Wi-Fi Hacking and Security

Shivam Lohani
Dept of Electronics and Communication Engineering
Birla Institute of Applied Sciences, Bhimtal, Uttarakhand-India

Abstract- *The wireless network has become an important part of our daily life. Wireless networks have replaced wired network to a great extent. But with the advancement of technology, many cyber-attacks have occurred. This paper is all about wireless networks (Wi-Fi), its uses, different modes of Wi-Fi, different types of Wi-Fi encryption (WEP, WPA/WPA2) and procedure to crack WEP and WPA/WPA2. We'll also come across some common attacks which a hacker performs after connecting to a network. Further, we will discuss the methods that can help us to protect our wireless home networks and a new method of using encrypted tunnel is also proposed in this paper.*

Keywords- Wireless Fidelity (Wi-Fi), Access Point (AP), Wired Equivalent Protection (WEP), Wi-Fi Protected Access (WPA), Media Access Control (MAC), Man in the middle (MITM), WiMax and aircrack-ng.

I. INTRODUCTION

The full form of Wi-Fi is 'Wireless Fidelity' [5], [7-10], [13]. It is being used as an alternative to wired Local Area Network (LAN). Nowadays, Wi-Fi plays an important role in almost every organization, schools, colleges, etc. Wi-Fi is used in many electronic devices like mobile phones, cameras, laptops, PCs, etc. It is easy to setup and portable. Also, multiple users can connect to a single Wi-Fi Access Point (AP) easily. But with ease of communication, many security issues have been occurred because of unauthorized users and Wi-Fi Hackers. In order to reduce unauthorized access, encryption techniques like WEP, WPA/WPA2 were introduced in Wireless network. These methods are used to encrypt the data flowing through the network so that hacker cannot fetch the data. But still, there are some loopholes and using them we can get an unauthorized access to any type of wireless network. Wi-Fi uses Radio Frequency (RF) to transmit data through the air. Wi-Fi also provides high-speed internet access and data transfer. In a Wi- Fi network, the most important component is an Access Point (AP).

The Access Point (AP) has a radio transmitter and a radio receiver. It is used to connect to an internet network. Nowadays Routers come with inbuilt access points and can be connected directly to the internet network using Ethernet cable. Previously we need to connect router and AP separately. First, we needed to connect AP to a router using Ethernet and then router to internet network as shown in the figure below:

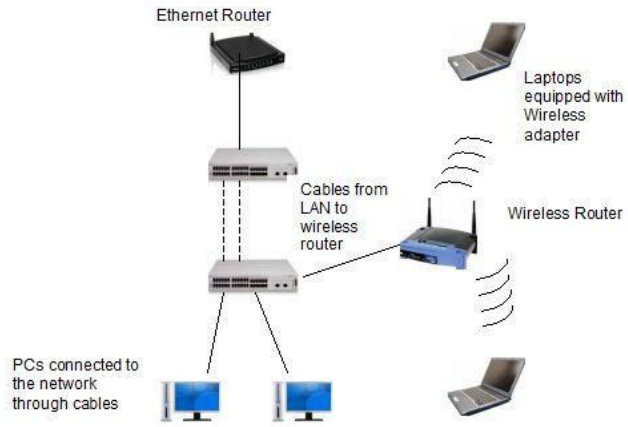

Fig.1: Access Point[19]

II. WIRELESS NETWORK CHALLENGES

We know that wireless network has completely changed the way of sharing information. The wireless network has proved to be very advantageous but on the other hand, it has to face some other challenges too. The three main challenges faced by a Wi-Fi network are [1], [2]:

1.Confidentiality:

Only authorized users are allowed to read or access data or information.

2.Integrity:

It is defined as the information should not be opened by third party and it should reach in the same format as it was sent by the sending party. Hackers may perform 'Man in the middle (Mitm)' [16] attack to steal the data and information flowing between sender and receiver.

MITM can be done using tools like Ettercap, mitm framework, burp suite, etc. [16]

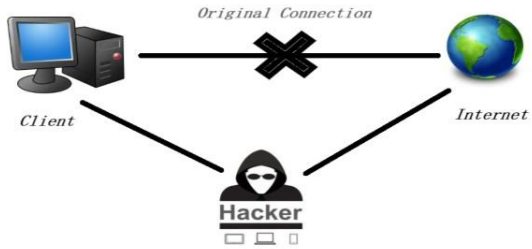

Fig.2: Man in the middle attack (MITM)

3.Authentication:

The main issue with a wireless network is its mode of transmission. Wi-Fi uses EM waves to send and receive data packets and can be easily captured using right transceiver equipment. So the authorized client must be allowed to connect to the wireless network.

III. WI-FI MODES

Before studying about encryption techniques and how to crack Wi-Fi passwords let us discuss the two modes of Wi-Fi [14-17] which are

1. Managed Mode:

It is the default mode of a wireless card. The AP will transfer or receive the data packet of the connected users only. In this mode, the AP will not monitor other packets within its range.

2. Monitor Mode:

In this mode AP will receive all the packets within the range i.e., it can monitor ever packet flowing within the range. This mode is used by Hackers to scan the available APs and users connected to these APs. This mode can be enabled using the command line or any other Wi-Fi hacking tool.

IV. WI-FI ENCRYPTION AND HOW THEY ARE HACKED

1.WEP:

WEP was the first cryptographic method to facilitate data privacy and authentication in a wireless network. It was introduced in 1997.WEP is a part of IEEE

802.11 network [1], [3], [8-11], [13] to defend link-level data during the wireless transmission. WEP uses an algorithm called RC4 (Rivest Cipher 4) to encrypt information. In this, each data packet is encrypted at the AP and then it is decrypted at the receiver end. WEP ensures that each packet has a unique 24-bit

Initialization Vector (IV), this IV is contained in the packet as plain text. In a busy network, we'll have very large no. of packets, this means the possibility of unique random IVs will be exhausted. When we sniff these packets we get similar IVs. So, the more IVs we collect there will be more chances to break the password. WEP encryption can be cracked within minutes. There are many tools that can break WEP encrypted Wi-Fi security but the most effective tools are aircrack-ng [14], [15], [17] and wifite.

After having such type of vulnerabilities, in 2003 the Wi-Fi Alliance WEP had been replaced by WPA. The main trouble of WEP was-it uses static encryption keys.

2.WPA/WPA2:

WPA was developed in 2003. WPA/WPA2 were developed for solving the problems in WEP method. WPA2 was introduced in September 2004. WPA addresses a subset of the IEEE 802.11i specification that addresses the weaknesses of WEP. WPA is easier to configure and it is extra secure than WEP. WPA uses TKIP (Temporary Key Integrated Protocol). In TKIP each packet is encrypted with a unique temporary key, this means the number of data packet we collect to crack the password (like WEP) is irrelevant. Now, TKIP can be broken easily. WPA2 uses Advanced Encryption Standard. WPA2 may not work with some older network cards. WPA2 have the four main advantages that are Mutual authentication, Strong encryption, Interoperability, Ease to use. WPA/WPA2 use the cryptographic hash function for data integrity.

To crack WPA/WPA2 we need to capture the handshake packet from the network. The only packets that contain info that helps us to crack the password are the '4-way handshake' packet. Every time a user connects to the AP a 4-way handshake occurs between the client and AP. By capturing this handshake packet we can crack the password from this handshake file.

So, to crack any WPA/WPA2 password

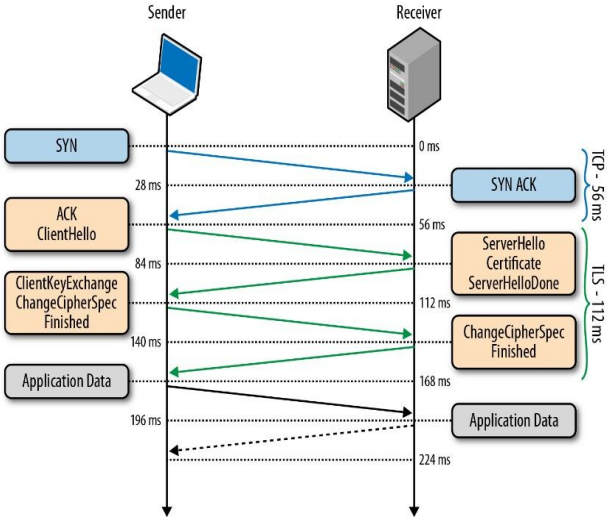

Fig.3: 4-Way Handshake [18]

- Identify your target
- Deauthenticate the connected users to capture handshake file when they connect to the AP again.
- Crack the handshake file using a wordlist or tools like 'John the ripper'

NOTE: If the password is very strong it may take several days to crack the password.

The Wireless Link should be secured from malicious attacks as well as DoS Attacks (Denial of Service Attacks).

The common attacks which reduces the security of Wireless Networks are Message Reply Attack, Man in the Middle Attack, etc. The Man in the Middle Attack (Mitm) attack occurs on that security mechanism which doesn't provide mutual authentication.

To make wireless networks more secured IEEE introduced the technology of disabling SSID, MAC (Media Access Control) filtering. In MAC filtering we can whitelist the MAC address of specific system and only that system can access the network. But with advancement in technology Hackers can change the MAC address of their system and can access the network and this method also became vulnerable. WiMax standards were introduced, for solving the security issues of older wireless networks. It is the new advancement in the wireless network [4]. WiMax is still undergoing development and still, the securing problems are not being decreased by WiMax technology. It also has some vulnerabilities like it lacks mutual authentication and is suspected to relays attacks, spoofing of MAC address of Subscriber Station (SS) and PMK authorization vulnerabilities.

V. SECURING WIRELESS NETWORKS: [6]

Change wireless network's name

The wireless network name i.e. SSID should be changed so that hackers cannot identify your router's model.

Use a strong password

The password should have a minimum of 8 characters and must include uppercase letters, lowercase letter, numbers and special characters.

Network encryption should be enabled

The best encryption setting to increase your Wi-Fi protection is WPA2 AES. Advanced Encryption Standard, is an encryption system used by governments around the world, including the USA. Nowadays, most of the Wi-Fi routers has WPA2 AES.

Updating router's software

The wireless router's software should be up to date so that its security is maintained.

Disable DCHP in router

When DCHP is enabled, 26 possible IP addresses can be allowed on the network. You can limit the range so that only a certain number of users can access the network. [1], [9], [10]

MAC Filtering

In MAC filtering, only the registered MAC addresses are allowed to use the network. It is one of the best methods to secure a wireless home network.

Disable wireless administrating

Disable the setting that allows administrating the router through a wireless connection this means we need to connect LAN wire for changing the administrator settings of router. This disables any wireless hacking into the router.

Using encrypted tunnel

Wi-Fi Alliance can use an encryption tunnel for secure exchange of password during 4-way handshake. The unencrypted packets can be securely sent using encrypted tunnel. An encrypted tunnel is a way off communication

which prevents any type of surveillance by telecom companies, Internet Service Provider (ISP) or any third party. It is used by WhatsApp community (end-to-end encryption) and many other companies.

VI. CONCLUSION

Wireless networks changed the way of communication but securing a wireless network is not an easy task. There are several protocols and methods that can protect the wireless network but until now there is no such protocol or method which can provide 100% secured wireless network. Many type of research are being conducted worldwide to design the best protocol for securing wireless networks. Many methods are discussed above so that we can maintain the security of our home network to some extent.

REFERENCES

[1] Data Communication and Networking by Behrouz A. Forouzan
[2] White paper: WLAN security Today: wireless more secure than wired by Siemens Enterprise Communications.
[3] Sara Nasre Wireless Lan Security Research Paper IT 6823 Information Security Instructor: Dr. Andy Ju An Wang Spring 2004.
[4] Security Issues on Converged Wi-Fi & WiMAX Networks by Prof. Anand Nayyar, Lecturer, P.G. Department of Computer Science, K. L. S. D College Ludhiana, anand nayyar@yahoo.co.in.
[5] Wireless network security? Author:-Paul Asadoorian, GCIA, GCIH. Contributions by Larry Pesce, GCIA, GAWN PaulDotCom.
[6] Securing Wi-Fi network (10 steps of diy security) by Rakesh
M Goyal and Ankur Goyal
[7] Establishing wireless robust security networks: a guide to IEEE 802.11i by Sheila Frankel Bernard Eydt Les Owens Karen Scarfone.
[8] Wireless LAN security today and tomorrow By Sangram Gayal and Dr. S. A. Vetha Manickam.
[9] Introduction to WI-FI network security by Bradley Mitchell, About.com.
[10] The state of WI-FI security by WI-FI Alliance.
[11] WI-FI security –WEP, WPA and WPA2 by Guillaume Lehembre.
[12] Wireless network security 802.11, Bluetooth and handheld devices by Tom Karygiannis, Les Owens.
[13] WEP, WPA, WPA2 and home security by Jared Howe.
[14] Introduction to Wi-Fi security and Aircrack-ng, Thomas d'Otreppe, Author of Aircrack-ng
[15] Aircrack-ng Documentation
[16] Black Track 5 Cookbook by David De Smet, Willie Pritchett
[17] The Beginner's Guide to Hacking Wireless Networks, Logan Styles
[18] nikhilmachcha.wordpress.com
[19] Orbit-computer-solutions