

Wi-Fi Networks Security Enhancement

By

Razibul Hasan

MIEEE, Baridhara, Dhaka-1206, Bangladesh

kustia@gmail.com

ABSTRACT

In this paper, author focuses on the security issues related to a particular wireless technology, namely Wi-Fi networks. Wi-Fi is one of today's leading wireless technologies, with Wi-Fi support being integrated into more and more devices. Wi-Fi networks can be simple or complex depending on needs and design. Poorly secured Wi-Fi networks can be utilized to attack networks and corporations from the inside, instead of attempting to do it externally from the Internet. An imperfectly secured Wi-Fi network can be exploited for other purposes that do not directly threaten the owner of the compromised Wi-Fi networks. Security is now an essential element that forms the cornerstone of every corporate network. There are many owners of Wi-Fi networks are oblivious to the risks involved and fail to secure their networks adequately. Even large corporations may not be able to secure their Wi-Fi networks as much as they wish. The constraints following a secure implementation will not always enable all of their users to connect with the ease required. More secure systems are complex, and interoperability can become a problem. Wi-Fi is an acronym for wireless fidelity, commonly seen as IEEE 802.11b. A user with a Wi-Fi product may use any brand of access point with any other brand of client hardware that is built to use Wi-Fi. In this paper author also focused some techniques in router settings which may use to safe any Wi-Fi Networks.

General Terms

Wireless Networks Security Enhancement, Information Security in Wi-Fi Networks

Keywords

Wireless Networks, Wi-Fi Security, WEP Attacks, WPA Attacks, WLAN, IEEE 802.11 Securities, Wireless intrusion.

1. INTRODUCTION

Wi-Fi has a lot of security vulnerabilities. Unfortunately for Wi-Fi the vulnerabilities and the severity of them became widely known too late. At the time of the famous paper on how to crack a WEP key, early 2001, there were already millions of 802.11 products sold world-wide. At that point, issuing a fix or recalling all products was not feasible. Instead, consumers in need of better security supplemented WEP with VPN and IEEE 802.1X. More secure alternatives, such as WPA, were introduced later and could only be made available as an addition to WEP. The

complexity of setting up a secure wireless network increased and the percentage of wireless networks that use the best mechanisms to enable security is not as high as it should be. The final replacement for both WEP and WPA; IEEE 802.11i, also referred to as Wi-Fi Protected Access version 2 (WPA2) by the Wi-Fi Alliance, is at present considered secure, but is not discussed in this thesis. The practical examples in this chapter are executed on the Linux operating system, but most of them can also be performed from the Windows platform.

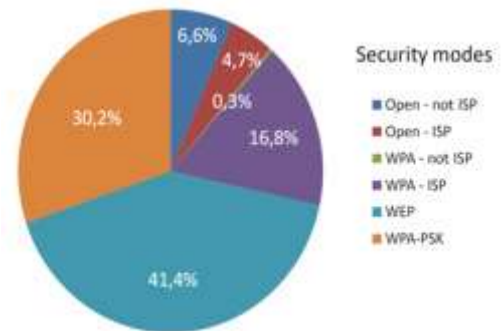


Fig 1: Security modes of Wi-Fi Access Points

The biggest contribution to the failure of WEP is quite certainly the ability for a malicious hacker to obtain the secret WEP key. Nothing more than access to the radio signal, off-the-shelf Wi-Fi equipment, and open source software are required. The attack to compromise the key was first described in "Weaknesses in the Key Scheduling Algorithm of RC4" to summarize the attack, some of the keys which are seeded to RC4 and generate a key sequence, expose bits of the actual key used. The value of the initial key sequence is determined by a small part of the key. When comparing a great number of key sequences generated by the set of weak keys, statistics will point to a specific secret key. Most Wi-Fi equipment will accept a pass phrase when initially setting up a WEP encrypted network. The pass phrase is used to generate the WEP key. Vendors have different methods of using the pass phrase to construct the final WEP key. This paper goal is explores security vulnerabilities in Wireless-Fidelity (Wi-Fi) networks.

2. CORPORATE Wi-Fi SECURITY CHALLENGES

A hacker or attacker can gather a lot of intelligence on the network and its users. That should make it clear why everyone should secure their Wi-Fi networks. The main focus of this paper is the discovery of the additional advantages an anonymity network, such as poorly designed Wi-Fi network. Although some hackers may connect to Wi-Fi networks for the pure fun and not use it for anything except confirming access is possible, others can benefit quite a lot from a connection to a Wi-Fi network. Innocent use such as checking the e-mail account and downloading the latest on-line newspapers are actually quite common among neighbors. The problem for the intruders of a Wi-Fi network is that the owners can monitor everything they use the connection for.

The corporate network owners can capture clear text passwords when intruders are checking e-mail, logging into resources on the web, etc. Every web site the intruders visit can be monitored, or altered by the owner of the network. Even man-in-the-middle attacks on secure Internet services can be attempted. All in all, using a compromised Wi-Fi network for anything considered normal usage of the Internet is a dangerous habit for an intruder. Vulnerable Wi-Fi networks give rise to a huge variety of possible further malicious exploitation. With the Tor network a “good” intruder can even protect himself from malicious Wi-Fi network owners, or other intruders. This paper only mentioned a few scenarios, reading e-mail, reporting spy activities, breaking into computers on the network, monitoring users of the network, and a couple more. If anyone still wants to keep their corporate Wi-Fi connection unsecured after reading this paper they should read it again. Primary factors that define security in a wireless environment can be sort out to five elements. Theft, Access Control, Authentication, Encryption, Safeguards.

2.1 Theft

Unauthorized users often try to log into a network to steal corporate data for profit. Employees who have been terminated often feel resentment and anger against their former employer. It is possible for some users to turn that anger into an attempt to steal corporate data before leaving their company. This is why the easiest type of security measure is simply to disable a user’s account at the time of termination. This action is a good security measure and prevents the likelihood of account abuse during the transition out of the company.

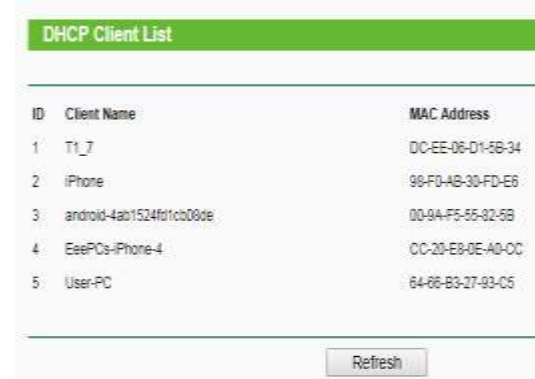
2.2 Access Control

Many companies set very simple access permissions. You must be wary that networks are designed to increase interoperability so that it is a simple matter for a user to click on his “Network Neighborhood” icon in Windows and see all the wired and wireless devices on his network segment. Some users want to share a document from one employee to another so they just share “Drive C” on the network. But if they don’t remember to turn off the sharing, everyone within that network segment has full read and write permission to that user’s Drive C. If there is a virus running across your network, you can bet that that user’s computer is fully vulnerable and will most definitely be compromised. Wireless networks not only have all the same

access control vulnerabilities as wired networks, but they can easily be accessed by outsiders. The most common type of attack is simply to sit outside an office building and use a wireless network interface card to roam onto any available 802.11b network. Since the majority of users fail to set even the simplest access control barriers that prevent a random user from accessing the network, everything on your network becomes vulnerable to attack, theft, or destruction from a virus.

2.3 Authentication

In most wireless networks, businesses often configure one account, “Wireless User,” and that account can be used by several different devices. The problem is that a hacker (with his own wireless device) could easily log onto to this general account and gain access to your network. To prevent an unauthorized user from authenticating himself into your network, you can set your router to permit only connections from authorized wireless network cards. Each wireless network card has a Media Access Control (MAC) address that uniquely identifies it. You can tell your router only to authenticate those wireless users with a network card that is pre-authenticated to use your network. This protects you against users who are trying to gain access to your system by roaming around the perimeter of your building looking for good reception to log onto your local area network.



ID	Client Name	MAC Address
1	T1_7	DC-EE-06-D1-58-34
2	iPhone	98-FD-AB-30-FD-E6
3	android-4a1524f1c008de	00-9A-F5-55-82-5B
4	EeePCs-iPhone-4	0C-20-E8-0E-A0-0C
5	User-PC	64-86-83-27-93-05

Fig 2: Clients MAC list in Router DHCP configuration of Wi-Fi

2.4 Encryption

If a user is not able directly to log into your network, he may use a wireless “packet sniff” to try and eavesdrop on the network traffic. In that way, even if the hacker is unable to authenticate himself onto your network, he can still steal sensitive corporate data by monitoring your traffic for usable information. In addition to viewing private data files, the hacker is potentially able to “sniff” usernames, passwords, and other private information to gain access onto your network. Wireless routers support medium and strong levels of encryption that scramble the data and make it unusable to anyone trying to eavesdrop on the network traffic. Only the users at either end of the “authorized” connection can view and use the data. Unfortunately, most users don’t turn on encryption in their wireless devices to protect themselves against eavesdropping! Most wireless

routers have an internal Web site that allows for the very simple and easy configuration of data privacy. Wired equivalent privacy (WEP) is a security protocol for wireless local area networks (WLANs) designated by the 802.11b standard. WEP offers a level of security similar to that of a wired LAN. Wired LANs offer greater security than WLANs because LANs offer the protection of being physically located in a building, whereas a wireless network inside a building cannot necessarily be protected from unauthorized access when no encryption is used. WLANs do not have the same physical confinements and are more vulnerable to hackers. WEP provides security by encrypting data over radio waves so that it is protected as it is transmitted from one end point to another. WEP, used on both data link and physical layers, does not provide point-to-point security. Most wireless routers offer 64- and 128-bit encryption with a user specified encryption key that scrambles your data according to your input. This key is needed at points to decode the data into a usable form. Most users, however, keep this option disabled and therefore are vulnerable to anyone intercepting network traffic or even roaming onto the network.

2.5 Safeguards

The best safeguard is to become familiar with your WLAN and your wireless router. You should take the steps above into serious consideration and establish an encryption key at least at the 64-bit, but preferably at the 128-bit level. However, it is important to note that some wireless network cards only support the lower level of encryption; many companies often charge a few more dollars to have their cards support the 128-bit encryption scheme. Once you have turned on encryption, you may then see that your system supports traffic only by wireless network card MAC addresses that you can specify. This precludes someone's trying to break into your WLAN from outside your building or from the parking lot that is in range of your wireless transceiver array. As a network administrator, there are a number of ways you can safeguard your WLAN against intrusion by following some very simple, commonsense steps to make certain you are not being hacked. Wireless routers always have an activity light that shows you when traffic is flowing across the WLAN. There are also a number of software utilities that measure network traffic, where that traffic is going, and the throughput of each connection. If you see an unusual amount of network traffic flowing across your wireless network and the activity light of your wireless router is congested with an enormous amount of traffic, then you know something is wrong! You can trace each connection into the router and if there is a connection that doesn't belong then you know someone may have hacked into your system. Commonsense types of safeguards would indicate that a normal user wouldn't be using the wireless connection to capacity for any prolonged period of time.

3. TYPES OF ATTACK ON WI-FI NETWORKS

WLANs have additional security threats to consider that are RF in nature. Protocol-level attacks that attempt to penetrate Wi-Fi data security include rogue access points,

authentication attacks, evil twin access points, man-in-the-middle, Wi-Fi phishing, and malicious eavesdropping. Most of these attacks exist at layer 2 of the OSI model. Proper authentication, encryption, and segmentation security solutions can be implemented to mitigate many of these well-known attacks. Layer 2 security monitoring solutions can also be put in place to detect when layer 2 attacks are taking place. Beyond wireless DoS attacks, there are several points of vulnerability within your WLAN that can be disrupted or destroyed by knowledgeable hackers who are trying to corrupt your wireless infrastructure. The most vulnerable points include Access point, Antennas, Wireless NICs, Cable connectors, Hardware servers, Software bugs and viruses. It is simple to infect software from virtually anywhere. However, what is not commonly known is that hackers can send firmware upgrade attacks to your wireless router and access point. The firmware in these devices is a software file that updates your device to take advantage of new features and functionality. If a hacker gains access to this device, he can rewrite a valid firmware file or simply corrupt it and fail to load the firmware correctly. 802.11 use spread-spectrum technology, which sounds almost like background noise to the average person. However, someone skilled in eavesdropping techniques can determine the transmission parameters of the 802.11 signal in order to decode the spreading code and put it into usable form. One form of protection is to shield your facility by limiting the range of your wireless equipment to those inside your corporate facilities only. Every packet transmitted in Wi-Fi networks contains bits of information used to maintain the various layers of the communication. Although packets may be encrypted in Wi-Fi networks, they still have plaintext headers.

3.1 Attacking WEP

Wired Equivalent Privacy (WEP) is a security algorithm for IEEE 802.11 wireless networks. Introduced as part of the original 802.11 standard ratified in September 1999, its intention was to provide data confidentiality comparable to that of a traditional wired network. WEP, recognizable by the key of 10 or 26 hexadecimal digits, is widely in use and is often the first security choice presented to users by router configuration tools. As mentioned above, the WEP protocol is flawless. No matter how complicated is the key used, it is possible to extract it with minimum effort. In the following pictures, we will see a network secured with this protocol. Although its name implies that it is as secure as a wired connection, WEP has been demonstrated to have numerous flaws and has been deprecated in favor of newer standards such as WPA2. Additionally, we have to consider that when a user wants to extract the produced key to store it in a flash drive or elsewhere, she need to copy each pair of the hexadecimal number separately. It is less possible that anyone will ever bother to change that key once it is produced. For our experiments, the key for the network was chosen on purpose to be a word not existing in the English or in the Greek dictionary. Even without a WEP key it is possible to scan the wired network for computers, and also port scan both wired and wireless computers. It can be argued that it is much easier to first crack the WEP key, and then perform the scanning detailed in the next section. But

this attack can be performed after the attacker has sent a single de-authentication frame in shared key authentication networks. In below figure author shows how one can check LAN and WAN settings in his network.



Fig 3: Wireless LAN adapter and wireless networks IP and Configuration

3.2 Attacking WPA

Unlike WEP, WPA is not vulnerable to such attacks. It implements a different algorithm so it has none of the weaknesses of its ancestor. It has only a serious weakness which has to be taken under serious consideration. The packet, which contains the key in question, is the "association" packet. In order to get upper hand on this packet, one needs to wait until a new station connects to the network or somehow force an already connected station to disconnect, so that station will obviously try to reconnect. This can be used also for Denial of Service Attacks. Because of the above security measure of the WPA protocol, the dictionary attack cannot happen against the real transmitting station AP. It has to take place off line.

3.3 Layer 1 DoS Attacks

A particularly troublesome issue for Wi-Fi security is the denial of service (DoS) attack. In a DoS attack, the goal of the attacker is not to penetrate or steal data from the network it is simply to disable the network. For mission-critical systems, this is a serious security concern. If the WLAN goes down, then any application or network resource being accessed through the WLAN is now no longer available. The wireless VoIP phone conversation comes to an abrupt end, communications with your database server are no longer possible, and wireless access to an Internet gateway has been closed. Many denials of service attacks exist at layer 2 and occur when an attacker manipulates information in the layer 2 headers of an 802.11 management frame and then retransmits the edited frames into a wireless environment with some sort of packet generator. Numerous published layer 2 DoS attacks exist. The most common is achieved by manipulating de authentication or disassociation management frames. Currently, layer 2 DoS attacks cannot easily be prevented, but can be easily detected.

3.4 Intentional DoS

Intentional DoS can be described as malicious attack from an individual that possesses some sort of RF signal generator device. Signal generators exist that transmit in both the 2.4 GHz ISM band and the 5 GHz UNII bands [13]. Signal generators often are used for legitimate testing purposes, such as to provide a power source to measure

coax loss with a wattmeter. The signal generator has now been transformed into a jamming device that will overtake most 802.11 radio cards that transmit at a maximum of 100 mw (+20 dBm). Higher gain antennas can be combined with the signal generator to achieve more radiated power and extend the range of the DoS attack. Unidirectional antennas can be used to focus a layer 1 DoS jamming attack.

3.5 Unintentional DoS

Can RF interference still cause a denial of service even though there is no malicious attack? All sorts of devices transmit in the very crowded 2.4 GHz ISM band. RF video cameras, baby monitors, cordless phones, and microwave ovens are all potential sources of interference. The whole point of the original site survey is to eliminate these sources of interference. Unintentional interference may cause continuous DoS, however, the disruption of service is often sporadic. This disruption of service will upset the performance of Wi-Fi networks used for data applications but can completely disrupt VoIP communications within a Wi-Fi network. At the very least, unintentional interference will result in retransmissions. The site survey eliminated these sources of interference initially; however, full-time or part-time spectrum monitoring may be necessary in case these interfering devices reappear.

4. SOME STEP TO SECURE

CORPORATE WI-FI NETWORKS

It is important to note that while no wireless security solution is 100 percent effective, you can take very simple preventive steps to ensure your corporate Wi-Fi is as secure as possible. When a hacker tries to intercept your network data or compromise your system, the more difficult you make his job, the more likely it is that you will have time to detect the attempted incursion into your system and prevent it. Protection is your best defense when it comes to 802.11.

4.1 Change Default Administrator User and Passwords

At the core of most Wi-Fi home networks is an access point or router. To set up these pieces of equipment, manufacturers provide Web pages that allow owners to enter their network address and account information. These Web tools are protected with a login screen (username and password) so that only the rightful owner can do this. However, for any given piece of equipment, the logins provided are simple and very well-known to hackers on the Internet. Change these settings immediately.

4.2 Turn on WPA / WEP Encryption

All Wi-Fi equipment supports some form of encryption. Encryption technology scrambles messages sent over wireless networks so that they cannot be easily read by humans. Several encryption technologies exist for Wi-Fi today. Naturally you will want to pick the strongest form of encryption that works with your wireless network. However, the way these technologies work, all Wi-Fi devices on your network must share the identical encryption settings. Therefore you may need to find a "lowest common denominator" setting.

4.3 Change the Default SSID

Access points and routers all use a network name called the SSID. Manufacturers normally ship their products with the same SSID set. For example, the SSID for Linksys devices is normally "linksys." True, knowing the SSID does not by itself allow your neighbours to break into your network, but it is a start. More importantly, when someone finds a default SSID, they see it is a poorly configured network and are much more likely to attack it. Change the default SSID immediately when configuring wireless security on your network [12].

4.4 Enable MAC Address Filtering

Each piece of Wi-Fi gear possesses a unique identifier called the physical address or MAC address. Access points and routers keep track of the MAC addresses of all devices that connect to them. Many such products offer the owner an option to key in the MAC addresses of their home equipment that restricts the network to only allow connections from those devices. Do this, but also know that the feature is not as powerful as it may seem. Hackers and their software programs can fake MAC addresses easily.

4.5 Disable SSID Broadcast

In Wi-Fi networking, the wireless access point or router typically broadcasts the network name (SSID) over the air at regular intervals. This feature was designed for businesses and mobile hotspots where Wi-Fi clients may roam in and out of range. In the home, this roaming feature is unnecessary, and it increases the likelihood someone will try to log in to your home network. Fortunately, most Wi-Fi access points allow the SSID broadcast feature to be disabled by the network administrator.

4.6 Do Not Auto Connect to Open Wi-Fi Networks

Connecting to an open Wi-Fi network such as a free wireless hotspot or your neighbour's router exposes your computer to security risks. Although not normally enabled, most computers have a setting available allowing these connections to happen automatically without notifying the user.

4.7 Assign Static IP Addresses to Devices

Most home net workers gravitate toward using dynamic IP addresses. DHCP technology is indeed easy to set up. Unfortunately, this convenience also works to the advantage of network attackers, who can easily obtain valid IP addresses from your network's DHCP pool. Turn off DHCP on the router or access point, set a fixed IP address range instead, and then configure each connected device to match. Use a private IP address range (like 192.168.0.x) to prevent computers from being directly reached from the Internet.

4.8 Enable Firewalls on Each Computer and the Router

Modern network routers contain built-in firewall capability, but the option also exists to disable them. Ensure that your router's firewall is turned on. For extra protection, consider

installing and running personal firewall software on each computer connected to the router.

4.9 Position the Router or Access Point Safely

Wi-Fi signals normally reach to the exterior of a home. A small amount of signal leakage outdoors is not a problem, but the further this signal reaches, the easier it is for others to detect and exploit. Wi-Fi signals often reach through neighbouring homes and into streets, for example. When installing a wireless home network, the position of the access point or router determines its reach. Try to position these devices near the centre of the home rather than near windows to minimize leakage [14].

4.10 Turn off the Network during Extended Periods of Non Use

The ultimate in wireless security measures, shutting down your network will most certainly prevent outside hackers from breaking in! While impractical to turn off and on the devices frequently, at least consider doing so during travel or extended periods offline. Computer disk drives have been known to suffer from power cycle wear-and-tear, but this is a secondary concern for broadband modems and routers.

5. CONCLUSIONS

Wif-Fi Networks may check their settings from command view by using ipconfig /all. WPA protocol should be used, WPA-2 is preferable, the network secret has to be changed frequently, the pass phrase should not exist in a dictionary and it should be at least 20 characters long. As an extra security measure the pass phrase should contain some symbols and some capital letters, MAC Address Security and filtering should be used only as a complimentary and an extra security measure. If used as a standalone security measure is useless as it can be penetrated in seconds with not much of an effort. Even equipment that can be configured to be secure, are left unsecured, many times due to the increased complexity of access point setups. The attention vulnerable Wi-Fi networks receive from hackers is tremendous, vulnerabilities are not only discovered, but they are refined by others and implemented and combined by a whole online community. A compromised network is a great utility for several parties. Malicious hackers can monitor the users of a network, giving the hackers many opportunities to cause havoc. The risk of getting a visit from someone with bad intentions is currently fairly low, but as it is rather easy to obtain enough knowledge and equipment to compromise a Wi-Fi network, the risks will only rise. The 92% of the wireless networks implemented today, are not using any serious security, although the wireless security nowadays is reliable. The fact that more and more networks become secure means that the remaining insecure network will be hunted down by malicious hackers and abused.

6. REFERENCES

- [1] IEEE STD 802.11i. IEEE Standard Amendment 6: Medium Access Control (MAC) Security Enhancements, 2004.

- [2] J. Edney, W. Arbaugh, "Real 802.11 Security: WiFi Protected Access and 802.11i Addison-Wesley", 2004.
- [3] Wi-Fi, <http://en.wikipedia.org/wiki/Wi-Fi>
- [4] Discussion forum surrounding Wi-Fi. URL <http://www.netstumbler.org>
- [5] Wi-Fi Alliance. (2003, February 6). Retrieved 01 16, 2008, from Enterprise Solutions for Wireless LAN Security: http://www.securitytechnet.com/resource/hot-topic/wlan/Whitepaper_Wi-Fi_Enterprise2-6-03.pdf
- [6] Andrew Vladimirov, K. V, Wi-Fi: The Secrets of Wireless Hacking, 2006
- [7] Hallvar Helleseth, Wi-Fi Security, "How to Break and Exploit", June 2006
- [8] Stewart S. Miller, Wi-Fi security, "Enhance security and maintain privacy of mission-critical data, even when going wireless", New York, 2003
- [9] Wi-Fi Security best practices, <http://www.airtightnetworks.com/fileadmin/pdf>
- [10] Frank Sweetser, WPI Network Operations and Security, <http://www.wpi.edu/Academics/>
- [11] Wi-Fi Protected Access, http://en.wikipedia.org/wiki/Wi-Fi_Protected_Access
- [12] How to Secure Your Wi-Fi Network, http://www.pcworld.com/article/130330/how_to_secure_your_wireless_network.html
- [13] David Coleman, and Neil Diener, "Protecting Wi-Fi networks from Layer 1 security threats", 2007
- [14] Wireless Home Network Security, <http://compnetworking.about.com/od/wirelesssecurity>