[An Introduction of Wireless Network Security and Vulnerabilities](https://papersowl.com/order?foc_o_paper_type=information%20science%20and%20technology&foc_o_name=An%20Introduction%20of%20Internet%20Security%20and%20Vulnerabilities&foc_o_subject=88&foc_o_pages=2&foc_o_service=1&foc_o_style=5&foc_o_desc=information%20science%20and%20technology&utm_campaign=custom-OF&utm_medium=L&utm_term=order-now&utm_content=fast-order&foc_run=run)

An Introduction of Wireless LAN Security, Vulnerabilities and Countermeasures

Abstract

Wireless Networks have come a long way from its inception of radio waves discovered by Heinrich Hertz in the 1880’s. The rise in the evolution of wireless technology transforming everything into digital changed the way we live and communicate with each other and the demand for the usage of wireless data transmission has witnessed inevitable surge because of the pandemic for relentless need of communication. The Flexibility, ease of installation, No Wires, Cost- effectiveness, Portability, and high coverage area made this technology can be seen everywhere from residences to corporate networks. However, with the greater advantages and security layers, it is also coupled with certain prominent types of attacks classified on the basis of authentication, availability, confidentiality and integrity. There is also been a constant tracking by researchers over the wireless networks to mitigate the problems but there are not sufficient and not always perfect*.* The aim of this study was to review literatures on the Wireless Networks in the areas of security, vulnerabilities, attacks and threats. This study also present solutions or countermeasures which will enhance its security.

Introduction

In the past decade, the world's mobility has increased dramatically, leading to the need for new methods of connecting the world that aren't suited to the challenges our new lifestyles pose. In the midst of the nationwide lockdowns and social distancing norms, a surge in using digital technology is inevitable to reduce the negative impacts on all aspects of life by converting to digitization, and wireless technology is making rapid advances to tackle the threat. Earlier, the users were connected to the network by means of wires or cables, a mentality that is overpowering in that people move around while networks remain stationary. Wireless connectivity has now resuscitated the world of networking and gives network users a great deal of freedom of movement. Now the wireless technologies are overpowering the realms of wired networks. The mobility, flexibility, and cost advantages of wireless networks over wired networks have increased in recent years(**M. Gast, "Introduction to Wireless Networks" in 802.11 Wireless Networks: The Definitive Guide, New York:O'Reilly, pp. 01-06, 2002.**). Data is stored centrally in wireless networks, yet users can access it while they are on the move, as can be seen in **figure 1.** This could boost productivity and further increase output. Earlier if a new user is being added to the network, there arises a need of running cables, installing new terminal and maintaining it in a new jack but wireless networking removes all this and now to offer services to a new user we only have to configure it to the existing infrastructure and not the whole process of installation and wiring is required.

The wireless technology known as Wi-Fi (Wireless Fidelity) is based on the IEEE 802.11 standard. It can be used to build (Wireless Local Area Networks) over both the 2.4 GHz ISM and 5 GHz .This network can be set up by using radio signal frequency to communicate among computers and other devices. It is getting more and more popular nowadays due to the simple setup feature and no cabling requirements for use(**W. A. Arbaugh, *Real 802.11 security: Wi-Fi protected access and 802.11 i*: Addison-Wesley Longman Publishing Co., Inc., 2003.).** Internet users at home and in public places are gradually adopting wireless Internet technology. Technology advances, along with increased price/performance advantages, have made wireless accessibility more widespread in offices and public settings. However, this era of technological flexibility can also expose networks to increased security threats. Signal interference and security are the two most pressing issues the wireless network faces. There have been numerous wireless security protocols designed and implemented since 1990, but none proved to be convincing against the ever-increasing threat of cybercrime threatening our systems and information. With this in mind, it is very important to address wireless network security more efficiently, depending on the business requirements. In the past two decades, wireless network researchers have developed three main security protocols: WEP, WPA and WPA2 are used in the Wi-Fi today, and WPA3 is the improvement of WPA2 came in 2018.

WLAN Encryption Methods.

Our discussion on encryption is primarily focused on encoding information within a session, reading information from a data stream, and scrambling it in order to make it unreadable to users outside the network.

Wired Equivalent Privacy (WEP)

Wi-Fi Protected Access (WPA)

Wi-Fi Protected Access 2 (WPA2)

WEP

The first security protocol that was used for wireless networks which is developed in 1999. WEP was the original security algorithm for IEEE 802.11 wireless networks. It utilizes RC4 for encryption and has been no longer used in today’s world because of vulnerabilities that can be used to find the security keys **(S. Manjula and I. Rasika, "Security weaknesses of WEP protocol IEEE 802.11b and enhancing the security with dynamic keys," in IEEE, Toronto, ON, Canada, 2009).** This encryption can be easily hackable with the help of reuse of initialization vector, improper RC4 implementation.

WPA

A strong encryption protocol called Temporal Key Integrity Protocol (TKIP) was used in WPA to replace WEP in the 802.11i draft. It utilizes dynamic keys with Message Integrity Check (MIC), and uses some of the same mechanisms as WEP, making it as secure as WEP. TKIP uses some mechanisms as WEP which allow similar attacks making it as vulnerable.

WPA2

WPA2 emerged as a response to WPA vulnerabilities by implementing Advanced Encryption Standard (AES). It replaced TKIP with the Cipher Block Chaining Message Authentication Code Protocol (CCMP). Both WPA and WPA2 offers personal and enterprise edition. A pre-shared key is used in the personal edition and the enterprise edition uses the 802.1X extensible authentication protocol. In October 2000, the National Institute of Standards and Technology (NIST) adopted the Advanced Encryption Standard (AES) as a robust solution to the Data Encryption Standard (F. Shao, Z. Chang and Y. Zhang, "AES Encryption Algorithm Based on the High Performance Computing of GPU," in IEEE, Singapore, 2010.) This method of encryption key generation is very robust and dynamic so that hackers cannot collect information from the network. The passphrase used between the access point and client is 8 to 63 characters and includes special characters and symbols. Despite the fact that this protocol offers stronger security with advanced encryption standards than other protocols, there are vulnerabilities that could compromise the network.

Wireless Network Threats  
Some of the wireless network attacks are given below.

A) Access Control Attacks

An access control attack occurs when an authority is needed to control which users have access to which areas and resources in a computer-based system which contains some valuable information. During these attacks, wireless local area network access control measures like access points, medium access control filters, and WI-FI port access controls are used to penetrate the wireless network. Below are some key types of access control attacks.

1. War driving

War driving, also referred to as access point mapping, is the act of finding and possibly exploiting wireless local area networks while driving around a city or elsewhere. Bypassing a private network may be illegal, and at least one person has been prosecuted for it.

1. Rogue access points

Rogue access points can be either set up by employees or by intruders, or they can be from another company in the area. Some malicious devices may take advantage of unauthorised access points and begin to operate on the network anyway. An intrusion detection system should be installed that will audit these access points and constantly learn if there are any rogue access points between them in order to protect against this attack(M. Le. Tung, Liu Ren Ping and Hedlev Mark, "Rogue access point detection and localization", Personal Indoor and Mobile Radio Communications (PIMRC) 2012 IEEE 23rd International Symposium on. IEEE, 2012.).

1. MAC (Medium Access Control) Spoofing

An impostor or hacker steals or spoofs a valid MAC address from the network and circumvents access control measures, giving him the advantage to pose as one of the valid MAC addresses.

1. Physical attacks on Access Points

Often, wireless access points are labeled with their security information on the back or front of the device. If the device is kept in an unsecured location, a hacker could sneak by and read the current credentials (if they haven't been changed) to use them later on(K. Lounis and M. Zulkernine, "Attacks and Defenses in Short-Range Wireless Technologies for IoT," in IEEE Access, vol. 8, pp. 88892-88932, 2020, doi: 10.1109/ACCESS.2020.2993553.).

B) Frame Spoofing

1. Device Deauthentication and Disassociation

This technique forces the client to reauthenticate, which when combined with the lack of authentication for control frames that are used for authentication and association, makes it possible for the attacker to spoof MAC addresses.( Bulk, Frank. “Learn the basics of WPA2 Wi-Fi security”.

Network Computing Jan. 27 2006. <http://www.information

week.com/story/showArticle.jhtml?articleID=177105338>). Similar to the deauthentication an attacker spoofs an access point and sends forged disassociation requests to connected Wi-Fi devices and dissociates them from the network. The target devices do not get deauthenticated; they just have to reconnect to the network.

2. Flooding

In this type of attack, the attacker sends flood of meaningless encrypted data packets to the client devices to their limited resources like battery and

C) Jamming

An attacker generates random noise (signals) on the operational radio channel in order to cause the connected Wi-Fi devices to think that the radio channel is busy.

D) Social Engineering attacks

It is a type of man-in-the-middle attack in which a fake access point is used to intercept traffic. An attacker can then plant malware on the system or capture traffic. It is similar to the phishing type of attacks.

E)Denial Of Service

Denial-of-Service attacks (DoS attacks) occur when an attacker repeatedly sends request messages, prematurely successful connections, failure messages, and other commands to a targeted AP (Access Point).

F) WEP Cracking

There are several types of attacks used to crack the WEP encrypted packets.

1. Caffee Latte Attack.
2. Koreks Chop Chop Attack
3. Fluhrer, Mantin, and Shamir (FMS) Attack
4. Pyshkin, Tews, and Weinmann (PTW) Attacks

G) Dictionary attacks

For dictionary attacks, a computer program is used to systematically enter words from a list as passwords to gain access to a system, account, or encrypted data. In online attacks, the attacker repeatedly attempts to login or gain access to restricted data. Both the WPA and WPA2 are prone to dictionary attacks.

Countermeasures

As long as users and businesses are aware of the aforementioned security considerations and follow best practices, they can prevent attackers from exploiting vulnerabilities in wireless connections.

Turning of the SSID Broadcast identifier(Signal Hiding Technique) will prevent from the attacker to intercept the traffic.

Change the default usernames and passwords that are provided by the service providers.

A firewall can be enabled in devices to provide added security, or a virtual private network (VPN) can be used to access assets remotely.

By auditing wireless networking activity and performance on a regular basis, you can identify problem areas which may require remedial actions such as removal of the offending device or measures to increase coverage and signal strength within the problem area.

Eliminate the Rogue Access points by using 802.1x authentication.

Make sure your wireless network is turned off when you're not using it

Don’t connect to the open networks , if you are connected make sure to browse using the virtual private network.

Effective training and educating to the users about the secure wireless behaviour.

It is recommended to update the firmware on a regular basis and install updated anti virus, firewalls , anti-malware on Wi-Fi devices.

Always use advanced encryption standards for your network communication. Do not use WEP as your encryption as it is outdated and it’s a child game now to crack WEP using the aircrack-ng tool.

Use SSH for remote connections to the network instead of the insecured telnet connection.

Enable MAC filtering to black out non legitimated users.

For even better security always use static ip address configuration compared to the DHCP since an attacker may use it as a leverage to enter into the network.

**CONCLUSION**

After visiting literature reviews that review mainly secondary sources as well as some primary sources, it appears that there are still some challenges in protecting wsireless networks entirely against an attack, threat, or vulnerability. Among the objectives of this study was to identify different security solutions relevant to wireless networks and to propose alternative solutions which would be more likely to allow wireless networks to be secured than current options. . Understanding these attacks and its countermeasures can help users understand the risks and how to mitigate them. In most of the literature, it was reported that securing a completely wireless network isn't easy but some portions of it can be secured, not the whole thing. Next generation researchers will surely be inspired by this study to devise more sophisticated and robust security mechanisms that are challenging to attackers and make networks more secure.

This survey will surely inspire next generation researchers to come up with intelligent and stronger security mechanisms and make a safer network.

Protected Access 2 (WPA2) protocol.

The huge demand for wireless data transmission is never met. *Wireless security is the avoidance of unlawful access or impairment to computers using wireless networks. Securing wireless network has been a research in the past two decades without coming up with prior solution to which security method should be employed to prevent unlawful access of data.*

*The aim of this study was to review some literatures on wireless security in the areas of attacks, threats, vulnerabilities and some solutions to deal with those problems.*

There is also been a constant tracking by rresearchers over the wireless networks to mitigate the problems but there are not sufficient and not always perfect

Wireless LANs are everywhere these days from home to large enterprise corporate networks due to the ease of installation, employee convenience, avoiding wiring cost and constant mobility support. However, the greater availability of wireless LANs means increased danger from attacks and increased challenges to an organization, IT staff and IT security professionals. This paper discusses the various security issues and vulnerabilities related to the IEEE 802.11 Wireless LAN encryption standard and common threats/attacks pertaining to the home and enterprise Wireless LAN system and provide overall guidelines and recommendation to the home users and organizations.

Keywords—WLAN; This paper also present solutions or suggestions which will improve Wi-Fi

Protected Access 2 (WPA2) protocol.