Turkish Journal of Computer and Mathematics Education Vol.12 No. 12 (2021), 4147-4155
Research Article

Wireless Network Security Threats and Best Method to Warn

Dr. J P Patra[1], Santanu Mukherjee[2]
[1]Professor, Shri Shankaracharya Institute of Professional Management & Technology, Raipur, patra.jyotiprakash@gmail.com
[2]Asst. Professor, Shri Shankaracharya Institute of Professional Management & Technology, Raipur, santanu.mukherjee@ssipmt.com

Article History: Received: 11 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 16 May 2021

***Abstract*:** Wireless Networking technology is now one of the most popular technologies but still, some drawbacks are closely associated with Wireless Networks. In wireless network communication, the data is transferred from one point to another point through radio waves which makes wireless networks weak for attacks. To eliminate threats, understanding said attacks always provides a good ability to defend the wireless network. This research paper will describe the overview of the wireless technology with its drawbacks, Present security and privacy issues, Potential wireless network Security threats (unauthorized access, Active eavesdropping, Man in the Middle Attack, Denial of Service, etc), tools that hackers often use to exploit vulnerabilities in wireless networking (NetStumbler, Kismet, Airsnort, Airsnarf, Airjack, etc) and will propose the best ways to secure Wireless Network.

Keywords: *ML, EDM, ID3, F-SCORE, Regression*

1. Introduction

Home and business users are implementing wireless technology because of its convenience, easy installation, troubleshooting and low price in the market but security is the big concern for this technology because these devices can be attacked by malicious attacks [1]. The Wireless networks must defence against these attacks as illustrated in this paper.

Common wireless network vulnerabilities are as under:

- End users are not security experts and may not be aware of the risks posed by wireless LANs.
- Approximately all access points having default configurations have not activated WEP security.
- Most of the users do not change the access point's default key used by all the vendor's products out of the box.
- The Wireless Access Points which are enabled with WEP can be cracked easily.

To access the internet in the wireless network, the clients are connected with the Access Point and that AP is connected to the wireless router. The function of the wireless router is to broadcast a signal through the air and all the wireless clients within the range can connect to the wireless network. IEEE has developed a wireless network standard that is called 802.11. This standard unfortunately has limited support and still could not provide full security, privacy and confidentially through Wireless Equivalent Privacy (WEP) [2]. The development of 802.11 standards was started in the late 1990s but true development has begun in 2000-2001. 717. This paper will describe security threats to IEEE 802.11 wireless network. The initial problem in 802.11 is that it used a media access control layer mechanism to talk with other networks.

2. Wireless Equivalent Privacy (WEP)

IEEE 802.11 uses Wired Equivalent Privacy (WEP) for security purpose against eavesdropping and other attacks that are used to hack a wireless network but unfortunately, still, there is the number of flaws /loopholes in the protocol [3]. Wireless Equivalent Privacy (WEP) use the RC4 algorithm and is based on data-link layer security technology. The first drawback of the WEP is that it uses a secret user key that is called the base key in the RC4 algorithm. The main goal of the secret key is to encrypt the data over the wireless network and at the same time; Cyclic Redundancy Check (CRC) is used to protect the integrity of the packets. WEP uses four different types of base keys. In 64-bit encryption, only 40 bits are encrypted and the remaining 24 bits are system generated bits. This thing is the big drawback of the RC4 algorithm as it is very easy to crack 40 bits key. Similarly, in 128 bits encryption, 104 bits are used for encryption, not 128 and vice versa [4].

It is pertinent to mention here that both senders and receivers use the same secret key. To generate cipher text in RC4 cipher algorithm, the sender client computer XOR the secret key with plain text and similarly the receiver computer who have already same secret key XOR the cipher text to generate original sent text as depicted below.

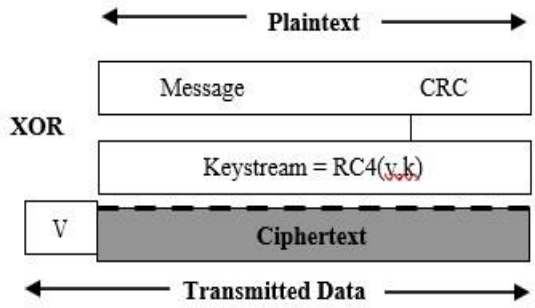

Fig. 1. Preparing the text using the algorithm

The above-stated working of RC4 cipher algorithm clearly shows that it is vulnerable to attack. The function that is used to drive the Keystream is RC4(v,k) as a function of the v and the security key k. The plain text is a raw message supposed it is denoted by M, and after applying checksum c, it can be written as P = (P. c (M)). On the other hand, the receivers, who have the same key, XOR the keystream with cipher text to get initial plain text [5-7]. The method to generate ciphertext shown in Figure No.1 is vulnerable to many attacks.

After seeing many drawbacks, IEEE introduced a new method to generate cipher text in which Integrity Check (IC) field in the packet and 24-bit Initialization Vector (IV) field. In this method, for every packet, a different RC4 key is used for example,

If $C_1 = P_1 \oplus \mathrm{RC4}(v, k)$
and $C_2 = P_2 \oplus \mathrm{RC4}(v, k)$
then

$$C_1 \oplus C_2 = (P_1 \oplus \mathrm{RC4}(v, k)) \oplus (P_2 \oplus \mathrm{RC4}(v, k)) = P_1 \oplus P_2.$$

The above technique generates overhead on the computation while the security is still poor.WEP2, a stopgap enhancement to WEP, uses 128-bit encryption and IV to generate ciphertext. The value of IV is large in WEP2 and this is a drawback of the WEP2 algorithm. WEP plus is also known as WEP+, it provided better security by avoiding Week IV drawbacks. To obtain complete effectiveness of WEP+, it is necessary to use it at both ends of wireless connections, Moreover, it is vender specific. It is quite possible that strong threats like replay attacks can break it. Wi-Fi Protected Access (WPA) was launched to remove security drawbacks in WEP. A new technique was adopted in this algorithm which is called Temporal Key Integrity Protocol (TKIP) which is used to rectify authentication and encryption loopholes in WEP [8,9]. It uses, Per packet key mixing function, Message Integrity Check (MIC), Initialization Vector with sequencing rules and Re-keying mechanism. WPA introduced one variation which is known as WPA Pre Shared Key, WPA (PSK). It provides strong encryption and encapsulation for authentication. If we combine both TKIP and WPA (PSK), then, the hacker will feel great trouble finding the secret key.

Wi-Fi Protected Access 2 (WPA2) provides authentication, confidentiality and integrity to the wireless network. For better protection, it is based on Layer-2 of the OSI model. It uses Counter-Mode with Cipher Block Chaining-MAC Protocol (CCMP). The CCMP uses Advanced Encryption Standard (AES) encryption algorithm rather a weak RC4 encryption algorithm. For better protection against threats, it is necessary to use WPA2 for encryption and authentication.

3. Wireless Network Threats

As mentioned above, wireless technology uses air as a medium to communicate with each other. This medium made the wireless network susceptible to threats by attackers.

There are two types of attacks in wireless security:

- Active Attacks
- Passive Attacks

In Active Attacks, the attackers change the contents of the information and generate fake information in the network to destroy network security like Unauthorized Access, Active Eavesdropping, Man in the Middle Attack (MITM), Session Hijacking, Denial of Service (DoS), Replay, while in Passive Attacks, the attacker just listen to the traffic of the network, obtain information from the packets without changing it like passive Eavesdropping and Traffic Analysis. These types of attacks are very hard to detect.

3.1 Unauthorized Access

In Unauthorized Access, the user gains access to the network and can obtain data and use the bandwidth of the network easily. The attacker can violate the confidentially and integrity of the network traffic by listening to packets, changing them as per requirements, send and receive the messages.

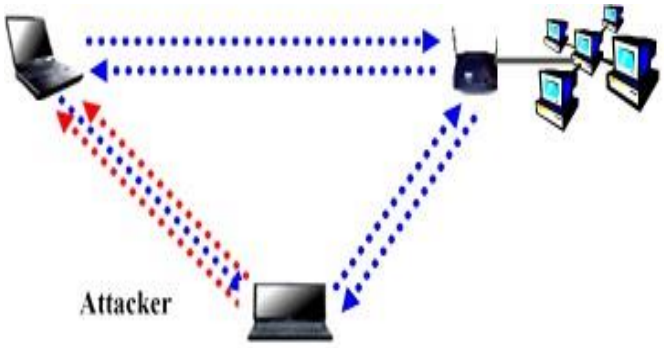

Fig. 2. The path uses for the attacker to gain network access [10]

3.2 Denial of Service (DOS)

Denial of Service (DoS) is a very famous attack to break down the wireless as well as a wired network. To break down the network, it sends huge traffic on the Access Point make it unable to respond [11]. In a Wireless network, the DoS attack is just carried out by using a powerful enough transceiver, interference in the shape of the noise is generated to jam to the network. Denial of Service (Dos) attack uses forged Disassociation technique to break network security. The attacker floods a large number of disassociation frames to the client computer to break its connection with the access point. After the break-up of connection, the client computer again attempts to establish its connection with the access point. It is pertinent to mention that the client computer is already authenticated and only need association. To prevent re-association, the attacker continues to send Disassociation frames up to desired period.

Similarly, the attacker can use the forged Deauthentication technique to break up network security. The attacker flood the Deauthentication frames to the client computer and resulted in, client computer unauthenticated with an access point and will try to again authenticate itself with the access point. To prevent again authentication, the attacker continues to send Deauthentication frames up to desired period. Several tools are available over the internet like LANJack, Hunter_killer that can be used to launch a DoS attack. IEEE 802.11 wireless network standard by using the Medium Access Control (MAC) address, does not authenticate the source IP address, resultant, the attacker spoof the MAC address and hijack the session. Furthermore, the Access Point does not prove itself as a genuine Access Point.

3.3 Active Eavesdropping

The core threat of the wireless network is eavesdropping in which data in the shape of signals is transferred from client workstation to access point. In Active Eavesdropping, the attacker injects its data into the network signals to crack the secret key as shown in Figure No.3. The goal of this attack is to determine the contents of the message. The attacker can partially access the part of plaintexts like source IP address, destination IP address etc or contents of all traffic.

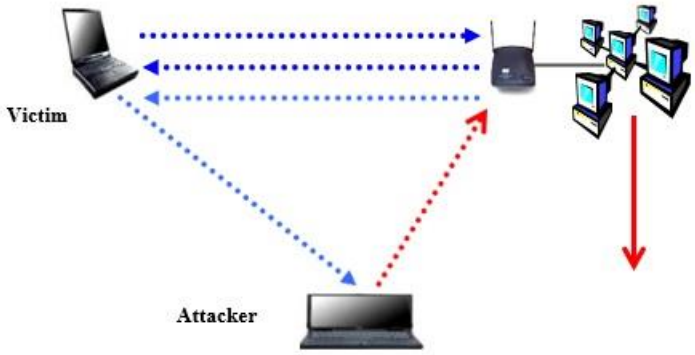

Fig.3.Active Evasdropping

In Figure No. 3, the attacker takes advantages of WEP drawbacks wherein WEP, the CRC is used to only check the integrity of the data not all the other contents of the packet like destination and source IP address. Hence, the attacker's changes in these parameters cannot be detected.IP Spoofing is an example of Active Eavesdropping in which the attackers change the destination IP address of the host that he controls.

3.4 Man in the Middle

The Man in the Middle is a very dangerous attack wherein the attacker eavesdropping the communication and modifies it before sending it. Although, the organization implemented VPN, SSH, IPSec security measures but these measures are breakable through MITM attack as these measures can only protect data confidentiality attack. The attacker connects himself to the Access Point as a user and to a user as an authentic Access point as shown in Figure No. 4. In this way, all the user data passed to the Access Point through the attacker and the attacker not only sniffs the data but also can change the data, insert viruses in downloading files, change web pages setting easily. IP Spoofing and Masquerading are the techniques that are used to make user fool. Moreover, encryption does not play a security role between Access Point and client user.

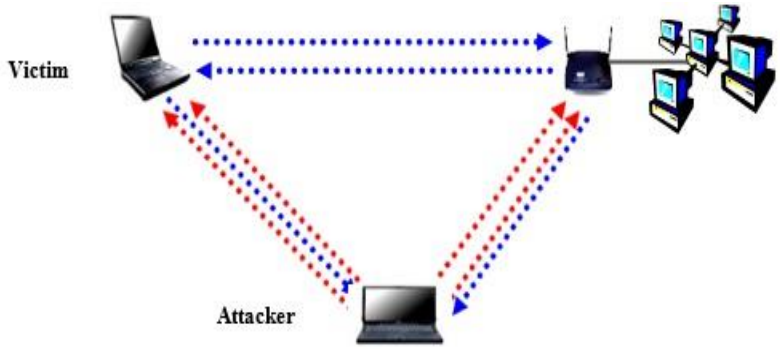

Fig.4. The attacker connects himself to the Access Point as a user

Address Resolution Protocol (ARP) poison is a technique that is used in Man in the Middle Attack. ARP enables the user to find the users MAC address. When the network receives a packet, whose destination IP address is missing or unknown, it caches the packet by sending this packet on a network and asks every client about it, if any machine match with it, then the machine reply with ARP Reply packet and in this packet MAC address is available. Once the cache has been updated, the attacker can act as MITM as shown in Figure No. 5.

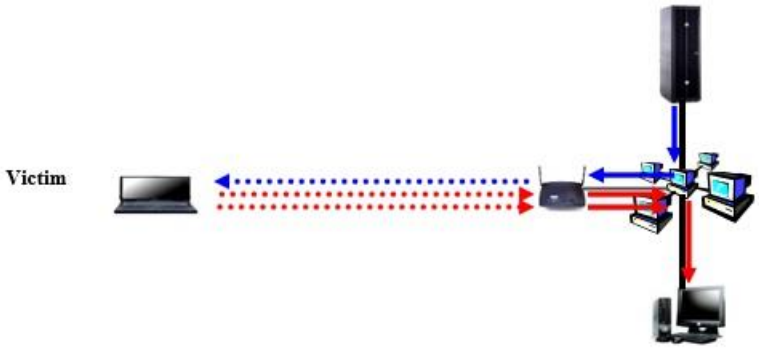

Fig.5.MITM

3.5 Session Hijacking

Session Hijacking indirectly resembles to the Man in the Middle Attack (MITM) wherein the attacker captures the session of the victim client. The victim just supposes that his/her session was expired due to whatever reasons while his/her session was handed over to the attacker and he/she can exploit it as per his

desire. In Session Hijacking, the attacker first obtains the MAC address of the victim and AP then it sends MAC Disassociation message to the victim. The victim closes its session from the network while his /her session in real opens in AP.

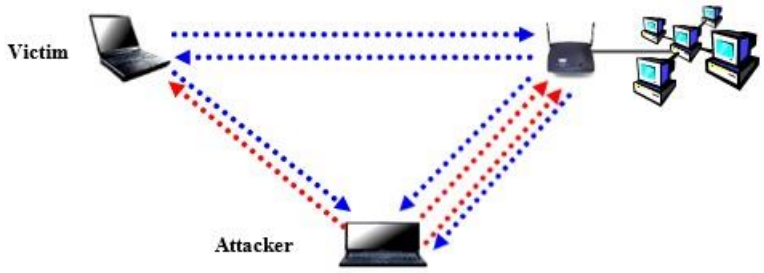

Fig.6.Gaining the victim's MAC address

The attackers, by using the victim MAC address, get control of the session. After getting control, the attacker uses the said session for whatever purpose they desire. Session hijacking attack occurs in true but can continue up to extended time.

3.6 Replay

The replay attack also resembles to the Man in the Middle Attack with a little bit of variation. In Replay attack is not a real-time attack as MITM attack, it grabs all the information (data and session) of the network and later on offline use the same to exploit the victim's information.

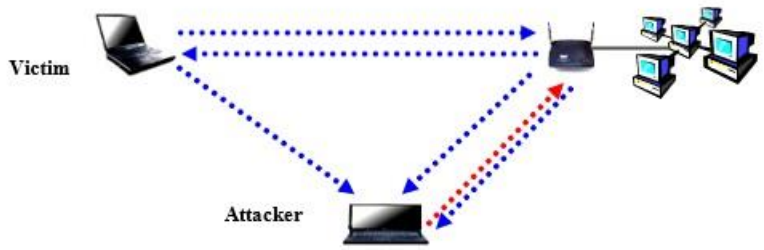

Fig.7. Authorizations of the target without the secret key

The goal of attack is to access the network with the authorizations of the target without secret key as shown in Figure No.7. Moreover, the attacker may use resources of the network by using target client authorization and permission. This attack is real and often used to exploit the security of the wireless network.

3.7 Traffic Analysis

The Traffic Analysis is very simple and easy technique in which the attacker just notes the number and size of the packets transmitted over the air, protocols used by the network and active access point as shown in Figure No. 8

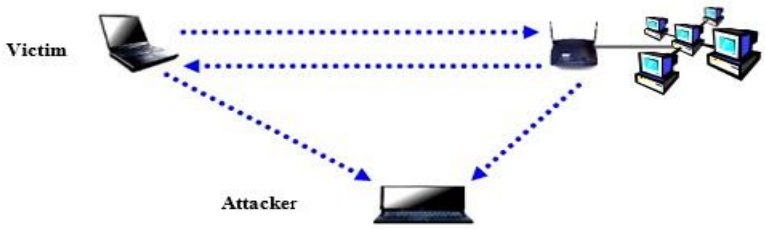

Fig.8.The attacker using the active access point

If packets are encrypted, then the attacker can get partial or full information from the packet of the message. The attacker, before starting an active attack should get preliminary information about the network properties. Wardriving is a freeware tool that is available over the internet is a very useful tool for traffic analysis. To find out the target Access Point, the attacker moves from one place to another to find out active

access points of the network. Every Access Point (AP) broadcast its Service Set Identifier (SSID) over the air to recognize itself to the wireless notes desired to connect to the network. Through this broadcasting information, access points allow everyone in its domain to identify them.

3.8 Passive Eavesdropping

This attack much resembles to traffic analysis attack. In this attack, the attacker gets the size of the packet, protocol used in wirelesses network, number of packets transmitted over air, and various characteristics of the packet as shown in Figure No. 9 [11,12].

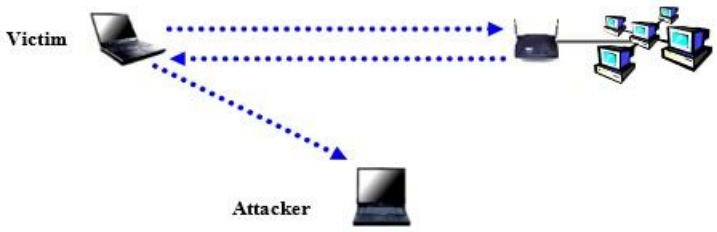

Fig.9.Passive Eavesdropping

In Passive eavesdropping attacks, the attacker exploits the victim's privacy and information. In case of the packet is encrypted then the attacker has to break its encryption to get plaintext or desired information from the packet.WEP has various vulnerabilities because it has small numbers of initialization vectors (IV) sequences and this thing made it susceptible to attack. Rapidly reusing the same IV and made the stream less vulnerable but can be cracked. WPA2 use AES and 3DES strong encryption algorithms to ciphertext and in presence of these algorithms, passive eavesdropping is very hard. It can only be possible if the packets are not encrypted.

4. The Hacker's Toolbox

To hack Wireless Network, several freeware tools are available on the internet. For better security in Wireless Network, the users must understand their methodologies and accordingly take security measures to protect their respective networks. The table given below enlists some most commonly used freeware hacker's tools with their description:

Table 1. Description of Free Wireless Hacking Tools

TOOL	DESCRIPTION
NetStumbler	NetStumbler is an active network scanner as well as a freeware Wireless Access Point identifier that shows AP's SSID, MAC address, type of encryption algorithm, Channels, noise, and signal strength. It is also used for fine-tuning a wireless link
Kismet	Kismet is a very advanced level freeware wireless network diagnostic tool. It is used for passive eavesdropping attack. Kismet is used to monitor traffic, store data, sort data to identify SSID, channels, connection speed, MAC address, signal to noise ratio (SNR), graphically mapping of the network by using GPS and range of IP addresses used in the network. If a hacker has multiple wireless networks cards, then it spits out load to all of them to expedite the work
AirSnort	AirSnort is a widely used freeware tool that is used to break the encryption of WEP. It is also used for passive monitoring of the wireless network as NetStumbler. After getting sufficient packets, it starts computing encryption to break the security
Ethereal	It is freeware WLAN analyzer software that is used for passive eavesdropping. The interesting feature of said tool is its summary and detailed summary for observed traffic.
WEPcrack	This tools name depicts its function WEPcrack is the wireless network cracking tool that used to exploit the vulnerabilities in RC4 algorithm by using the latest discovered drawbacks in 802.11.
THU-RUT	Freeware WLAN discovery tool. It used *brute force* attack to obtain low traffic access points. *"Your first knife on a foreign network."*
WEPWedgie	It is used for active eavesdropping attack as it used to determine WEP Keystreams and inject with known Keystreams. It has a ping scanning and port scanning facility via injection channels.

AirSnarf	It is an AP spoofing tool that is used to deceive users by forwarding their important/sensitive information to an attacker. To victimize the user, AirSnarf imitates legitimate AP and to create the same login page that normally be displayed by the access point. When the user logins, its login, information will be sent to the attacker and he/she will use it as per his/her desire. This is a very simple but effective tool for wireless network hacking.
Airjack	Air jack is a very dangerous tool for the wireless network. It is used for Denial of Service (DoS) and Man in the Middle (MITM) attacks as it begins with sending disassociate or de-authenticates frames at very high speed to access point and accordingly AP drops connections with its all connected users.
Cain&Abel	Password recovery tool that is used to recover passwords by cracking encryption. It uses Dictionary attack, Brute-Force, and Cryptanalysis attacks. It is also a very effective and easy to operate freeware tool to hack wireless network within few minutes.
Host AP	It is the firmware for Prism cards to act as AP the host has multiple scanning, broadcasting and managements options that is used to connect disconnected clients with the HostAP and after that, the attacker can grab all the information as per his/her requirements.
Hotspotter	Passively monitor all the activities of the wireless network.
AS LEAP	It is a toolkit used to recover LEAP networks passwords. It is also used to de-authenticate users from the network and force them to connect with rogue AP.
WEP Attack	WEP Attack tool is used for Brute-Force. WEP cracking by using Dictionary attacks against WEP keys.
IKEcrack	Powerful tools to crack authentication by using Brute-Force Dictionary attack. A very helpful tool to crack IKE authentication.
AiroPeek	Packet Analyzer especially IEEE 802.11b. It is used for evaluating network performance, signal strength, number of channels, and speed/data rate.

5. Countermeasures

Although there are various flaws in the WEP algorithm still users can secure their respective wireless networks. To deal with the above-mentioned security threats, the following techniques are recommended to minimize the security risks involved in the wireless network.

5.1 Training and Educating Users

The first step in wireless network security is to educate the users about how to secure the network. It is often observed that end-users do not know how to implement security and leaves various loopholes for attackers. If users will well aware of wireless tools configurations/settings and how to secure their respective network, then it is quite possible to reduce security risks.

5.2 Wireless Network Auditing

It is a powerful technique to secure a wireless network. The user should scan his/her network through a network scanner to know about the activities of the network. Several free network scanning software like NetStumbler and Kismet is available over the internet.

5.3 Turn Off AP When You Would Not Use It

If the user turns off his/her wireless network router/access point, when he/she is not using it then we can limit the time that it is susceptible to hack

5.4 Change Router's Pre-Set Password

Every manufacture of the wireless router/access point set the default user name and password. If the user does not change it, then it is a very sweet cake for the attacker as the attacker simply scans the access point and accesses it through its default username and password. Therefore, it is strongly recommended that in the first instance, the user should change by default username and password.

5.5 Change SSID

Every access point has by default ID and the attacker can easily find an access point by entering the default ID. All the devices that connect to the wireless network use the same SSID. If the user does not change the default SSID, then it is like to leave the default password. Moreover, it is also best practice to change SSID within 30 days or before.

5.6 Turn Off SSID Broadcasting

Access Point uses the SSID broadcasting technique to show its presence in the environment in which it is

working. By turning off the SSID broadcasting function, it is very hard for the attacker to scan the network. Therefore, it is recommended to turn off this function if the router allows this.

5.7 Utilize Virtual Private Network

In securing a wireless network, it is the very best security technique to put behind wireless access point to Virtual Private Network (VPN). A Virtual Private Network is a very good solution to authenticate unauthorized users who try to connect themselves to the network and encrypt their respective communication. If an organization has more than one access points, then it is strongly recommended that connect all of them with one common switch and connect this switch to a VPN server.

5.8 Location of Access Point

During designing of wireless network, it is suggested to always place an access point in the middle of the network place to avoid unnecessary signal broadcasting outside the network place. For better security, the signal strength and power level should set as per the boundary of the network.

5.9 Use of Antivirus, Firewall and Anti Spyware

To exploit the security, viruses and Malwares play their roles accordingly. For better security, it is recommended that the client must install an updated firewall, antivirus, anti-malware and Anti Spyware software on his computers.

5.10 Encryption

The best way to secure wireless network from unauthorized users/attackers is to use encryption for ciphertext. WEP algorithm has various vulnerabilities and it is not recommended to use it for encryption purpose. IEEE 802.11i use Advance Encryption Standard (AES) and Triple Data Encryption Standard (3DES).

5.11 SSH

Most users use telnet utility for remote connection which is insecure in the wireless network, the users should use SSH with tunnelling feature to provide secure remote connection.

5.12 Third-Party Wireless Security Tools

Various third-party security tools are available over the internet to provide better security for wireless networks. Some of them are given below:

5.12.1 Nextcomm, Inc

It uses the MD5 hash algorithm to generate Keystream. Netxcomm provides this facility through an IC chip which should be part of the access point and wireless card. MD5 has rapidly changed Keystream which is also known as Key hopping to prevent attackers to get enough analysis information.

5.12.2 Interlink Networks

It provides wireless security through RADIUS for secure authentication.

5.12.3 Air defence

It is a very powerful and famous wireless security tool that provides intrusion protection, show vulnerabilities, prevent the network from attackers and also provides assistance to users, improve their security and performance.

5.13 Enable MAC Filtering

MAC filtering is a very famous and best technique to only authenticate clients who are part of the network.

5.14 Upgradation of Access Point Firmware

The older Access Points (APs) cannot support the latest security algorithms. The client should update its Access Point (AP) firmware software to WPA2.

5.15 Turn Off DHCP Server

The attacker while connecting attacking the required IP address of the network. If the DHCP server will enable then it is a sweet cake for the attacker. Therefore, for better security measures, it is suggested to assign a static IP address to every client computer and turn off the DHCP server on Access Point.

6. Conclusion

Wireless technology is very famous all over the world due to its low cost and easy to install characteristics, although it has numerous security flaws still it captures the market. This paper discusses brief taxonomy about the Wireless Equivalent Privacy (WEP) vulnerabilities, wireless security threats and attacks, hacking tools which are freeware and available on the internet to hack the wireless network and also describes various. countermeasures techniques to secure wireless network. By understanding these attacks techniques with freeware tools and their countermeasures make a user understand the said risks and how to mitigate them. We have indicated several existing freeware hacking tools that implement attack techniques to exploit the weaknesses in the protocol designs. Moreover, we have pointed out several best practices that can mitigate the insecurities.

References

1. Welch, D. and Lathrop, S. (2003). Wireless Security Threat Taxonomy. IEEE Workshop on information assurance, 76-83.
2. Arbaugh, W., Shankar, N. and Wan, Y.C.J. (2002). Your 802.11 wireless network has no cloths. Wireless Communications, IEEE, 9, 44-51.
3. Bittau, A., Handley, M. and Lackey, J. (2006). The final nail in WEP's coffin. Security and Privacy, 2006 IEEE Symposium.
4. Hassan, H.R. and Challal, Y. (2005). Enhanced WEP: An efficient solution to WEP threats, Wireless and Optical Communications Networks, 2005. WOCN 2005. Second IFIP International Conference, 594-599.
5. Fluhrer, S., Mantin, I. and Shamir, A. (2001). Weaknesses in the Key Scheduling Algorithm of RC4. Lecture Notes in Computer Science, 2259/2001, 1-24.
6. Choi, M.K., Robles, R.J., Hong, C. and Kim, T. (2005). Wireless Network Security: Vulnerabilities, Threats and Countermeasures. International Journal of Multimedia and Ubiquitous Engineering, 3, 77-86.
7. Berghel, H. and Uecker, J. (2004). Wireless Infidelity II: Airjacking. Communications of the ACM, 47,15-20
8. Malekzadeh, M., Azim, A., Ghani, A., and Subramaniam, S. (2010). Design of Cyberwar Laboratory Exercises to Implement Common Security Attacks against IEEE 802.11 Wireless Networks. Journal of Computer Systems, Networks, and Communications, 2010.
9. He, C. and Mitchell, J.C. (2005). Security Analysis and Improvements for IEEE 802.11i. The 12th Annual Network and Distributed System Security Symposium (NDSS'05), 90-110.
10. Khakurel, S., Tiwary, P.K., Maskey, N., Sachdeva, G. (2010). Security vulnerabilities in IEEE 802.11 and adaptive encryption for better performance. Industrial Electronics & Applications (ISIEA), 2010 IEEE Symposium, 207-210.
11. Yuan, X., Archer, R.L., Xu, J. and Yu, H. (2008). A Visualization Tool for Wireless Network Attacks. Journal of Education, Informatics and Cybernetics, 1.
12. Beaton, A.E. and Tukey, J.W. (1974). The fitting of power series, meaning polynomials, illustrated on band-spectroscopic data. Technometrics, 16, 147-186.