ordinary people till prices of wireless equipment went down around the year 2000. Before that, the military was the number one client for wireless security products, especially during the cold war [3,4]. Wi-Fi networks follow a standard set of rules to achieve their communication; the standard is known as IEEE 802.11. The name of Wi-Fi comes from the Wi-Fi Alliance [5,6]. For interoperability, only Wi-Fi certified equipment is guaranteed, even though non-certified equipment also follows the standard laid out by IEEE. In 1997, the 802.11 standards were made an international standard. In 1999, two new versions, namely 802.11a and 802.11b, were introduced to enable higher data rates. 802.11's use is still growing and is considered an enormous success. Nowadays WLAN is more prevalent in everywhere. However, peoples are afraid of security. They are finding charm to get free from hackers. From that necessity, this work tried to find some secure way. The proposed method gave security using the MAC address and a randomly generated password. There have two strong walls and more steps to ensure security which is most difficult to destroy or hackers will be unable to hack.The main objective of this work is to make a more robust security feature of the wireless networks. This paper describes a few existing security mechanisms with their drawbacks. Then the proposed mechanism is described in section 4.

2. Overview of Wi-Fi Network

The opportunity is given by a wireless-fidelity (Wi-Fi) network to nearby enthusiasts to break into the attached wired network.   It has invented from the dream to network PCs and other devices without any cost and complexity of cable in the last few years ago. It is one of the wireless technologies which came most early in the wireless market. It was designed to use within a short-range communication, for example, shopping malls, office environments, and University premises. The overall goal of this technology is to provide service for mobile computing devices like Laptops, PDA, and smartphones. Wi-Fi networks are the very least consist of two entities that communicate without using any wires. Wi-Fi certified equipment, tested and approved by the Wi-Fi Alliance, bears the Wi-Fi logo as shown in Figure 1. In 1999, the IEEE 802.11 standard was made an international standard and two different versions were made.

Figure 1: Wi-Fi Logo

The 802.11 standard specifies two basic modes of operation. The infrastructure mode [7] is the most commonly used. It allows for either one of the entities to be an access point, and the other entities are referred to as clients. All entities are considered clients in ad-hoc mode. The other mode known as ad-hoc mode may also be referred to as independent mode. Stations in ad-hoc mode, participate in an ad-hoc network; likewise, if they are in infrastructure mode, they participate in an infrastructure network. The wireless interface of a client or access point contains a radio and an antenna to support communication over a wireless medium. IEEE 802.11 specifies groups of frequencies that may be utilized by a network for the avoidance of interference and allow networks to operate in the same locations [8]. Two groups are in the radio frequency band and one in the infrared band of the electromagnetic spectrum. The radio frequencies available to Wi-Fi are in the 2.4 GHz Industrial, Scientific, and Medical (ISM) band and the 5 GHz Unlicensed National Information Structure (UNII) band. Depending on regulatory authorities, the range used by IEEE 802.11b and 802.11g is 2.402-2.495 GHz, 5.12-5.25, 5.25-5.35, and 5.725-5.875 GHz for IEEE 802.11a. The IEEE 802.11 standard divides the 2.4GHz band into 14 channels, but only into three non-overlapping channels. A Wi-Fi network may operate in all of these channels, but a single wireless interface may only operate in one channel. The data rate of a channel can be dynamically adjusted depending on the quality of the channel. The initial version of 802.11 supported data rates of up to 54Mbps (IEEE 802.11a and 802.11g).

3. Overview of Wi-Fi Security

Ensure security is the main thing of the WLAN network. Security is the main thing because it protects transmissions from eavesdropping. The IEEE 802.11 standard is IEEE’s first standard for WLAN. Nevertheless, nowadays, network experts have identified this standard as a lack of some security mechanism.

3.1. WEP

Wired Equivalent Privacy (WEP) was the default encryption protocol introduced in the first IEEE 802.11 standard back in 1999. This security protocol is intended to protect against eavesdropping and physical security attributes, which is equivalent to the security of a wired network. IEEE802.11 architecture specifies WEP as the encryption standard. WEP encrypts a data frame, and it is content to protect authorized users on a WLAN. When anyone enables WEP, a network security key is set up. One computer sends the encrypted information to another computer across that network that is encrypted by that key. The secret key for authentication and encryption used by WEP has the size of 40-bit, whereas other IEEE 802.11 allows 104-bit secret key encryption. WEP is an older network security method that is still available to support older devices, but it is no longer recommended. However, cracking WEP security is relatively easy.

3.2. WPA & WPA2

WPA and WPA2 are two security protocols developed by WI-FI Alliance [9], [10], [11], [12]. WPA provides developed to solve the problems in the WEP cryptographic method. WPA was developed in 2003. Both WPA and WPA2 have two modes of operation: Personal and Enterprise. The Personal mode involves the use of a pre-shared key for authentication, while the Enterprise mode uses IEEE 802.1X and EAP for this purpose. WPA2 was introduced in September 2004. WPA2 extends WPA to include the full set of IEEE 802.11i requirements. WPA uses the improved encryption algorithm known as TKIP (Temporal Key Integrated Protocol). WPA and WPA2 use the cryptographic hash function for data integrity. Now TKIP can be broken easily. There are several trivial weaknesses that have been found, still, none of them are risky with the security recommendations.

However, Authentication mechanisms in WPA-PSK are vulnerable to a dictionary attack, which has already been implemented [13]. This attack is based on capturing the 4-way handshake between client and AP which clearly provides enough information to start an attack. Unlike WEP, where statistical methods can be used to speed up the cracking process [13], the pre-Shared Key (PSK) is derived using the password Based Key Derivation Function (PBKDF2) which is the pseudorandom function that takes several inputs and hashes them multiple times to produce a key[14]. This means that the attacker has all the information and the only thing that the attacker needs is brute force the handshake to match the 256-bit key which can be a passphrase of 8 to 63 printable ASCII characters [3]. The Pairwise Transient Key (PTK) is derived from the PMK via the 4-Way Handshake with information used to calculate its value is transmitted in plain text [15]. This information includes the MAC address of the client, the MAC address of the AP, and the two random numbers (ANonce and SNonce) [15]. The only item missing is the PMK/PSK, so the attackers can simply brute force PMK with the need to know the SSID which is easy to be obtained with a sniffer [13]. Even though WPA-PSK is a 256 bits key in length, it has a major weakness because it is based on the pairwise master key (PMK) that is generated by PBKDF2 key derivation. The PBKDF2 in WPA has five input parameters which are: PMK=PBKDF2 (Password, SSID, SSID length, 4096, 256) [15]. Where 4096 is the number of the iterations of a sub-function and 256 is the length of the output. This means that the strength of PTK relies only on the PMK value, which is the Pre-Shared Key (passphrase) [15].

3.3. RF Shielding

It is practical in some cases to apply specialized wall paint and window film to a room or building to significantly attenuate wireless signals, which keeps the signals from propagating outside a facility. Despite security measures as encryption, hackers may still be able to crack them.

3.4. MAC Address Filtering

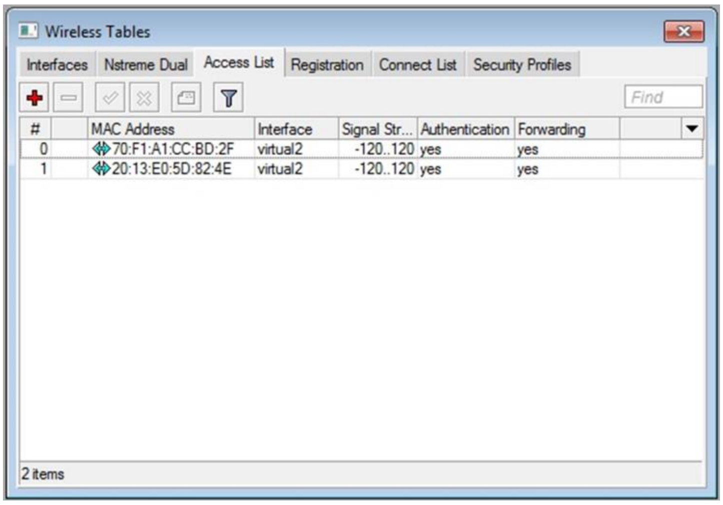
IEEE 802.11 network card has the property to view each client computer by a unique MAC address. Using MAC address filtering, each access point must have a list of authorized client MAC address in its access control list to secure its operation. Initially, MAC address filtering is time-consuming because the administrator has to input the client MAC addresses manually in each access point. Again, since the MAC address list must be kept up-to-date, it’s better suited for a smaller network. MAC address filtering is straightforward to break. By using Sniffers, anyone can get all information on the network and can break security.

4. Experiment

The experiment is divided into two steps. The first step is to obtain and filter the MAC address. The other one is the generation of random password for the requested clients. The following subsection describes the steps briefly.

4.1. MAC Address Filtering Concept

Most Wi-Fi access points and routers embed with a feature called hardware or MAC address filtering. This feature is usually turned "off" by the manufacturer because it requires a bit of effort to set up correctly. However, to improve the security of Wi-Fi LAN (WLAN), consideration of enabling and using MAC address is strongly needed. When the MAC address is enabled, however, the access point or router performs an additional check on a different parameter. The likelihood of preventing network break-ins will be greater if more checks are made. For MAC address filtering, a WLAN administrator must conFigure a list of allowable clients to join the network. First, get the MAC addresses of each client from its operating system or configuration utility. Then, the administrator enters those addresses into a configuration screen of the wireless access point or router, and after that, the filtering option switches on. Once enabled, whenever the wireless access point or router receives a client's request to join the WLAN, it compares the requested client's MAC address with its stored list. Clients in the stored list are authenticated as usual; clients not in the list are denied any access to the WLAN. Another option is online registration. Every new device automatically gets a pop-up message through the browser of the device for online registration. Here clients will be provided his/her phone number, and then the server automatically enters the MAC address into a configuration screen of the wireless access point or router. After that, when a request to join with the WLAN receives by the wireless access point or router, it compares the requesting client's MAC address with the stored list, and the matched client gets access to the WLAN.



#		MAC Address	Interface	Signal Str...	Authentication	Forwarding
0		70:F1:A1:CC:BD:2F	virtual2	-120..120	yes	yes
1		20:13:E0:5D:82:4E	virtual2	-120..120	yes	yes

2 items

Figure 2: Authenticating MAC Address

4.2. Randomly Password Generating Concept

When the requested Clients MAC addresses on the list authenticate as expected, then the Server PC automatically generates a text or password. Then this text or password will be sent on that client with a request to enter this password. When the client will be entering this text or password and again make a request to join with the WLAN, it compares the text or password against which was generated for this client’s MAC address. If it matches then finally that client will be able to access the WLAN. One text or password will be provided against only one authenticates MAC address. The client will get randomly another text or password for each several time access; when the client will be going out of range or disconnect the WLAN.

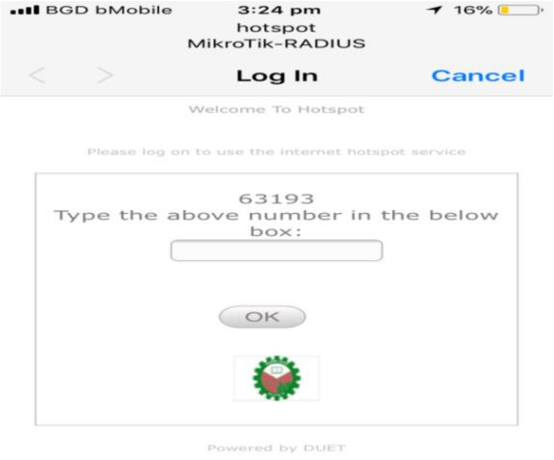
Step-1: The client will be sent a request for a connection.

Step-2: When the wireless access point or server found a request at that time, it will be checked whether that client MAC address is in the database.

Step-3: If the client MAC address is not in the database, then the database will not entertain further requests from that client.

If the client MAC address is found in the database, then it will go the next step.

Step-4: In this step, Server PC will randomly generate a text or password and send it to that client with a request to enter this.



BGD bMobile 3:24 pm 16%

hotspot
MikroTik-RADIUS

Log In Cancel

Welcome To Hotspot

Please log on to use the internet hotspot service

63193
Type the above number in the below box:

OK

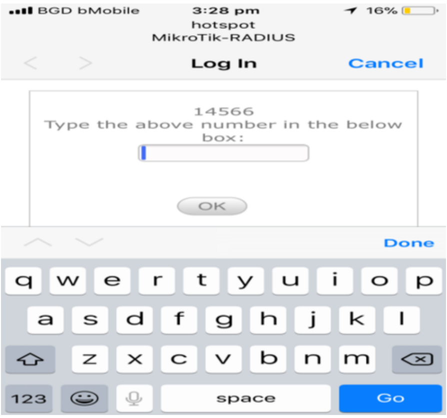
Powered by DUET

Figure 3: Random Password Generation

Step-5: Here client will enter that text or password and sent it to the server PC.

Step-6: The server PC checks the text or password with the provided text or password. If matches, the server will give access to Wi-Fi use.

If don't match, then step4 will be repeated.



BGD bMobile 3:28 pm 16%

hotspot
MikroTik-RADIUS

Log In Cancel

14566
Type the above number in the below box:

OK

Done

Figure 4: Client Enters the Randomly Generated Password

The overall experimental operation of the proposed method is shown in Figure 5.

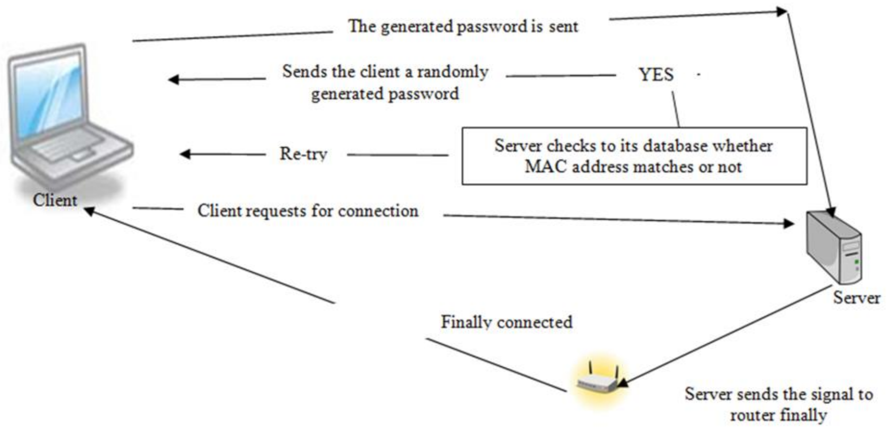

The generated password is sent
Sends the client a randomly generated password
YES
Re-try
Server checks to its database whether MAC address matches or not
Client
Client requests for connection
Server
Finally connected
Server sends the signal to router finally

Figure 5: Experimental operation of the proposed protocol, with the request from left to right

5. Conclusion

In this paper, we have shown how security in wireless data networks has evolved over the last decades. We have also discussed how wireless networks play a crucial role in exposing the system to more possible attacks. Security hazards will always be around; they can only be avoided if the right policies are used. We proposed some of the ways that can be utilized to improve the security of wireless networks within the University premises. We have used MAC address filtering and random password generation technique to secure the Wi-Fi network of our University premises. Here we have two measures from protecting the hackers. Only authentic clients will be able to use the network and receive the expected speed.

6. Recommendations

We have studied different security measures and applied MAC address filtering and random password generation to secure the Wi-Fi of University premises. Our further analysis will be concentrated on merging other available more existing security features.

References

[1]. James P. Anderson, Computer Security Technology Planning Study Volume II, ESDTR-73-51, Vol. II, Electronic Systems Division, Air Force Systems Command, Hanscom Field, Bedford, MA 01730.

[2]. NIST Special Publication 800-153, Guidelines for Securing Wireless Local Area Networks (WLANs), February 2012.

[3]. Edney and William A. Arbaugh, Real 802.11 Security: Wi-Fi Protected Access and 802.11i, Addison-Wesley Longman Publishing Co., Inc., USA, 2003.

[4]. Thomas Hardjono and Lakshminath R. Dondeti, Security In Wireless LANS And MANS, Artech House, Inc., USA, 2005.

[5]. Justin Berg, The IEEE 802.11 Standardization: Its History, Specifications, Implementations, and

Future, Technical Report GMU-TCOM-TR-8, Technical Report Series, George Mason University, USA.

[6]. Science Direct Topics, Computer Science, Wireless Fidelity, viewed 27 July 2020. < https://www.sciencedirect.com/ topics/computer-science/wireless-fidelity>.

[7]. IEEE Standards Association. STD 802.11, 1999 Edition (R2003), 2003. < https://standards.ieee.org/standard/802_11-1999.html>.

[8]. Sandeep Sharma, Rajesh Mishra, and Karan Singh, A Review on Wireless Network Security, International Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness, January 2013, PP.668-681.

[9]. Promila and R. S. Chhillar, Review of Wi-Fi Security Techniques, International Journal of Modern Engineering Research (IJMER), Vol. 2, Issue 5, Sep.-Oct. 2012, pp-3479-3481.

[10]. Discover Wi-Fi, Security, viewed 29 July 2020. <http://www.wi-fi.org/discover-wi-fi/security>.

[11]. Guillaume Lehembre, Wi-Fi Security-WEP,WPA and WPA2, Hakin9-IT Security Magazine, June 2005, pp. 114.

[12]. Jared Howe, WEP, WPA, WPA2 and Home Security, viewed 28 July 2020. <http://blog.privatewifi.com/wep-wpa-wpa2-and-home-security>.

[13]. Lehembre, G.: Wi-Fi Security- WEP, WPA and WPA2 (June 2005).

[14]. Beck, M., Tews, E.:- Practical attacks against WEP and WPA ||. In: WiSec 2009: Proceedings of the Second ACM Conference on Wireless Network Security. ACM, NewYork (2009).

[15]. Mylonas, P., Mavridis, I.P., Androulakis, A.-I.E, Halkias, A.B.: Real-life paradigms of wireless netwok security attacks (2011).