IJMSIT

International Journal of Multidisciplinary Studies and Innovative Technologies

Volume : 3
Number: 2
Year: 2019
Pages: 86 - 98

Wi-Fi Security Analysis For E&M-Government Applications

Ahmet EFE*[1], Mesrure Betül KAPLAN [2]

[1]*Ankara Development Agency, PhD, CISA, CRISC, PMP, Turkey*
[2]*Department of Computer, Faculty of Engineering, Yıldırım Beyazıt University, Ankara, Turkey*
** Corresponding author: icsiacag@gmail.com*

Abstract- As a sub-branch of Radio Frequency (RF) technology, the Wi-Fi and its area of usage has evolved over time and become pervasive for availability of all e-government applications and services. Computers and many other devices, including smart phones and PDAs, can connect to the internet wirelessly using Wi-Fi. Also, wireless networks are desirable to many organizations because they increase workforce flexibility and save cabling costs. Wi-Fi is considered as the main internet connection for home, small corporate and local government internal networks, while for central government and mid and big size companies it is a complementary and parallel to cabled internet. As the war-driving has become one of the major threats to Wi-Fi users, free-to-serve and open-to-public Wi-Fi poses another threat to hackers and lamer as they can hide themselves to catch their internet traffic and credentials. That is why; the Wi-Fi and its security become important and popular concepts in the knowledge era and technological era. For all various users that range from experts who work at computer science or information technology, to novices who use the Internet; this paper describes the fundamental Wi-Fi and Wi-Fi security issues to establish a greater awareness.

Keywords- *Wireless Fidelity, WLAN, E-government security, Information Security*

I. INTRODUCTION

Both businesses and government agencies are increasingly concerned about the surging threats to/from wireless devices and networks. The development of e-government, which is based on internet, meets fatal security problems due to the complexity and vulnerability of network. Generally speaking, the security risks e-government facing includes the following aspects [25]:

Information Intercepting

It means that the related e-government users or invaders capture or steal the e-information from governments or other users. This is a breach of confidentiality of information. Personal, corporate, strategic and health data can be obtained by third parties.

Information Tampering

The internet attackers tamper, insert or delete original data through various technical methods, and transmit them to the destination, in order to damage the integrality of the data. This can affect availability of data for data users and owners.

Services Denying

It is the complete invalidation of the network system or the servers system in some period. It mainly comes from the attack of the hackers or the virus, and the man-made destruction of the devices as well. This also can affect availability of data for data users and owners.

System Resources Stealing

In the network system environment, the stealing of the system resources is very common. This can be done either physically or virtually.

Information Tampering

It means that after the attackers know the rules of the data in the network information or after they have decoded the government information; they could pretend legal users or make false information to cheat other users. The main forms include pretending users to get illegal certifications, forging e-mails, etc. This can affect integrity of data for data users and owners.

Factor	E-government	M-government
Designed To	Service Centric	Individual Centric
Key Access Channel	Portals, Websites	iPhone, Android, Blackberry, Tablets…Mobile Apps
Data Location	Classic Data Center	Usually Cloud Based
Application Delivery	Web based	Government App store or public app store
Public Private Partnership (service development)	Low	High (developers can build apps using government open data)

Figure 1. Transition from e-government to m-government [5]

As it is seen in the above fig.1 it is evident that there is a tendency from e-government towards mobile m-government. This mobilization in the electronic government services is partly stemming from widespread usage of wireless that triggers and eases use of mobile apps.

The paper expresses the Wi-Fi and the Wi-Fi security issues with an emphasis on e-government aspects. As more and more wirelessly connected networks come online and also, almost many people utilize and take advantage the Internet, Internet based technologies and applications wirelessly using Wi-Fi. Thereby, the security becomes a prominent concern. Wi-Fi insecurity can result in detrimental effects to both individuals and organizations. An unsecured Wi-Fi connection makes it easier for hackers to access private files and information, and it allows strangers to use internet connection. Hence, we try to explain these two terms in this paper to establish a greater awareness of the problems associated with wireless security.

The Wi-Fi stands for “Wireless Fidelity”. Wi-Fi is the name given by the Wi-Fi Alliance to the IEEE 802.11 suite of standards. 802.11 defined the initial standard for wireless local area networks (WLANs), but it was considered too slow for some applications and so was superseded by the extensions 802.11a, 802.11b, 802.11g, 802.1n and later by 802.1ac. At its most basic, Wi-Fi is the transmission of radio signals. It was designed to provide in-building broadband coverage. So, Wi-Fi has become the de facto standard for last mile broadband connectivity in homes, offices, and public hotspot locations [4].

Before Wi-Fi, we were using maps and compass when we wanted to travel to anywhere that we don’t

know how to go. However, now with Wi-Fi, we have used the Google Maps for arriving at places. Thus, with Wi-Fi we have gained some benefits. But, what are the benefits of Wi-Fi over a more traditional wired network? The following list summarizes some of the benefits of a Wi-Fi network.

•Wireless Ethernet: Wi-Fi is an Ethernet replacement. Wi-Fi and Ethernet, both IEEE 802 networks, share some core elements.

•Extended Access: The absence of wires and cables extends access to places where wires and cables cannot go or where it is too expensive for them to go.

•Cost Reduction: As mentioned above, the absence of wires and cables brings down cost. This is accomplished by a combination of factors, the relatively low cost of wireless routers, and no need for trenching, drilling and other methods that may be necessary to make physical connections.

•Mobility: Wires tie someone down to one location. Going wireless means someone has the freedom to change his/her location without losing connection.

•Flexibility: Extended access, cost reductions, and mobility create opportunities for new applications as well as the possibility of creative new solutions for legacy applications.

Wireless security is the prevention of unauthorized access or damage to electronic devices using wireless networks. Securing communication and services in wireless networks is a complex problem. Wireless networks are a broadcast technology, meaning that anyone within radio range can intercept the signal. Hackers can easily intercept wireless network traffic over open air connections and extract information like passwords and credit card numbers. Several Wi-Fi security technologies have been developed to combat hackers, of course, although some of these technologies can be defeated relatively easily. If the signal is not encrypted, the transmission can be read by anyone with a Wi-Fi capable device. Approximately 65% of all wireless networks use some form of encryption, but many use older, less secure standard. This insecurity has allowed wireless networks to serve as the vector for a number of high-profile attacks.

Attacks on the Wi-Fi network can be divided into two classes: one on network access control, data confidentiality and data integrity protection and attack; the other is based on wireless communication network design, deployment, and maintenance of the unique methods of attack. For the first type of attack can also occur in the cable under the environment of network, wireless network security is on the basis of a traditional wired network adds new security threats. But in all cases they should be handled by the security techniques.

II. PROBLEM DEFINITION

There is a rapidly growing concern for threats of wireless networks. A security expert at the University of Leuven in Belgium published findings that showed that a widely used encryption system for wireless networks could give attackers an opening to steal sensitive information such as emails, chat histories and credit card numbers. The government organization also referred users to a vulnerability note published by Carnegie Mellon University's Software Engineering Institute. The exploit would allow hackers to eavesdrop on Internet traffic between computers and wireless access points. The findings are significant because of the wide range of devices that could be affected [22].

The impact of exploiting these vulnerabilities includes decryption, packet replay, TCP connection hijacking, HTTP content injection and others," the alert says, detailing a number of potential attacks. It adds that, since the vulnerability is in the protocol itself, rather than any specific device or software, "Most or all correct implementations of the standard will be affected [17].

A similar risk arises from the easy availability of mobile wireless routers. For very little cost a "hacker" can set up a free WiFi hotspot and mount a "man-in-the-middle" attack to obtain valid user names and passwords, which can then be used to gain access into corporate computer systems. As a result, the value of valid credentials to a cybercriminal is eight times greater than current credit card details. Such attacks can even be used to defeat the security around SSL and SSH encrypted traffic [18].

In a written statement, the researchers have discovered serious weaknesses in WPA2, a protocol that secures all modern protected WiFi networks. An attacker within range of a victim can exploit these weaknesses using key reinstallation attacks. Attackers can use this novel attack technique to read information that was previously assumed to be safely encrypted. This can be abused to steal sensitive information such as credit card

numbers, passwords, chat messages, emails, photos, and so on. This attack is believed to target a process called a handshake, an automated negotiation that happens between devices on a network [19].

III. COMPLEXYTY ANALYSIS OF WIRELESS

Although the Albert Einstein Archives in Jerusalem informed us that there's no record of Einstein ever saying this, it's apt: wireless transmission doesn't make intuitive sense; we can only use analogy to understand how information moves from one place to another without physical elements we can see in between. Fortunately for us, wireless just works—look at cordless phones, cell phones, AM and FM radio stations, walkie-talkies, and satellite television dishes. Wireless is all over these days, and unintuitive or not, it is rooted in basic physics.

Wireless networking relies on the same principles that drive cordless phones and all these other wireless devices. A transceiver (a combination of transmitter and receiver) sends signals by vibrating waves of electromagnetic radiation that propagate out from an antenna; the same antenna receives signals by being appropriately vibrated by passing signals at the right frequencies (Huang, Ye, & Shi, 2014).

Early wireless networks used frequencies of electromagnetic radiation just below the visible spectrum, namely infrared. Infrared networking had (and still has) a huge limitation: anyone needs perfect line of sight from one infrared transceiver to another. In large offices with numerous cubicles, it is difficult to position the transceivers high enough for the signal to get over partitions and equally hard to ensure that people standing around gabbing don't block the network signal (Karthik & kuracha, 2015).

Wireless networking overcomes the line-of-sight problem by jumping to a different portion of the electromagnetic spectrum. Modern wireless networks typically work at 2.4 GHz or 5 GHz, far below the visible light spectrum (Figure 1). At those frequencies, the wavelength of each transmission is so small that signals can pass through seemingly solid objects.

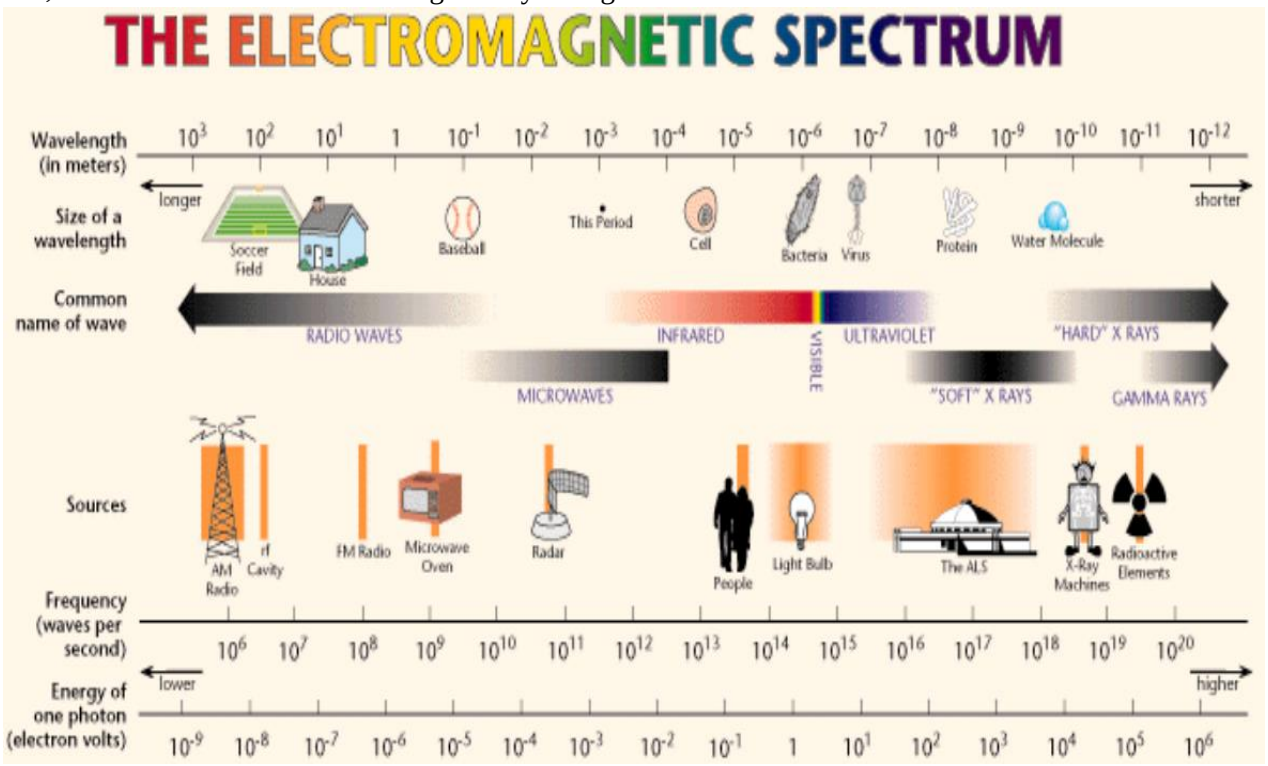

Figure 2. Electro Magnetic Spectrum [25]

Although modern wireless networks offer the longest range when they have line of sight, they also work perfectly well over short distances in interior spaces (Figure 2). However, some interior obstacles can reduce signal quality and make it necessary to adjust the network layout. For instance, brick walls can hold a lot

of water, and water can block energy from the frequencies at which 2.4 GHz networks work. Some houses and offices have metal in their interiors, such as chicken wire supporting plaster or ductwork, and metal can also interfere with network signals (Engst & Fleishman, 2004).

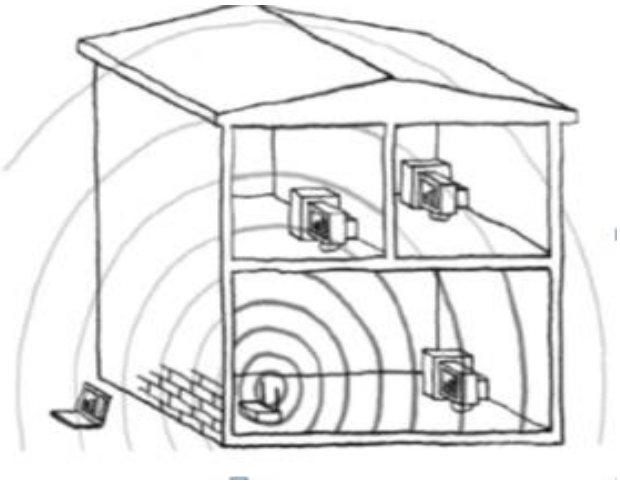

Figure 3. How Radio Waves Travels (Digi, 2008)

.

IV. WORKING CONCEPTS

A. Radio Signals

Radio Signals are the keys, which make Wi-Fi networking possible. These radio signals transmitted from Wi-Fi antennas are picked up by Wi-Fi receivers, such as computers and cell phones that are equipped with Wi-Fi cards. Whenever, a computer receives any of the signals within the range of a Wi-Fi network, which is usually 300-500 feet for antennas, the Wi-Fi card reads the signals and thus creates an internet connection between the user and the network without the use of a cord.

B. Access Points

An access point is the brains of a wireless network. It can perform a number of different tasks, some of which are optional, depending on what needed. Unfortunately, someone likely to run across numerous different terms for access point, including “wireless gateway,” “wireless router,” and “base station.” Also, the term is frequently abbreviated to “AP” in technical literature.

Access points, consisting of antennas and routers, are the main source that transmit and receive radio waves. Antennas work stronger and have a longer radio transmission with a radius of 300-500 feet, which are used in public areas while the weaker yet effective router is more suitable for homes with a radio transmission of 100-150 feet.

C. Wi-Fi Cards

Wi-Fi cards are invisible cards that connect computer to the antenna for a direct connection to the internet. Wi-Fi cards can be external or internal.

D. Wi-Fi Hotspots

A Wi-Fi hotspot is created by installing an access point to an internet connection. The access point transmits a wireless signal over a short distance It typically covers around 300 feet. When a Wi-Fi enabled device such as a Pocket PC encounters a hotspot, the device can connect to that network wirelessly.

Most hotspots are located in places that are readily accessible to the public such as airports, coffee shops, hotels, book stores, and campus environments. 802.11b is the most common specification for hotspots worldwide. The 802.11g standard is backwards compatible with 802.11b.

The largest public Wi-Fi networks are provided by private internet service providers (ISPs); they charge a fee to the users who want to access the internet. So, Hotspots are increasingly developing around the world. In fact, T-Mobile USA controls more than 4,100 hotspots located in public locations such as Starbucks, Borders, Kinko's, and the airline clubs of Delta, United, and US Airways. Even select McDonald's restaurants now feature Wi-Fi hotspot access.

Any notebook computer with integrated wireless, a wireless adapter attached to the motherboard by the manufacturer, or a wireless adapter such as a PCMCIA card can access a wireless network. Furthermore, all Pocket PCs or Palm units with Compact Flash, SD I/O support, or built-in Wi-Fi, can access hotspots.

Some Hotspots require WEP key to connect, which is considered as private and secure. As for open connections, anyone with a Wi-Fi card can have access to that hotspot. So in order to have internet access under WEP, the user must input the WEP key code (NSK, 2014).

E. Wi-Fi Standards

No matter what the context, successful communication can take place only if all parties are speaking the same language about the same topic. In the networking world, such a language is called a *specification*, and if it's sufficiently agreed-upon by enough parties or given a stamp of approval by an industrial body or institution it may increase in status to become a *standard*.

When it is talked about wireless networking, it is about a family of standards that work together: equipment that supports one standard is always compatible with other devices that support the same standard. Even better, backward compatibility has been the rule rather than the exception. That is why; *the 802.11 standard* is defined through several specifications of WLANs. It defines an over-the-air interface between a wireless client and a base station or between two wireless clients. All wireless routers at the time were built around these standard specifications (Mitchell, 2017).

V. WI-FI SECURITY STANDARDS FOR MITIGATIONS AND PERFORMANCE

The original IEEE 802.11 specification provided a security strategy known as WEP, which was quickly found to be flawed. It was widely implemented in Wi-Fi networks and is still in use today.

The next generation of security strategies, popularly known as WPA and WPA2. They are both based on the IEEE 802.11i specification. Prior to the ratification of 802.11i by the IEEE, Wi-Fi Protected Access (WPA) was released by the Wi-Fi Alliance as a firmware upgrade to WEP based systems. WPA is based on the third draft of 802.11i, whereas WPA2 is based on the final, ratified version. Authentication, access control and key management are the same in WPA and WPA2; however, the mechanisms used to ensure data integrity and confidentiality is different (Scarfon & Dicoi, 2007).

A. WEP

The original IEEE 802.11 specification introduced Wired Equivalency Privacy (WEP). As the name implies, WEP was supposed to ensure the same security as exists for a wired connection. Unfortunately, it does not. But even though it is easily broken, WEP is still worth using. Why? Because WEP is broken like a lock is broken after someone kicks in front door. There is no question that the lock did not keep out the intruder who showed up on owner's porch, but garden variety burglar is not that energetic and is looking for an easier mark, someone who has left their door unlocked or even open. In other words, if WEP is all someone have access to, and then by all means use it. Meanwhile, be aware that there are several security limitations with this method;

• *No mutual authentication*: only clients can authenticate, not access points. This can lead to rogue APs.

• *No user-level authentication*: static WEP key stored on device. This is a problem if the device is stolen or otherwise accessed without permission.

• *Reuse of static key*: the key used for authentication and encryption is the same.

B. WPA

WPA stands for Wi-Fi Protected Access. It is a security technology for Wi-Fi wireless computer networks. WPA improves on the authentication and encryption features of WEP. In fact, WPA was developed by the networking industry in response to the weaknesses of WEP.

WPA provides stronger encryption than WEP through use of either of two standard technologies: *Temporal Key Integrity Protocol (TKIP)* and *Advanced Encryption Standard (AES).* WPA also includes built-in authentication support that WEP does not offer. Overall, WPA provides comparable security to VPN tunneling with WEP, with the benefit of easier administration and use. Wi-Fi devices typically support multiple variations of WPA technology. Traditional WPA, also known as *WPA-Personal* and sometimes also called WPA-PSK (for pre-shared key), is designed for home networking while another version, *WPA-Enterprise*, is designed for corporate networks.

C. WPA2

WPA2 is an improved version of WPA supported by all newer Wi-Fi equipment. The WPA implemented a new key management scheme known as the Temporal Key Integrity Protocol (TKIP). Like WPA, WPA2 also exists in Personal/PSK and Enterprise forms. It's an upgrade from the original WPA, which was designed as a replacement for the older and much less secure WEP.

WPA2 is used on all certified Wi-Fi hardware since 2006 and is based on the IEEE 802.11i technology standard for data encryption. When WPA2 is enabled with its strongest encryption option, anyone else within range of the network might be able to see the traffic, but it will be scrambled with the most up-to-date encryption standards.

WPA and WPA2 sometimes interfere with each other if both are enabled on a router at the same time, and can cause client connection failures. Usage of WPA2 decreases the performance of network connections due to the extra processing load of encryption and decryption. That said, the performance impact of WPA2 is usually negligible, especially when compared with the increased security risk of using WPA or WEP, or even no encryption at all.

D. 802.1X

It provides network authentication to both Wi-Fi and other types of networks. It tends to be used by larger businesses as this technology requires additional expertise to set up and maintain. 802.1X works with both Wi-Fi and other types of networks. In a Wi-Fi configuration, administrators normally configure 802.1X authentication to work together with WPA/WPA2-Enterprise encryption. 802.1X is also known as RADIUS..

VI. HOW TO PROVIDE WIFI SECURITY?

Security has been one of the major deficiencies in WiFi. A wireless device needs to have some way to reliably prove its identity and to reliably confirm the identity of the device on the other end of the connection (Wiki, 2017). Without cables and Ethernet jacks, this is not as straightforward as it once was. The fact that no obvious physical connection is required to send and receive packets brings up questions regarding the ability of others to not only read legitimate packets but also to be able to interject their own. These activities may or may not be malicious, but in all cases they should be handled by the security components of the network (Rowan, 2010).

A. Security Goals of Wi-Fi

There are three goals that must be met to have a successful security strategy in a wireless network:

• Mutual Authentication

• Private Communication

• Data Integrity

The goal of mutual authentication is to make sure that both the client and AP are who they say they are. Both parties have an interest is verifying identities since either side can cause trouble for the other. Typically, the AP is a gatekeeper for access to other network resources and regardless of the relative importance of the resource, be it family photos from last year's vacation or the database from a major bank detailing customer account information, access to that resource needs to be controlled by the proper authority. On the other side, there is a need for the AP to authenticate itself because rogue APs can do substantial damage by stealing passwords from unsuspecting clients and causing denial-of-service attacks. The goal of privacy addresses the challenge of sending information through open space, which is accessible to everyone, friend and foe alike. Strong encryption algorithms and dynamic key derivation strategies solve this problem. The goal of integrity means that the data is intact when it is received. The protocols used for mutual authentication, privacy and integrity will be discussed in more detail throughout this section of paper (Specially WEP, WPA and WPA2) (Griffith, 2016).

B. Wi-Fi Security Issues

Attacks on the WIFI network can be divided into two classes (Ranjan, R.N.Shukla, & Lohia, 2014):

1- The first is on network access control, data confidentiality and data integrity protection and attack and

2- The second is based on wireless communication network design, deployment, and maintenance of the unique methods of attack.

Based on these classes, some Wi-Fi security issues need to be analyzed:

C. Weaknesses of the WEP encryption

Mechanism of WEP was intended to provide cryptographic measures to prevent eavesdropping of the wireless network communication. However, WEP was found to have many weaknesses in the end. Encryption algorithms are too simple; WEP is easy to crack keys by someone else. Key management is complex, use WEP keys need to accept an external key management system of control, because of the way this process is complex and requires manual operation, so many networks to

facilitate the deployment, use the default WEP key, and allowing hackers to crack the key difficulty is significantly reduced.

D. Wireless signal attack and war-driving

Search for wireless signal is also a method of attacking wireless networks; there are many identification and attack techniques and software for wireless networks. Nets tumbler software is software that is widely used to found a wireless network. Many wireless network is not using encryption, even if the encryption feature is used, if it is not turn off the AP broadcast message feature, AP Radio and still contains a lot of information can be used to infer the WEP key information in clear text, such as network name, SSID, and other conditions to hackers intrusions (Stanley, 2005).

Here we demonstrate a wlan hack using Kali Linux. There is various software to crack Wi-Fİ using Kali. “Airmon-ng” is a software package in the aircrack-ng network software suite “Aircrack-ng” is a network software suite consisting of a detector, packet sniffer, WEP and WPA/WPA2-PSK cracker and analysis tool for 802.11 wireless LANs. The program runs under Linux and Windows. The aircrack-ng suite has airmon-ng as a program that is used to set a network adapter to monitor mode to allow it to capture the packets transmitted from a network or access point without having to connect to it first. The captured packets may later be analyzed using other packages from the “aircrack-ng” suite. As it is seen in the figure below, WPA username and password is easily taken using airmon tool.


root@kali:~# airmon-ng check kill
Killing these processes:
PID Name
1186 wpa_supplicant
root@kali:~# airmon-ng check
No interfering processes found
root@kali:~# airmon-ng start wlan0
No interfering processes found
PHY Interface Driver Chipset
phy0 wlan0 ath9k Qualcomm Atheros AR9485 Wireless Network Adapter (rev 01)
(mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]wlan0mon)
(mac80211 station mode vif disabled for [phy0]wlan0)
root@kali:~# airodump-ng wlan0mon
BSSID PWR Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
B0:C5:54:86:5D:70 -63 42 1 0 8 54e. WPA2 CCMP PSK Deepu_007
EC:22:80:5B:7F:DC -86 8 2 0 1 54e WPA2 CCMP PSK D-Link_DIR-600M
BSSID STATION PWR Rate Lost Frames Probe
B0:C5:54:86:5D:70 44:80:EB:B7:6D:12 -53 0 - 0e 0 1
EC:22:80:5B:7F:DC 9C:D3:5B:28:84:90 -1 0e- 0 0 2
root@kali:~# reaver -i wlan0mon -b B0:C5:54:86:5D:70 -vv -K 1
Reaver v1.5.2 Wi Protected Setup Attack Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tacnetsol.com>
mod by t6_x <t6_x@hotmail.com> & DataHead & Soxrok2212
[+] Waiting for beacon from B0:C5:54:86:5D:70
[+] Switching wlan0mon to channel 1
[+] Switching wlan0mon to channel 2
[+] Switching wlan0mon to channel 3
Running reaver with the correct pin, wait ...
Cmd : reaver -i wlan0mon -b B0:C5:54:86:5D:70 -c 8 -s y -vv -p 14600715
[Reaver Test] BSSID: B0:C5:54:86:5D:70
[Reaver Test] Channel: 8
[Reaver Test] [+] WPS PIN: '14600715'
[Reaver Test] [+] WPA PSK: 'dhiman007'
[Reaver Test] [+] AP SSID: 'Deepu_007'

There are alternate ways of cracking Wifi WPA WPA2 passwords, by using HashCat or cudaHashcat or oclHashcat techniques to crack unknown Wifi WPA WPA2 passwords [13].. The benefit of using Hashcat is the ability to create hacker's own rule to match a pattern and do a Brute-force attack. This is an alternative to using dictionary attack where dictionary can contain only certain amount of words. Hashcat can crack Wifi WPA/WPA2 passwords and anyone can also use it to crack MD5, phpBB, MySQL and SHA1 passwords [14]. (Dark, 2015). Using Hashcat is a good option as if it is possible to guess 1 or 2 characters in a password, it only takes few minutes. For example: if just 3 characters in a password are known, it takes 12 minutes to crack it. If 4 characters in a password, it takes 3 minutes. Possibilities of cracking are a lot higher in this way.

root@kali:~# wifite –wpa

WiFite can also be used instead of other guides that use Aircrack-ng, it is because it's faster and we don't have to type in commands. WiFite can capture handshake sessions.

D. Wireless network eavesdropping

Disclosure threats include eavesdropping, interception and Monitoring. Tap refers to eavesdropping through a network of computer communication in electronic form, it is passive and intrusion detection cannot detect the device. Even if the network isn't foreign broadcasting network information, if someone can find any information in clear text, an attacker can still use some of the network tools, such as AiroPeek and TCPDump to monitor and analyze traffic, so as to identify information that can be overcome.

VII. MEASURES FOR WI-FI SECURITY

According to wireless network management and maintenance practices to troubleshoot wireless networking security threats, mainly uses the following security measures.

Overall Design of the Wi-Fi Network

Analysis of network security as a whole is to conduct a comprehensive analysis of security threats on the network may save. When identifying potential invasive threat, to be included in the network planning, take timely measures, excluding the wireless network security threats. Select comparison has security guarantee of products to deployment network and set for of network structure is ensure network security of premise conditions, while also to do is as follows several points: modified device of default value; to base station as a RAS; specified dedicated wireless network of IP agreement; in AP using speed most fast of, and to support of security function; considered antenna on authorized user and intrusion who of effect; for all user using consistent of authorized rules; in does not is easily damage of location deployment hardware.

Enabling of WEP Encryption

Enhance wireless network security must be the correct mechanism for using WEP shared key authentication to achieve security objectives and functions; the five regard must be done. First is by in each frame in the joined a check and of practices to guarantee data of integrity, prevent some attack in data flow in the insert known text to tries to crack key flow. Second is must in each client and each AP implementation WEP to work. Third is does not using advance defined of WEP key, avoid using default options. Fourth is the key by user to set, and to often change. Fifth is to using most solid of WEP version, and standard of latest update version keep synchronization.

Wireless Network Access Point's MAC Addresses Filtering

MAC address filtering can reduce a large number of attack threats, large-scale wireless networks are a very viable option. First MAC filtering is as a first layer of protection measures. The second is should record each MAC address used on the wireless network, and configured on the AP, allows only those addresses access to the network, MAC access prevents non-trusted network. Third, it can be used the logging errors and checked on a regular basis, determine whether an attempt to break through the security measures.

Wireless Network Protocol Filtering

Protocol filtering is a way of reducing network security risks. in protocol filters are set correctly on the appropriate protocol filter for wireless networks to provide security guarantee. It is quite an effective method filtering protocol to restrict those who try to access wireless devices through SNMP network users to

modify the configuration; it can also be prevented the use of large denial of service attack.

Shield SSID (Service Set Identifier) Broadcast Information

Although radio frequency communication can easily be captured, from the AP to the outside world by preventing the SSID broadcast, this risk can be overcome this drawback. Closed to traffic throughout the network to avoid invalid connections can occur at any time. Securely distributing configuration information to clients that need wireless network users should be considered.

Rational Allocation of IP Addresses

Assign IP addresses are static and dynamic address in two ways, which determine the wireless networks assign IP methods best suited to their own institutions, essential for network security. Static address can prevent hackers to obtain an IP address automatically, pass restrictions on the network layer access to the device and dynamic addresses simplifies the use of WLAN, it can be used to reduce the heavy administrative work.

Wi-Fi Security at Home

Today's Wi-Fi networking products don't always help the situation as configuring their security features can be time-consuming and non-intuitive. Since people also access to e-government sites from their home computers, there should be measures to ensure security for e-government. The recommendations below summarize the steps one should take to improve the security of one's home wireless network.

Changing Default Passwords and Usernames

At the core of most Wi-Fi home networks is a broadband router or other wireless access point. These devices include an embedded Web server and Web pages that allow owners to enter their network address and account information. These Web tools are protected with login screens that prompt for a username and password so that only authorized people can make administrative changes to the network. However, the default logins provided by router manufacturers are simple and very well-known to hackers on the Internet. Change these settings immediately.

Opening Wireless Network Encryption

All Wi-Fi equipment supports some form of encryption. An 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 including WPA and WPA2. The way these technologies work, all Wi-Fi devices on a network must share matching encryption settings.

Changing the Default SSID

Access points and routers all use a network name called the Service Set Identifier (SSID). Manufacturers normally ship their products with a default SSID. For example, the network name for Linksys devices is normally "linksys." Knowing the SSID does not by itself allow one's neighbors to break into another's network, but it is a start. More importantly, when someone sees a default SSID, they view it is a poorly configured network and one that's inviting attack. Change the default SSID immediately when configuring wireless security on one's network.

Enabling MAC Filtering

Each piece of Wi-Fi gear possesses a unique identifier called the physical address or Media Access Contral (MAC) address. Access points and routers keep track of the MAC addresses of all devices that connect to them. Such products offer the owner an option to key in the MAC addresses of their home equipment, which restricts the network to only allow connections from those devices. Doing this adds another level of protection to home network, but the feature is not so powerful as it may seem. Hackers and their software programs can fake MAC addresses easily.

Disabling Permanent SSID Broadcast

In Wi-Fi networking, the router or access point 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. Inside a home, this broadcast feature is unnecessary, and it increases the likelihood someone will try to log in to one's home network. Fortunately, most Wi-Fi routers allow the SSID broadcast feature to be disabled by the network administrator.

Disabling Auto-Connecting to Open Wi-Fi Networks

Connecting to an open Wi-Fi network such as a free wireless hotspot or someone's neighbor's router exposes PC to security risks. Although not normally enabled, most computers have a setting available allowing these

connections to happen automatically without notifying the user. This setting should not be enabled except in temporary situations.

Strategically Positioning the Router or Access Points

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 spreads, the easier it is for others to detect and exploit. Wi-Fi signals often reach through neighboring homes and into streets. When installing a wireless home network, the location and physical orientation of the access point or router determines its reach. Try to position these devices near the center of the home rather than near windows to minimize leakage.

Deployment of Firewalls and Security Software

Modern network routers contain built-in network firewall, but the option also exists to disable them. Ensure that router's firewall is turned on. For extra protection, consider installing and running additional security software on each device connected to the router. Having too many layers of security applications is overkill. Having an unprotected device (particularly a mobile device) with critical data is even worse.

Assigning Static IP Addresses to Devices

Most home network administrators use Dynamic Host Configuration Protocol (DHCP) to assign IP addresses to their devices. DHCP technology is indeed easy to set up. Unfortunately, its convenience also works to the advantage of network attackers, who can easily obtain valid IP addresses from a network's DHCP pool. Turn off DHCP on the router or access point, set a fixed private IP address range instead, and then configure each connected device with an address within that range.

Stopping the Network during Extended Periods of Non-Use

The ultimate in wireless security measures, shutting down 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.

VIII. CONCLUSION

In this paper, we have tried to explain and analyze the Wi-Fi basics and major Wi-Fi security issues particularly for e-government services. Also we have been examined the standards, technologies, methods and tips to solve the problems for the Wi-Fi security. It is concluded that the wifi security concerns will continue to emerge as mobile devices and mobile apps alongside with m-government solutions tend to increase. There should be a strategic approach to organizational environment, public access points and home users categorically.

E–government system in the wireless and mobile platforms should first of all ensure the confidentiality, availability and integrity of data, information and information resources through information security architecture, training and frameworks to minimize the human error and exploitation in the protection of information at government level. Second - the security system needs to be centralized by urging a certain standard such as Federal Information Processing Standards (FIPS) [23]. (Frankel, Eydt, Owens, & Scarfone, 2007). Third - the security policy, frameworks and security architecture must be built on a single standard to ensure the confidentiality, availability and integrity of information. Fourth –trainings ad certification of security professionals such as Cyber Security Nexus (CSX) [21] (ISACA, 2017) and Certified Wireless Network Professional (CWNP) [22] (Coleman, 2007) are of crucial importance.

Wi-Fi is a universal wireless networking technology that utilizes radio frequencies to transfer data. Wi-Fi allows high-speed Internet connections without the use of cables. It has some advantages: convenience, mobility, productivity, and easy-setup, expandable and low-cost. It allows one to connect to the Internet from just about anywhere that is a coffee shop, a hotel room, or a conference room at work. It is almost 10 times faster than a regular dial-up connection. To access Wi-Fi, it is needed Wi-Fi enabled devices (laptops or PDAs). These devices can send and receive data wirelessly in any location equipped with Wi-Fi access.

As with all things, the Wi-Fi security is challenge and important issue. WIFI network access and data transfer processes are prone to security problems. However, these problems can be handled with the combination of technology and management to building secure Wi-Fi network platform. Hence, the mutual

authentication, the private communication, data integrity and data encryption should be needed to consider when encountered the Wi-Fi security. To balance through these issues and to be safe in Wi-Fi, there are a lot of standards, techs and methods.

.

REFERENCES

[1]. Coleman, D. D. (2007). *CWSP Certified Wireless Security Professional Study Guide: Exam CWSP-205.* USA: Wiley.

[2]. Collins, T. (2017). *'Almost all' home routers are at risk of being HACKED.* Retrieved 02 11, 2018, from dailymail: http://www.dailymail.co.uk/sciencetech/article-4984166/Flaw-WPA2-lets-cyber-criminals-spy-WiFi-network.html

[3]. Dark. (2015). *Cracking MD5, phpBB, MySQL and SHA1 passwords with Hashcat on Kali Linux*. Retrieved 02 20, 2018, from Dark more ops: https://www.darkmoreops.com/2014/08/14/cracking-md5-phpbb-mysql-and-sha1-passwords-with-hashcat/

[4]. Digi. (2008). *An Introduction to Wifi.* Retrieved 02 25, 2018, from Digi international: http://ftp1.digi.com/support/documentation/0190170_b.pdf

[5]. Egov. (2014). *e-government vs. m-government.* Retrieved 02 22, 2018, from egovconcopts: www.egovconcepts.com

[6]. Engst, A., & Fleishman, G. (2004). *"The Wireless Networking Starter Kit.* CA.

[7]. Frankel, S., Eydt, B., Owens, L., & Scarfone, K. (2007). *Establishing Wireless Robust Security Networks.* Retrieved 02 11, 2018, from Nist: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-97.pdf

[8]. Greenberg, A. (2015). Human error cited as leading contributor to breaches, study shows. *scmagazine*, https://www.scmagazine.com/study-find-carelessness-among-top-human-errors-affecting-security/article/535928/.

[9]. Griffith, E. (2016). 12 Ways To Secure Your Wi-Fi Network. *pcmag*, http://www.pcmag.com/article2/0,2817,2409751,00.asp .

[10]. Huang, L., Ye, X.-E., & Shi, X. (2014). The Design and Application of WiFi-Smart Socket in Smart Home. *Advanced Material Research*.

[11]. ISACA. (2017). *Cybersecurity Fundamentals Certificate*. Retrieved 02 10, 2018, from ISACA: https://cybersecurity.isaca.org/csx-certifications/csx-fundamentals-certificate

[12]. James, S. (2017). *The real risk of cyber attack on unsecured networks*. Retrieved 02 10, 2018, from computerweekly: http://www.computerweekly.com/feature/Security-Zone-The-real-risk-of-cyber-attack

[13]. Karthik, K., & kuracha, S. (2015). Security in Wireless Cellular Networks. *International Journal of Application or Innovation in Engineering & Management (IJAIEM)*.

[14]. Micro. (2015). *Elecromagneticspectrum.* Retrieved 02 11, 2018, from microworlds: http://www2.lbl.gov/MicroWorlds/ALSTool/EMSpec/EMSpec2.html

[15]. Mitchell, B. (2017). *Wireless Standards 802.11a, 802.11b/g/n, and 802.11ac.* https://www.lifewire.com/wireless-standards-802-11a-802-11b-g-n-and-802-11ac-816553: Lifewire.

[16]. News. (2017). *'All wifi networks' are vulnerable to hacking, security expert discovers.* Retrieved 02 22, 2018, from The Guardian: https://www.theguardian.com/technology/2017/oct/16/wpa2-wifi-security-vulnerable-hacking-us-government-warns

[17]. NSK. (2014). What is wirelss Network? and how its differs with Wired Network? . *Networking*, http://255net.com/2014/538/.

[18]. Ranjan, S., R.N.Shukla, & Lohia, P. (2014). Information security analysis of Wi-Fi networks. *International Journal of Electronics, Electrical and Computational System*.

[19]. Rowan, T. (2010). Negotiating WiFi security. *Network Security*, 8-12.

[20]. Safer. (2017). *10 Public Wi-Fi Security Threats You Need to Know*. Retrieved 02 22, 2018, from safervpn: https://www.safervpn.com/blog/10-public-wi-fi-security-threats/

[21]. Scarfon, K., & Dicoi, D. (2007). *Wireless Network Security for IEEE 802.11*. Retrieved 01 22, 2018, from Nist: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.109.6200&rep=rep1&type=pdf

[22]. Shaban, H. (2017). *Every modern, protected WiFi network is vulnerable, warns government cybersecurity watchdog.* Retrieved 02 20, 2018, from TheWashington Post: https://www.washingtonpost.com/news/the-switch/wp/2017/10/16/every-modern-protected-wifi-network-is-vulnerable-warns-government-cyber-watchdog/?utm_term=.a2a7d35c21bc

[23]. Stanley, R. A. (2005). *Managing Risk in the Wireless Environment: Security, Audit and Control Issues.* USA: ISACA.

[24]. Wiki. (2017). *Wireless security*. Retrieved 02 11, 2018, from Wikipedia: https://en.wikipedia.org/wiki/Wireless_security

[25]. Zhou, Z., & Hu, C. (2008). Study on the E-government Security Risk Management. *IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.5, May*, 2008-2013.