Risks of using Public Wi-Fi

Name: Amina Marat
Major: Cybersecurity
GCYSEC_501_0A
Gannon University, Erie, PA.

Abstract:- Public Wi-Fi hotspots have become omnipresent in coffee shops, airports, and other commercial locations where customers have come to expect internet access for their computers, smartphones, and tablets. Public Wi-Fi users continue to sign in to email accounts, social networks, bank accounts, and other websites containing confidential personal data despite the fact that most of the traffic on public networks is not encrypted. Such a setting, where a considerable base of users sends private information over an unsecured network, could also serve as a hub for malicious hacker activities. This paper examines the risks associated with using public networks, analyzes the known hacker exploits of public Wi-Fi networks, such as man-in-the-middle attacks, packet sniffing, evil twin, and side jacking, and offers preventive measures for safer public Wi-Fi usage.

***Keywords**: -1- Public Wi-Fi, -2- Risks, -3- Attacks, -4- Protection.*

I. INTRODUCTION

Users can access the Internet from a variety of public locations and at any time of day because of the expansion of public Wi-Fi networks in small businesses such as coffee shops and restaurants, higher education institutions, and municipalities in the United States and around the world. Most of the time, people can easily access these wireless networks without the need for any kind of user identification or authentication. Public Wi-Fi consumers typically check their email, view social networks, shop online, surf the internet, or even use their bank accounts once they are logged in to these networks. Unfortunately, many public Wi-Fi networks are not encrypted, making it simple for malware to spread, man-in-the-middle attacks to occur, and connections to be hijacked. As a result, they put their users' privacy and security at risk in numerous ways.

Recognizing these dangers, users of public Wi-Fi must take particular safety measures when using these networks. For example, consumers are advised to only enter personal information on secured websites (websites whose URL addresses begin with https), to use Virtual Private Network (VPN), and refrain from sending emails containing personal information. Few experts even go so far as to advise users to totally avoid internet banking and accessing private information when using public Wi-Fi since suspicious Wi-Fi networks might be easily deployed by criminals in order to trick people into logging into them (despite the fact that these websites are encrypted). (Maimon, “et al.”, 2017)

To get more confidentiality, users can try more secure access networks including 3G and 4G networks. However, using these networks is typically expensive. Users' awareness of privacy violations is also limited. For instance, when people have a choice between public Wi-Fi and cellular networks, they typically prefer Wi-Fi because it is usually faster and cheaper than 3G/4G cellular networks. Because there is presently no means for users to know the extent to which their privacy is exposed in free public Wi-Fi networks, people regularly ignore the privacy threats they face. Furthermore, with existing technology, mobile operating systems choose a single course of action for all applications.

In this paper, we investigate the potential privacy risks from user-end activities such as web surfing, search engine running, and mobile application usage in public hotspots. Understanding how public Wi-Fi networks release personal information has both technical and social impacts. It may encourage the development of better privacy protection programs from a technical perspective. In terms of social impact, having an in-depth understanding of vulnerabilities and risks can make people more aware of the issue created by the rapid development of mobile technology in daily life and, as a result, minimize possible dangers such as identity theft. (Cheng, “et al.”, 2013)

II. ISSUE STATEMENT

When someone chooses to use public Wi-Fi, they start to make themselves an extremely simple target for attackers by simply placing their private information at risk. Huge numbers of users all over the world who use public Wi-Fi are unaware that their sensitive data is at threat of being hacked. Even though free Wi-Fi has many advantages for society, there are risks associated with using it because the data transmitted over such an open connection is frequently unencrypted and unsafe, making consumers highly susceptible to numerous cyber-attacks. With that said cyberattacks will only significantly increase, putting more and more people at risk of being attacked, if we do not introduce society to these threats or explain the preventive measures of this problem.

III. TYPES OF PUBLIC WI-FI ATTACKS

Eventually, more than half of free Wi-Fi users are unaware of the serious risks that open Wi-Fi networks imply. As was previously mentioned, such open networks are generally not encrypted, making it possible for anyone with inexpensive hardware or simply downloaded free software to intrude into and access any data being transmitted over the network. While using public Wi-Fi hotspots, the following hacks could happen:

- *Sniffers*

Hackers can passively seize data sent across web browsers and web servers on the Internet by using software sniffers. With this technique, hackers can acquire airborne data and then investigate it at their own pace. Data packets are sent across an unencrypted network by a device and can be read by free software programs like Wireshark, NMAP, or Metasploit. These software applications are used to identify web traffic vulnerabilities that require patching. However, hackers have access to a lot of data, which they can quickly search through for crucial information.

- *Evil Twin*

The "Evil Twin" is one of the variations of the MITM (Man in The Middle) attack. This cyberattack method snoops on user data as it is being transmitted, but it gets past any security measures a public Wi-Fi access point may have. A fake access point (AP) is relatively simple to set up, and it is well worth the effort and time for cybercriminals. Hackers can establish an AP with the same name as an actual hotspot using any internet-capable device, including a laptop, smartphone, or tablet. Any data sent after logging into a fake network is sent directly to the hacker.

- *Man-in-the-Middle*

Also known as MITM, this attack involves a third-party intercepting message between two participants. The direct data transfer between the server and the client is disrupted by another component. The unwanted cybercriminal then allows their own customized network to be shown to you, accomplishing it with their own unique messages. A man-in-the-middle attack is especially dangerous for anyone using public Wi-Fi. Since no data is encrypted as it is transmitted, not only is the hotspot public but also your data as well. It is similar to taking candy from a baby, but in this instance, the vulnerable parties are the users of these networks. A suspicious router has the ability to gather a lot of confidential and sensitive data.

- *Scanning*

Finding other hosts on the network is done through scanning. Although scanning has many beneficial and legitimate purposes, an intruder can scan the network for vulnerabilities that can be exploited. Scans are typically hard to detect, and the majority of public hotspots lack the tools necessary to keep an eye on such activity. Despite the number of different kinds of scanning techniques, they all operate on the same core principle: sending particular types of packets to all potential IP addresses on the network and analyzing the responses. An attacker could be able to "fingerprint" or identify precise details about machines from those responses, such as the operating system or open ports. With this information, an attacker may have the ability to spread malware, launch a denial-of-service attack using a different host, or engage in other illegal activities.

- *Denial of service*

A denial of service (DoS) attack intends to stop service to the device of the users. The MITM and spoofing techniques mentioned earlier can be used in a DoS attack, as well as network flooding. An attacker can trick other network users into requesting access to him by using spoofing. The attacker only needs to prevent the request packets from reaching the intended receiver in order to carry out the denial of service. A user would lose access to the router in a public Wi-Fi hotspot, and all network activity would appear to stop.

One disadvantage of public Wi-Fi is the limited bandwidth it forces on users, especially during peak hours. In this situation, an attacker could essentially consume the entire allotted bandwidth by flooding the network with false packets. Users would recognize extremely slow or no network traffic coming into and going out of their devices. It might appear that the hacker in this scenario would be simple to identify, but the attacker can forge the sender address on the malicious packets. Another attack the intruder might use involves tricking another user's computer into carrying out the attack. It is very challenging to identify the true offender and establish guilt as a result of this redirection.

- *Side jacking*

Using the side jacking technique, an attacker can obtain a session cookie that includes usernames and passwords from numerous websites, including LinkedIn and Facebook, by using a packet sniffer, a tool that can catch or log traffic transferring over a digital network.

Almost any public Wi-Fi network is susceptible to wireless eavesdropping. Numerous users believe that if they pay for access to open Wi-Fi at a mall or airport, that connection will be just as secure as the one they have at home or at work. It is impossible for a person who does not have any experience to control the security of a public Wi-Fi network and to identify those that are risky and expose users to hacking. Sadly, it is now up to Wi-Fi users to defend themselves against such dangers. It is crucial to raise awareness of vulnerable attacks, and every Wi-Fi consumer should be informed of what happens behind the scenes. Connecting to any of these open networks puts users at a high risk of a channeling attack. Hackers regularly use "channeling" to carry out man-in-the-middle attacks with the goal of stealing usernames, passwords, and other private information sent by the user. The operation is dangerously easy to perform. Hackers can easily capture passwords and other data by creating an unauthorized entry point in an airport lounge without the consumer's knowledge. (Hammonds and Muhammad, 2019)

IV. PROTECTION PRACTICES AND TECHNIQUES

Why are open-access wireless networks so unsafe? Sadly, there is a trade-off between user comfort and data confidentiality. Finding a good balance between these two can be challenging, and many public networks meet the needs of users' demands for quick, simple access by providing very little security. This section offers some recommendations for precautionary steps that both network developers and users of these networks can take.

➢ *Providers*

Network security is viewed as being "use at your own risk" by vendors of public Wi-Fi. Most providers of free public Wi-Fi hotspots will direct users to a page containing "terms of service" agreements before the client can connect. This redirection is referred to as a "captive portal," and it could also be employed to verify the authenticity of users or collect connectivity fees. While this tactic gives users some hint that the portal is unsafe, it falls short of appropriately alerting users to the potential risks. Instead, a long legal document that guards the provider against liability for data leakage is frequently presented on this page, which the majority of users are likely to skip over without reading. Users are largely unaware of the risk of losing personal data when they visit their neighborhood coffee shops. Therefore, the very first step in creating a safer public internet is education initiatives and detailed, straightforward warnings regarding public networks.

Even though public vendors might not be willing to give up simplicity for confidentiality, adding encryption to their networks could very well significantly reduce the possibility of data leakage. Although encryption wouldn't completely protect information on a network (for instance, an attacker with a Wi-Fi password might still decrypt the data), it does add a level of difficulty that might convince an attacker to give up the idea.

➢ *Users*

When using public Wi-Fi hotspots, users have a variety of options for ensuring that their personal data is protected. It goes without saying that the best safety measure is to avoid sending any information that the user would not want to be compromised. The consumer will have to give up some comfort, such as paying the coffee shop bill, in exchange for security. A user should make sure that all traffic is encrypted for the period of the connection using a transport layer security (TLS) or secure socket layer (SSL) if delicate data needs to be sent via HTTP from a public network. The time and complexity required may deter an attacker from attempting, even though he still may in some cases be capable of breaching secure protocols.

The user's next choice is to route every transmission through a VPN (a virtual private network). A VPN functions as a "benign man-in-the-middle," enabling users to interact with any other spot on the internet over an encrypted channel. One disadvantage of using a VPN is the extra expense, as most VPN providers charge a fee for their services. Additionally, users must also be aware of how to use VPN technologies before installing any software or configuring the service. (Mancinelli, 2013)

➢ *HTTP and VPN together*

Using a Virtual Private Network connection is presently the only efficient method to reduce the risk of public Wi-Fi traffic being seized at the entry point if accessing websites or other online spots that use HTTP must be made. An encrypted tunnel is created by the VPN connection among user's device and a VPN endpoint, allowing traffic to be delivered to a safe location before entering the internet. Even with the use of a VPN, it is important to keep in mind that accessing websites or other online spots via HTTP is not secure since the unencrypted HTTP traffic will escape the VPN before it reaches the desired website or online location.

The configuration of access points allows for either encryption or non-encryption of the traffic between user devices and the entry point. Consumer devices should only connect to entry points that are protected by WPA2 or a more latest security encryption. Users should verify their gadgets to configure WPA2 and disconnect previous security encryption options in order to guarantee that only WPA2 or newer security encryption is used.

Generally, having anti-virus, anti-exploit, antimalware, and anti-ransomware software installed on a device is by far the most crucial step a user can take to improve their safety when using public Wi-Fi. When a device connects to an unprotected Wi-Fi hotspot, the default configuration is not secure. (Almarri, 2019)

V. CONCLUSION

Public Wi–Fi hotspots are here to stay. Consumers will view free public Wi-Fi as the routine instead of the exception as more devices will enter the marketplace. The modern customer is likely to select a place with internet access rather than without. As a result, both users and public Wi-Fi vendors have something to obtain from protecting open networks, and an increased workload from providers would contribute to a safer internet for all users. Vendors should think about taking a number of steps in the future to protect their networks, including VPN tunneling, stronger encryption techniques, and basic informational campaigns. However, this does not imply that users are not equally accountable for the information they transmit over open networks. Although relying on public Wi-Fi poses a significant security risk, there are measures we can take to ensure the safety of our personal data. Unfortunately, the more risks we take using a free network connection, the more likely it is that a security breach will occur. All things considered, our chances of minimizing the possible danger increase with better protection of ourselves.

REFERENCES

[1]. Maimon, D., Becker, M., Patil, S., & Katz, J. (2017). {Self-Protective} Behaviors Over Public {WiFi} Networks. In *The LASER Workshop: Learning from Authoritative Security Experiment Results (LASER 2017)* (pp. 69-76). https://www.usenix.org/system/files/conference/laser2017/laser2017_maimon.pdf (lit 4)

[2]. Muhammad, J. Does Connecting to Public Wi-Fi Have an Effect on Your Personal Information and Privacy. http://iac.science.hamptonu.edu/media/docs/20210712_215730_Hammonds_ADMI2019.pdf (lit 13)

[3]. Mancinelli, D. (2014). Public Wi-fi: Friend or Foe. https://www.cs.tufts.edu/comp/116/archive/fall2013/dmancinelli.pdf (lit 12)

[4]. Cheng, N., Wang, X. O., Cheng, W., Mohapatra, P., & Seneviratne, A. (2013, April). Characterizing privacy leakage of public wifi networks for users on travel. In *2013 Proceedings IEEE INFOCOM* (pp. 2769-2777). IEEE. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6567086 (lit 3)

[5]. ALMARRI, A. J. (2019). *An investigation of the different risks associated with: The public Wi-Fi and Hotspots* (Doctoral dissertation, The British University in Dubai (BUiD)). https://bspace.buid.ac.ae/bitstream/handle/1234/1467/20170468.pdf?sequence=1&isAllowed=y (lit 14)

[6]. Noh, J., Kim, J., & Cho, S. (2018). Secure authentication and four-way handshake scheme for protected individual communication in public wi-fi networks. *IEEE Access*, *6*, 16539-16548. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8314146

[7]. Hole, K. J., Dyrnes, E., & Thorsheim, P. (2005). Securing wi-fi networks. *Computer*, *38*(7), 28-34. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1463102

[8]. Pandey, S. (2011). Modern network security: Issues and challenges. *International Journal of Engineering Science and Technology*, *3*(5), 4351-4357. https://elmnet.ir/Content/UserProfile/Document/10038047-960f334f-4f27-41ee-a5f5-6b7c21023a8e.pdf

[9]. Karaymeh, A., Ababneh, M., Qasaimeh, M., & Al-Fayoumi, M. (2019, October). Enhancing data protection provided by VPN connections over open WiFi networks. In *2019 2nd International Conference on new Trends in Computing Sciences (ICTCS)* (pp. 1-6). IEEE. https://ieeexplore.ieee.org/abstract/document/8923104