Review on Various Threats on connecting to a common WIFI

P.Buvanya Shri[1], A.Jeevarathinam[2]

[1]PG Scholar, Master of Computer Application, Kumaraguru College of Technology, Coimbatore. [2]Assistant Professor, Hindusthan Institute of Technology, Coimbatore.

***Abstract*— The recent emergence of free public Wi-Fi has been a huge windfall. Hackers are a threat to Wi-Fi users, but there are number of ways to prevent them from hacking. Most of the places that offer free connection points, including cafes, hotels, airports, bookstores, and even odd retail establishments for data access. However, this independence has a cost, and few people are actually aware of the dangers of using public Wi-Fi. The objective of this study is to illustrate the process of protecting the network and ensure the data security.**

Keywords—component, formatting, style, styling, insert (key words**)**

1. INTRODUCTION

WiFi has unavoidably turned into an alluring target for numerous security risks because it carries over 75% of the last-mile mobile Internet traffic. Hackers are drawn to free Wi-Fi hotspots for the same reasons that customers are primarily, the lack of authentication needed to establish a network connection. As a result, the hacker has a fantastic opportunity to gain unrestricted access to unprotected devices connected to the same network. The globe is growing more interconnected every day. Although widespread (and expanding) wi-fi connectivity is practical and necessary for our contemporary lifestyles, it is not entirely risk-free. This article discusses the biggest risks associated with open wi-fi networks for businesses, cyberthreats to be on the lookout for, and how to reducing the exposure to these dangers. Even though there is a chance that private information like login passwords could be stolen by hackers, many employees use public Wi-Fi hotspots to access their work emails and networks. Many employees neglect to adopt security measures because they are unaware of the dangers that their favorite coffee shop's Wi-Fi poses. Even staff members who are aware of Wi-Fi security problems frequently downplay the dangers.

A record-breaking year for cyberattacks was 2020. American professionals retreated to their home offices while offices across the nation closed indefinitely, quarantines were imposed, and stay-at-home regulations were implemented. Many people continued to work remotely as society began to open up again. By 2025, according to some estimates, more than 36 million Americans will have totally remote or flexible work, an increase of 87% since the epidemic. One might deduce that having the opportunity to work outside of the office has led many employees to select open areas like coffee shops, restaurants, train stations, airports, and other public venues to do their tasks, increasing the vulnerability of organizations and employees to cyberattacks.

2. LITERATURE SURVEY

By referring the below papers taken from various reputed journals, the common indications that the Wi-Fi may be hacked. One has to know about the threats and how to secure the wireless networks.

- Wi-Fi that is really slow
- an increase in phone antivirus messages or phishing emails
- Unidentified devices are logging onto the router
- Installing software without permission
- Unexpected Wi-Fi password modification
- Suddenly, the router wants a password

Even though there is a chance that private information like login passwords could be stolen by hackers, many employees use public Wi-Fi hotspots to access their work emails and networks. Many employees neglect to adopt security measures because they are unaware of the dangers that their favorite coffee shop's Wi-Fi poses. Even staff members who are aware of Wi-Fi security problems frequently downplay the dangers.

3. COMMON THREATS

3.1. Piggybacking

The broadcast range of the majority of wireless routers and access points (WAPs) is between 150 and 300 feet indoors and up to 1,000 feet outside. An unprotected Wi-Fi network is accessible to any user within this radius. More knowledgeable users can even drive across areas looking for unsecured wireless networks while equipped with a computer and a strong antenna. Wardriving, a form of piggybacking, is what this is. The issue is that when unauthorized individuals using internet connection, they are able to steal the personal files, monitor and record web traffic, and engage in other unlawful actions.

3.2. Evil twin assault

Also referred to as a pirate Wi-Fi hotspot, this circumstance occurs when an attacker installs an unauthorized access point near where a business has set up its network. The attacker utilizes the same SSID as the network, or one that is close and appears to be authentic. Users connected to this fraudulent access point will think they are on the authentic network because it uses a separate internet connection. Even though the user's link to the access point is encrypted, the attacker, who has complete control over the connection, can intercept, decrypt, and read all information sent. Users who access the internet usually have success with this attack. Since the evil twin is not linked to the enterprise network, users wanting to reach internal services would be unable to do so and would at the very least be aware that there is a fault with the network.

Cybercriminals build up their own system to look like a real WAP in this kind of Wi-Fi assault. To trick unwary users into connecting to their system, they use a broadcast signal that is stronger than the actual one. Any data (such as credit card numbers, login credentials, and personal information) that a user provides over the internet can be easily viewed by the cybercriminal once the user is connected to the false system.

3.3. Malware, worms & viruses

The forced installation of malware, commonly referred to as malicious software, on user devices is one of the main hazards that may encounter when using public wi-fi. All programming and applications written to damage devices or intercept information fall under this general heading. Hackers are able to infect the public WIFI network, which subsequently spreads to the connected devices. Malware may cause havoc and spy on the systems it infects and comes in a variety of forms. In contrast to worms, which may replicate independently and cause much more damage, viruses are a sort of malware that spread through a host file and are activated and replicated by a human.

3.4. Unauthorized use of a computer

Intruders can access the device's data and folders when connected to an unsafe wireless network without turning off file sharing.

3.5. Wireless bug-hunting

Numerous WAPs lack security and do not encrypt the traffic they carry. Any information that send across while connecting to these is visible for hostile actors to intercept using sniffing tools. Because of these reasons, the confidential communications or transactions are at danger. Wi-Fi signals from end devices and access points spread forth in all directions, contrary to what is theoretically depicted in network diagrams. Wireless signals typically spread freely through open space, but different types of antennas can distribute these signals through space in specific patterns. This implies that any Wi-Fi device (laptop, tablet, or smartphone) can snoop on signals coming from nearby users and access points. These signals can be recognized, and the packets they convey can be recorded, saved, and examined with the right software. A packet sniffer is one such piece of software, and while it can be very helpful for troubleshooting and analyzing network performance, it can also be maliciously used to attack a wireless network that has not been properly set up.

These packets are susceptible to collection and storage by an attacker inside range of these signals. What does that imply in terms of security? An attacker can gather packets and reassemble emails, IP phone conversations, credit card data, and even a user's browser history if the network's security measures are inadequate. In essence, anything communicated across an unprotected network is open to attack.

3.6. Credential Vulnerability for Login

Weak and obvious passwords lead to log-in credential vulnerability. By making sure all of the passwords for websites, apps, and WIFI networks are strong and distinctive, the security issues can be avoided.

3.7. Session hijacking

Public WIFI networks provide a platform for a practice known as session hijacking, which involves abusing a valid web surfing experience. This is yet another way that hackers can access a network user's device's data without authorization, making any data pertaining will be incredibly exposed.

3.8. Attack with cracks

This Wi-Fi assault, which is launched using either simple (brute force) or advanced tactics, takes advantage of a wireless network's security flaws to gain access to it. Such weaknesses are sometimes brought on by inadequate configuration or shoddy or incorrect security methods.

3.9. Channel interference

A Denial of Service (DoS) attack in which users are prevented from accessing the system or service under attack. In the case of Wi-Fi, an access point that produces an unlawfully potent signal on the same channels as the genuine network can be put within the coverage area of a network. Users lose network connectivity as a result of interference that disturbs access points and user devices.

4. CONCLUSION

The final conclusion of this study is, the treats can be avoided by following the procedures below:

The SSID, which is a default name provided by all routers for the Wi-Fi network, is widely used. The issue is that the SSID will be kept in its current form, a potential attacker can quickly determine the model of router and use any known weaknesses to their advantage. Hiding the SSID will be used to protect the data, also changing the name of SSID & Wi-Fi will also ensure the router security.

To improve the security, wireless routers and WAPs' default admin passwords should be changed frequently and by using a password of at least 20 characters and a mix of numbers, letters, and different symbols is advised by the Department of Homeland Security (DHS). Also, by verifying the network's data is encrypted and by Limiting the access to the network. It can also be controlled by the usage of a firewall protection and by maintaining the recent patches for wireless router and WAP software.

5. REFERENCES

[1] Pavelić, M., Lončarić, Z., Vuković, M., & Kušek, M. (2018, October). Internet of things cyber security: Smart door lock system. In 2018 international conference on smart systems and technologies (SST) (pp. 227-232). IEEE.

[2] Soroush, H., Gilbert, P., Banerjee, N., Levine, B. N., Corner, M., & Cox, L. (2010). Improving mobile networking with concurrent Wi-Fi connections. Technical Report UM-CS-2010-041, Department of Computer Science, UMASS Amherst.

[3] Lombera, I. M., Moser, L. E., Melliar-Smith, P. M., & Chuang, Y. T. (2014). Peer-to-peer publication, search and retrieval using the Android mobile platform. Computer networks, 65, 56-72.

[4] Bardenova, V., & Thomas, B. L. (2023). Student Voices as the Common Thread through Changing Pedagogical Partnerships. Teaching and Learning Together in Higher Education, 1(38), 4.

[5] Colom, S. V., & Haw, M. A. (2023). Open-source Wireless Sensor Network (Wi-Se Net) for Flexible Deployment. In AIAA SCITECH 2023 Forum (p. 1540).

[6] Kong, H., Lu, L., Yu, J., Chen, Y., Xu, X., & Lyu, F. (2023). Toward Multi-User Authentication Using WiFi Signals. IEEE/ACM Transactions on Networking.

[7] Peng, H. (2012, April). WIFI network information security analysis research. In 2012 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet) (pp. 2243-2245). IEEE.

[8] Suroto, S. (2018). WLAN security: threats and countermeasures. JOIV: International Journal on Informatics Visualization, 2(4), 232-238.

[9] Abedi, A., & Abari, O. (2020, November). WiFi Says" Hi!" Back to Strangers! In Proceedings of the 19th ACM Workshop on Hot Topics in Networks (pp. 132-138).

[10]. S. Sathishkumar, S. Ramesh kuamr, A. Jeevarathinam, K.S. Sathishkumar, K.V. Ganesh Kumar, Temperature dissipation and thermal expansion of automotive brake disc by using different materials, Materials Today: Proceedings, Volume 49, Part 8, 2022, Pages 3705-3710, ISSN 2214-7853.