RESEARCH ARTICLE OPEN ACCESS

How Wireless Security Can Be Compromised

Shripal Rawal
Undergraduate 3rd year
Department of Computer Science and Engineering,
DRIEMS, Mumbai University, Mumbai
Maharashtra - India

ABSTRACT
Wireless Security is preventing the Networks from unauthorised access or hijacking of the wireless networks. Even a small flaw in Wireless security may lead to entire Network compromising or even worse. Usually Attackers search for public wireless networks which can be compromised easily and access can be gained over the network. By using certain Protocols and Standard Encryption techniques it is possible for wireless network to be secure to a certain limit. Although applying these protocols may result in better security but it cannot be concluded that the system are fully secured only by using these protocols. There are others aspects which may come handy while securing any wireless network.

Keywords: - *Hijacking*, Security, Compromise, Unauthorised, Flaw, Attacker, Protocols, Encryption, Aspects.

I. INTRODUCTION

Wireless security is the prevention of unauthorized access or damage to computers using wireless networks. The main goal behind securing Wireless Networks is to avoid any type of malicious threat that can completely compromise our entire network as well as the local systems. It has become more important to secure our wireless networks in a world where cybercrimes have increased to a greater extent. According to a survey conducted in 2015 it was discovered that over the past few years cybercrimes has increased tremendously threatening the Entire World. Most of the cybercrimes are conducted due to lack of knowledge which tends most of the individuals to make a security flaw which if noticed by Attacker, may result in unauthorised access of the network.

Wireless Networks can be secured using certain protocols and Encryption standards. Using the correct and secured protocols is must because, Ultimately, It's your network, it's your data, and if someone hijacks your network for their illegal hijinks, it'll be the police knocking on your door. Since the late 1990s, Wi-Fi security algorithms have undergone multiple upgrades with outright depreciation of older algorithms and significant revision to newer algorithms. A stroll through the history of Wi-Fi security serves to highlight both what's out there right now and why you should avoid older standards.

Different Protocols and encryption standards that are used in wireless security are listed below.

A. Wired Equivalent Privacy (WEP).
B. Wi-Fi Protected Access (WPA).
C. Wi-Fi Protected Access II (WPA2).

A. Wired Equivalent Privacy (WEP) :-

WEP is an old IEEE 802.11 standard from 1999, which was out-dated in 2003 by WPA, or Wi-Fi Protected Access. WEP is a notoriously weak security standard. The password it uses can often be cracked in a few minutes with a basic laptop computer and widely available software tools. Wired Equivalent Privacy (WEP) is the most widely used Wi-Fi security algorithm in the world.

WEP was first used as in September 1999. The first versions of WEP weren't strong enough and could be breached easily with freely available software over the internet. Initially WEP was only a 64-bit encryption but it wasn't sufficient to secure the network using such encryption standards, so it was upgraded to 128-bit and 256-bit standard encryption. Despite of 256-bit WEP encryption, 128-bit remains most common implementations.

Even after using advanced algorithms for WEP encryption there were numerous security flaws that were continuously reported and as computing power increased it was easier for malicious attacker to exploit these security flaws. As early as 2001 most security flaws were floating around the globe and in 2005 FBI demonstrated these flaws in order to increase public awareness of the WEP encryption where they cracked WEP passwords using freely available software. Despite various improvements in WEP Encryption technique it was still vulnerable to attackers. In 2004 WEP system was finally discarded and replaced by an advanced and more reliable algorithm i.e (WPA) Wi-Fi Protected Access.

B. **Wi-Fi Protected Access (WPA) :-**

Wi-Fi Protected Access is the result of the failure of the WEP system. The vulnerabilities that were reported regarding the WEP system encryption techniques are fully overcome in this advanced algorithm. WPA is an IEEE 802.11i standard which was originally introduced in the year 2003 i.e a year prior to when the WEP system was officially discarded. The most common WPA configuration used is WPA-PSK (Pre-Shared Key). The keys used by WPA-PSK are 256-bit encryption keys which are more efficient and secure as compared to 64-bit and 128-bit WEP encryption.

WPA enterprises uses an authentication server to generate keys or certificates. Most WPA implementation uses a pre-shared key (i.e WPA-PSK) which is commonly termed as WPA personal, and the temporal key integrity protocol (TKIP) for encryption. Some of the significant changes that were made in the advanced WPA algorithm included message integrity check which includes the verification of the packets passed between the access point and the client.

TKIP sends a per packet key system that was ultimately more secure than the fixed keys used in WEP system.

Despite a significant improvement in the WPA algorithm it was still vulnerable. TKIP, a core component of WPA, was designed to be easily rolled out via firmware upgrades onto existing WEP-enabled devices. As such it had to recycle certain elements used in the WEP system which, ultimately, were also exploited. Like WEP, WPA has been shown via both proof-of –concept (POC) and applied public demonstrations to be vulnerable to intrusion. More interestingly the process using which the WPA is breached is not a direct attack on the WPA algorithm but by attack on the supplementary system that was rolled out with WPA.

C. **Wi-Fi Protected Access II (WPA2):-**

WPA2 is an IEEE 802.11i standard which was finalized in the year 2004. The most significant advancement or enhancement in the WPA2 over WPA was the use of Advanced Encryption Standard (AES) for encryption. The security provided by Advanced Encryption Standard (AES) technique is more secure than any other wireless protocols and standards.

Another significant change that was made in WPA2 was introduction of CCMP (Counter Cipher Mode with Block Chaining Message Authentication Code Protocol) as a replacement for TKIP. Currently the primary security concerns of security of the algorithm are obscure. And the security issue of WPA2 vulnerabilities are limited to the enterprise level networks and little to no practical consideration in home networks.

Despite of being secure it has a vulnerability that can be exploited through the attack vector in the Wi-Fi Protected Setup (WPS), although breaking into WPA/WPA2 networks using this vulnerability may require approx. 2 to 14 hrs of continuous effort with a modern computer having a good hardware which can withstand the resources required for such breaking. It is still a vulnerable aspect and WPS should be disabled for better security.

II. MODES OF UNAUTHORIZED ACCESS

The different ways using which a malicious attacker can gain complete control over entire wireless network are categorized under the Modes of unauthorized Access. A smart attacker will always find a way to hijack a network but the most common ways using which networks are hijacked are listed below.

1. Accidental association.
2. Malicious association.
3. Ad hoc networks.
4. Non-traditional networks.
5. Identity theft (MAC spoofing).
6. Man-in-the-middle attacks.
7. Denial of service.
8. Network injection.

1. **Accidental association:-**
   Accidental association the case of wireless vulnerability known as "mis-association". Violation of the security area network can be intended in many ways. On of this method is termed as Accidental association. When a user starts a computer and it latches to a wireless access point from a neighbouring company's overlapping network, the user may be unaware of this event but still this is considered as security breach.

2. **Malicious association:-**
   Malicious associations are when a wireless device can be actively made by attackers to connect to a company's network through their laptop instead of the company's access point. These types of laptops are known as "soft-Aps" and are created by running some software which makes it look like a genuine access point. Once the attacker has gained access he/she can get all the data, passwords and even launch attacks from the compromised systems.

3. **Ad hoc networks:-**
   Ad-hoc networks are usually defined as peer to peer network i.e networks between wireless computers that do not have an access point in between them. In this types of networks encryption methods can be used to provide some security. The security flaw provided by the Ad-hoc networking is not the Ad-hoc network itself but the bridge it provides into the other networks. Thus the user may not even know about the insecure networks in operation on their computer.

4. **Non-traditional networks:-**
   Non-traditional network includes any point to point communication example Bluetooth devices. Personal networks such as Bluetooth devices are not safe from hacking and should be regarded as security risk. Even barcode readers and wireless printer should be secured. These non-traditional networks can be easily overlooked by IT personnel who have narrowly focus on laptops, office systems and access points.

5. **Identity theft (MAC spoofing):-**
   Identity theft occurs when the attacker is able to listen the packets on the network able to identify the MAC address of the computer wit network privileges. Most systems allows MAC filtering which allows only authorised user to gain access over the system. However there are software for network "sniffing" which allows the hacker to get into the network.

6. **Man-in-the-middle attacks:-**
   Man-in-the-middle attack is also called as "session hijacking". In this attack the attacker or hacker slows down the traffic and can monitor the entire system or even modify any request to the network. . Man-in-the-middle attacks are enhanced by software such as LANjack and AirJack which automate multiple steps of the process, meaning what once required some skill can now be done by script kiddies.

7. **Denial of service:-**
   A Denial of service attack (DOS) occurs when the victim is bombarded with bogus request, basically in Denial of service attack the attacker tries to congest the host by sending continuous data packets of huge size. The usual reason for performing a DOS attack is to observe the recovery of the wireless network, during which all of the initial handshake codes are re-transmitted by all devices, providing an opportunity for the malicious attacker to record these codes and use various cracking tools to analyse security weaknesses and exploit them to gain unauthorized access to the system. DDOS attack (Distributed Denial of Service) is an extension of DOS attack

8. **Network injection:-**
   In a network injection attack, a hacker can make use of access points that are exposed to non-filtered network traffic, specifically broadcasting network traffic such as "Spanning Tree", OSPF (Open Shortest Path First), RIP (Routing Information Protocol), and HSRP (Hot Standby Router Protocol). The hacker injects bogus networking re-configuration commands that affect routers, switches, and intelligent hubs. A whole network can be brought down in this manner and require rebooting or even

reprogramming of all intelligent networking devices.

III. WIRELESS INTRUSION PREVENTION CONCEPTS

Securing a wireless network can be very challenging job for common individual without any specialized skills or prior knowledge about the network. But here are some preventive measures depending on the type of networks, which can be taken by individuals to secure their wireless network.

1. For closed networks the most common way is to restrict the access points, which includes encryption and check on MAC address. Closed network includes home users and organisations. Another option for closed network is to disable ESSID broadcasting, making the access point difficult to detect for outsiders. Wireless intrusion systems can be used to provide wireless LAN security.
2. For commercial providers, hotspots, and large organizations, the preferred solution is often to have an open and unencrypted, but completely isolated wireless network. The users will at first have no access to the Internet nor to any local network resources. Commercial providers usually forward all web traffic to a captive portal which provides for payment and/or authorization. Another solution is to require the users to connect securely to a privileged network using VPN.
3. Wireless networks are less secure than wired ones; in many offices intruders can easily visit and hook up their own computer to the wired network without problems, gaining access to the network, and it is also often possible for remote intruders to gain access to the network through backdoors like Back Orifice. One general solution may be end-to-end encryption, with independent authentication on all resources that shouldn't be available to the public.

IV. CONCLUSION

It can be concluded that the various protocols and standard encryption techniques used in wireless security are not stand-alone solution to the increasing cybercrimes. Despite of using such an advanced algorithm for encryption there is always a possibility of the network being unsecured. With the modern computers attackers have all the possible tools that may breach wireless network hence compromising data. So the effective measure from an individual perspective is given explicitly to prevent such network breach in future. Every individual on the network must be fully aware of security standards used in wireless systems to make the network more secure.

REFERENCE

[1]. *Kevin Beaver, Peter T. Davis, Devin K. Akin.- "Hacking Wireless Networks For Dummies".*

[2]. "Wireless Security: It's Like Securing Your Home" https://www.intermec.com/public-files/white-papers/en/WirelessSecurity_wp_web.pdf .

[3]. *Bradely Mitchell. "What is Ad-Hoc Mode in Wireless Networking?" about tech.* http://compnetworking.about.com/cs/wirelessfaqs/f/adhocwireless.htm.

[4]. *"Wi-Fi Protected Access – WPA ". Wi-Fi Alliance* https://web.archive.org/web/20070521092851/http://www.wifialliance.org/knowledge_center_overview.php?docid=4486.

[5]. *"Top reasons why corporate WiFi clients connect to unauthorized networks". InfoSecurity* http://www.infosecurity-magazine.com/opinions/comment-top-reasons-why-corporate-wi-fi-clients/.

[6]. *"What is a WEP key?"- lirent.net.* http://lirent.net/wifi/what-is-a-wep-key.html.