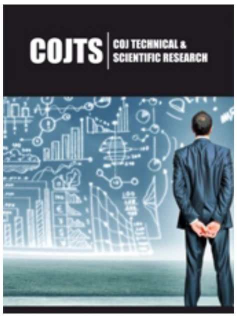
Crimson Publishers
Wings to the Research

Review Article

Security Attacks, Limitation in Wireless Networks and their Solutions

Anam Nigar*

School of Electronics and Information Engineering, Changchun University of Science and Technology, China



***Corresponding author:** Anam Nigar, School of Electronics and Information Engineering, Changchun University of Science and Technology, Changchun 130022, China

Submission: March 23, 2023

Published: May 22, 2023

Volume 4 - Issue 3

How to cite this article: Anam Nigar*. Security Attacks, Limitation in Wireless Networks and their Solutions. COJ Tech Sci Res. 4(3). COJTS. 000587. 2023.

Abstract

The aim of this paper is to review some wireless security issues such as attacks, threats, and vulnerabilities as well as some solutions for dealing with them. Wireless security can prevent unauthorized access to a Wi-Fi network. To keep their staff connected to the internet at all times, businesses today rely significantly on Wi-Fi or wireless networking. On the other side, Wi-Fi is incredibly vulnerable to intrusion by cybercriminals. If you want high-level wireless security, you willl need to implement these steps. Despite 20 years of research, there is still no clear answer on the best technique to prevent wireless networks from security issues.

Keywords: Wireless network; Network security issues; Hacker attacks; security protocols

Introduction

Wireless security is the prevention of unauthorized users from accessing your wireless network and stealing the data using your Wi-Fi network. To be precise, wireless security ensures protection to a Wi-Fi network from unauthorized access. The term can also mean protecting the wireless network itself from intruders trying to compromise the confidentiality, integrity, or availability of the network. The most common types are WIFI security, which includes Wired Equivalent Privacy (WEP) and WIFI Protected Access (WPA) [1]. WEP is an older IEEE 802.11 standard adopted in 1997. This is a notoriously weak security standard. The passwords used by this standard can be cracked in minutes using a simple laptop computer and popular software tool. WEP was replaced by WPA or WIFI Protected Access in 2003. WPA was a faster alternative to WEP to improve security [2]. The current standard is WPA2. Some hardware may not support WPA2 without updating or replacing the firmware. WPA2 uses an encryption engine that encrypts the network with a 256-bit key. Longer key lengths provide better security than WEP. Enterprises often provide security using certificate-based systems to authenticate connected devices according to the 802.11X standard. At all times, the internet is there in our life. We use cellphones, tablets, laptops, gaming systems, and even automobiles to achieve this task. We'll focus on Wi-Fi security because there are many ways to communicate wirelessly. Wireless networks are used by both businesses and individuals on a regular basis. Many laptop computers come with pre-installed wireless cards. A major benefit of being mobile is being able to access the internet at any time [3]. In contrast, there are several security risks with wireless networking. Because of how easy it has become for hackers in the last few year's wireless networks, they've been using wireless technology to break into wire networks as well. Effective wireless security policies are essential for preventing unauthorized access to important resources. Wireless Intrusion Prevention Systems (WIPS) are commonly used to enforce wireless security policies.

These attacks are categorized as follows: an assault against [4].

a) Unauthorized data access

b) Unauthorized network access

c) Unauthorized service integrity are the three key dangers to privacy and security.

Modern cryptographic approaches, such as RSA and AES encryption, can prevent eavesdropping, packet replay attacks, and packet modification or spoofing. Denial-of-Service (DoS) attacks are the most common term for this type of attack (DoS). Counter-attackers infiltrate the sensor network and introduce fake data into the system. If a denial-of-service attack succeeds, the WSN's performance can be severely compromised [5].

Background

Related work

Wireless encryption protocol was the only encryption mechanism available to users in the early days of wireless technology (WEP) uses a 40-bit or 128-bit key to encrypt data. An internet search will yield a plethora of tools that may be used to circumvent this protocol. It is possible to attack WEP in a variety of ways [6]. The ways of listening in on encrypted traffic include passive, active and table-based eavesdropping. The WEP algorithm's weaknesses and various attacks can be found on the page "Security of the WEP algorithm" These attacks are designed to exploit the numerous weaknesses of WEP. As attacks on 802.11b and other wireless technologies increase in both volume and sophistication.

Current Solutions

Wi-Fi Alliance certification began in 2018 with WPA3, the latest wireless security standard. Devices seeking Wi-Fi certification by July 2020 must include WPA3, according to the Wi-Fi Alliance. WPA3 requires the use of Protected Management Frames (PMFs) to avoid eavesdropping and forgery [7]. As well as standardizing the 128-bit cryptography suite, this bans the usage of dated security measures. Further protecting business, financial, and government data is made possible by the inclusion of WPA3-Enterprise's additional 192-bit security encryption key and 48-bit initialization vector (IV). WPA3-Personal employs CCMP-128 and AES-128 as its cryptographic algorithms. Good news for organizations is that the WPA3 standard has been approved for continual improvement, ensuring that they have better protection and additional security measures as the threat landscape shifts [8]. WPA3 as a result of the potential pitfalls of migrating from WPA2 to WPA3, network administrators must ensure that their architects are well-versed in the newer protocol before implementing it.

There are four main goals for network security

Security encompasses the four tenets of confidentiality, access, authenticity, and integrity. Stream and block cyphers, in particular, are used for this purpose. When two parties communicate electronically, an intruder or attacker can't access the messages they have sent [9].

Availability: is the most important service in the digital age. Disruption caused by DoS attacks is always present.

Authentication: Authenticated users can only access the data or information. Entities and data sources are both authenticated. Its common to utilize authentication mechanisms for this purpose. Intruders can't get to your data [10].

Integrity: Data and information must be encoded before being sent over the air. Data must be decrypted exactly as it was sent from the source when it reaches its final destination [11].

Comparison

WEP, WPA, WPA2 and WPA3: Which is best? When choosing from among WEP, WPA, WPA2 and WPA3 wireless security protocols, experts agree WPA3 is best for Wi-Fi security. As the most up-to-date wireless encryption protocol, WPA3 is the most secure choice. Some wireless APs do not support WPA3, however. In that case, the next best option is WPA2, which is widely deployed in the enterprise space today. At this point, no one should use the original wireless security protocol, WEP, or even its immediate successor, WPA, as both are outdated and make wireless networks extremely vulnerable to outside threats. Network administrators should replace any wireless AP or router that supports WEP or WPA with a newer device that's compatible with WPA2 or WPA3 [12].

Proposed Solution

Solutions to wireless security threats

In order to ensure the safety of wireless networks, it is important to look at the policies, management, and security design that are in place both outside and internally. Using these policies, you can control who has access to your wireless network and prevent unwanted users from accessing it [13].

Theft prevention: strategies are including: Once the leak has been accurately prevented, it is possible to identify sensitive information. In order to protect particular devices and the cloud, passwords must not be easy to guess, but passwords that include letters, numbers, and symbols must be used to protect all devices and the cloud. A public Wi-Fi connection should be avoided since the unencrypted data that is sent or received can be seen by anybody [14]. Allowing the use of two-factor authentication across the board. Install a firewall to guard against malicious websites infecting your computer.

Damage to hardware, including data loss because of failure: Various good e techniques are as described in the following: It's time to do some hardware maintenance. The equipment must be kept clean and water-resistant for a lengthy period of time. Local drives are backed up: If not the entire disc, but at least some of the most important files must be backed up to the cloud and preserved on another device for the sake of the business. Customer service or a professional technician may be able to help [15]. When dealing with a hardware breakdown, it is best to leave it to a qualified expert to fix the problem, as this could result in further harm to other parts of the device.

Malware and viruses: The most recent software updates should be downloaded and installed. Malware and ransomware frequently target machines with out-of-date operating systems.

Antivirus software should be installed. There are no new updates available for free antivirus software, thus it is always best to use a paid version instead [16]. Don't open e-mails that you don't recognize. It is advisable not to open attachments in email communications since they may include dangerous code that might infect the machine. Before allowing them to be downloaded or plugged into a USB drive, perform a scan.

Credentials in jeopardy: Be on the lookout for phishing websites that look just like the real thing but are actually intended to steal your login details. Until the website gets an SSL certificate, do not enter any personal information. Sensitive information, such as passwords, should only be sent via HTTPS addresses. Keep your credentials in a safe place, not on an infected computer. If you know the PC is compromised with malware, it is advisable not to enter your password. Make use of two-factor authentication so that you can keep track of and, if necessary, halt unauthorized access to your data [17].

Failure of the company's website: The use of third-party security services like Cloud Flare can help prevent DDOS and other web-based attacks on companies and organisations.

Denial of Service (DoS): In a denial-of-service attack, the attacker prevents data from reaching the sensor area altogether. Because of inaccurate or misleading information, Denial of service attacks are created. One of the Denial-of-Service (DoS) methods used to disrupt the functioning of a network is jamming. In order to prevent legitimate users from connecting to the network, malicious attackers target those who use unofficial wireless devices [18]. The company's website should be hosted on a reputable host that does not have any backdoors. Use an SSL certificate to ensure that hackers can't listen in on the data being passed between your website and the servers. Let's simulate a Denial of Service (DoS) attack to analyze it via Wireshark. For the demo, I am using the macof tool, the component of the Sniff suit toolkit, and flooding a surrounding device's switch with MAC addresses. The image below shows IP address is generating requests to another device with the same data size repeatedly. This sort of traffic shows a standard network DoS attack For a DDoS attack, use the macof tool again to generate traffic [19]. Observe the fake source and destination IP addresses are sending many packets with similar data sizes.

Natural calamities that may cause server damage: The placement of the server is critical, so be sure to pick a spot away from any natural disaster zones. In the event of a power loss, there should be a backup source of energy [12]. Make your data redundant and save it in servers located in different geolocations, you can also use cloud services for this.

Evolution of Solution

Wireless protocols protect wireless networks from hacking by encrypting personal data that travels over radio waves. Wired Equivalent Privacy (WEP) was the first wireless network security protocol developed in 1997. However, this protocol contains some shortcomings, so Wi-Fi Protected Access (WPA) was developed to overcome the shortcomings of the WEP protocol. WPA 2 was later developed with advanced features and encryption features. This advanced protocol uses the Counter Mode Block Chain Message Authentication Code Protocol (CCMP) to encrypt data [20]. Wi-Fi Protected Access 3 (WPA 3) is a modern wireless protocol that provides advanced encryption options for both private and public networks

How to secure a wireless network?

a) To protect your Wi-Fi network from unauthorized access, it is always a good idea to hide the wireless network name.

b) Experts recommend checking for bad Wi-Fi hotspots

c) It is always better to upgrade your Wi-Fi encryption and secure your Wi-Fi network by resetting strong and complex passwords for your wireless protocols [21].

Different Type of Security Attacks

Threats to Wireless Internet Security Confidentiality, integrity and access to wireless networks are all protected by network security measures. The vulnerability of security protocols is a source of potential risks. The various sorts of security attack tactics are discussed in this section. Both privacy and integrity can be violated by using these strategies, or they can be used to simply breach confidentiality and integrity. Fig. illustrates the various types of security threats [22].

Traffic analysis detects a denial of service (dos) dictionary

Analysis of traffic: An attacker can gain access to three different sorts of data using this method. There are two types of information that can be gleaned from a network. The attacker must also know where to gain physical access to the surrounding region in order to carry out their attack. The attacker can also gather information about the communication protocol through traffic analysis. In order to gain access to the package's size and number, an attacker must collect data over a long period of time [23].

Eavesdropping: A thief can listen in on private conversations without the agreement of the victims. In addition to listening attacks, there are active listening attacks and active listening attacks that use less well-known plain text.

Passive eavesdropping: To keep tabs on the unrestricted wireless session, passive eavesdropping was employed. In order for an attack to be successful, the attacker must have access to the exit area. It is possible for an attacker to read the data during its deployment and acquire data indirectly by scanning packages with an encrypted connection [24]. The information obtained in this method does not violate anyone's privacy, but it has the potential to be exploited in the most dangerous attacks.

In Active eavesdropping: Attackers watch wireless time and inject their own messages into the session so that they can see what the other person is saying. There must be access to the message's contact information, as well as any other identifying data like an

IP address, in order to conduct this type of attack. The attacker is able to alter the contents of a package so that the integrity of the message is not compromised. Changes in IP or TCP addresses are frequently made by attackers to hide their tracks.

Unauthorized access: In the event that a hacker acquires unrestricted access to a network, he or she will be able to launch more attacks and make undetected use of the system. Unauthorized network use may be regarded as a minimal threat to the network due to the fact that attackers will have a tough time accessing resources due to access rights. Obtaining unauthorized access is frequently the initial stage in an ARP (Address Resolution Protocol) attack chain, and it is the most difficult. Using VPN and IPsec solutions, it is possible to protect users against attacks that damage the application's privacy and confidentiality [25]. This type of attack can be carried out in a variety of ways depending on the circumstances. When an attacker interrupts a session and prevents the channel from reestablishing the AP connection, this is referred to as a technique of attack by the attacker. Although the channel makes every attempt, it is only able to establish a connection with the AP located in the attacker's environment. At the same time, the attacker establishes an AP connection and performs authentication on the network. There is a direct link between the attacker and the access point, however there is no direct contact between the attacker and the channel. Consequently, the hacker has complete access to both the network's modified data and the operating channel on which the hacking occurred. Due to the fact that it only targets a wired component of the network, rather than the wireless clients, this is a modest sort of man in the middle attack. The ARP attack is a type of cyberattack. This type of attack is carried out by a hacker who conceals or misrepresents his or her identity to the victim. The attacker impersonates a verified user and gains access to the network as a result of obtaining a false authorization.

High-jacking: is a type of assault in which the genuine owner is denied access to a legitimate and certified session by the assailants. As soon as the owner loses access to the session, the attacker has already taken his or her time, but the owner believes he or she has lost access to the session as a result of a slow network connection [26]. If the attacker is patient enough, he or she may be able to use the weapon to several uses over the course of several days or weeks. In the present tense, we are witnessing an attack that is taking place directly in front of our eyes. A re-play attack is a method through which an authorized network user can get access to a system. Nothing changes or interferes with the session that is being targeted. When an attack takes place, it does not take place in real time. The attacker acquires access to the network after the initial expiration period has passed. Several sessions are authenticated, and the attacker responds to each session after a period of time or a few times, recording the authenticity and responding to each session.

Denial of Service (DoS): In a denial-of-service attack, the attacker prevents data from reaching the sensor area altogether. Because of inaccurate or misleading information, Denial of service attacks are created [27]. One of the Denial-of-Service (DoS) methods used to disrupt the functioning of a network is jamming. In order to prevent legitimate users from connecting to the network, malicious attackers target those who use unofficial wireless devices.

Dictionary building attack: Dictionary-building attacks, in which the attacker goes through a list of probable passwords for each victim and looks for any information about the victim or language relevant to the target, are a viable option for attackers to consider. An attack on the dictionary's structure may occur after analyzing a large amount of network traffic [28].

Conclusion

In this review article we studied some security issues and explained them in details also covered wireless security protocols and how we can prevent from these attacks and what precautions we have to take whenever we have to connect our devices on private or public internet connection and we also analysis users traffics while using Wi-Fi connections on our devices we used Wireshark which is an essential tool that many blue team and network administrators use daily. The objective might differ, but they analyze network traffic using it. In this article, we have explored several network traffic types like HTTPS, etc. In addition, we have seen few attacks using Wireshark, like the DoS attack.

References

1. Sobh T (2013) Security, Wi-Fi networks security and accessing control. 5(7): 9.
2. Nawshin IJ, Jyoti SJ, Zeba SA (2014) A study of security protocols for wireless local area network. India.
3. Mustafa RN, Hasanian AT, Baraa IF (2021) An analyzing process on wireless protection criteria focusing on (WPA) within computer network security. 9(1): 242-252.
4. Josephin JJ, Jerine S (2021) Survey on various attacks and intrusion detection mechanisms in wireless sensor networks. 12(11): 3694-3704.
5. Zhibo Z, Hussam A, Ernesto D, Chan YY, Fatma T (2022) Explainable artificial intelligence applications in cyber security: State-of-the-art in research. IEEE.
6. Kevin C, Elaine Smyth (2006) Demonstrating the wired equivalent privacy (WEP) weaknesses inherent in Wi-Fi networks. Telecommunication and Network Security 15(4): 17-38.
7. Efstratios C, Georgios K, Constantinos K (2022) How is your Wi-Fi connection today? DoS attacks on WPA3-SAE. Journal of Information Security and Applications 64: 103058.
8. Vink M, Poll E, Verbiest A (2020) A comprehensive taxonomy of wi-fi attacks. The Netherlands.
9. Singh A (2014) Information security: Components and techniques.
10. Stamp M (2011) Information security: Principles and practice.
11. Menezes AJ, Van Oorschot PC, Vanstone SA (2018) Handbook of applied cryptography.
12. Victor OE, Arif S, Agbotiname LI, Piyush KS, Musah A (2022) Assessment and test-case study of wi-fi security through the wardriving technique. Mobile Information Systems.
13. Roman R, Zhou J, Lopez J (2013) On the features and challenges of security and privacy in distributed internet of things. Computer Networks 57(10): 2266-2279.
14. Islam K, Shen W, Wang X (2012) Wireless sensor network reliability and security in factory automation: A survey. 42(6):1243-1256.

15. Islam K, Shen W, Wang X (2012) Security and privacy considerations for wireless sensor networks in smart home environments. IEEE.
16. Karygiannis T, Owens L (2002) Wireless Network Security. USA.
17. Ivan S, Vincent N, Eric A, Yves D, Mohamed K, et al. (2013) Survey on security threats and protection mechanisms in embedded automotive networks. IEEE.
18. Gurkan T, Dimitrios GK, Cagri G, Cengiz G, Erhan T, et al. (2017) A survey on information security threats and solutions for Machine to Machine (M2M) communications. Journal of Parallel and Distributed Computing 109: 142-154.
19. Peng T, Leckie C, Ramamohanarao K (2007) Survey of network-based defense mechanisms countering the DoS and DDoS problems. ACM Computing Surveys 39(1): 3.
20. Kalinin MO, Minin AA (2017) Security evaluation of a wireless ad-hoc network with dynamic topology. 51: 899-901.
21. Rahman A, Ali M (2018) Analysis and evaluation of wireless networks by implementation of test security keys. Emerging Technologies in Computing pp: 200.
22. Yulong Z, Jia Z, Xianbin W Lajos H (2016) A survey on wireless security: Technical challenges, recent advances, and future trends. 104(9): 1727-1765.
23. Chelli K (2015) Security issues in wireless sensor networks: Attacks and countermeasures. Proceedings of the world congress on engineering, UK.
24. Mavridis IP, Androulakis AIE, Halkias AB, Mylonas P (2011) Real-life paradigms of wireless network security attacks. IEEE.
25. Karim L, Mohammad Z (2020) Attacks and defenses in short-range wireless technologies for IoT. IEEE 8: 88892-88932.
26. Padmavathi G, Shanmugapriya D (2009) A survey of attacks, security mechanisms and challenges in wireless sensor networks. IEEE.
27. Mini S, Aditya T, Subhashini N, Bharat B (2017) Classification and analysis of security attacks in WSNs and IEEE 802.15. 4 standards: A survey. IEEE.
28. Murtaza AS, Celestine I, Kniezova J, Noble A (2022) Analysis on security-related concerns of unmanned aerial vehicle: attacks, limitations, and recommendations. Math Biosci Eng 19(3): 2641-2670.