BFH1925002F

by Iftekhar Efat

Submission date: 13-Mar-2022 01:53AM (UTC-0500)
Submission ID: 1782995741
File name: BFH1925002F.pdf (217.44K)
Word count: 3399
Character count: 17690

The dangers of connecting your device to a public wireless network

Ishrat Jahan Rintu
BFH1925002F

March 13, 2022

Report submitted for **SE2206: Information Security** under BSc. in Software Engineering Program, Institute of Information Technology (IIT), Noakhali Science and Technology University

Project Area: **Information Security .....**
Project Supervisor: **MD. IFTEKHARUL ALAM EFAT**
Assistant Professor
Institute of Information Technology (IIT)
Noakhali Science and Technology University

Abstract

Wireless networks are becoming the norm in the society, where hotspots bestow users ingress to the internet through mobile devices.Unknown wireless networks, open public networks with unknown identity, pose threats as hackers can gain unauthorized access to users' private information stored in their mobile devices.This report examines the different exposures and vulnerabilities of connecting to public Wi-Fi that place users at risk of compromising their sensitive data while making it available to cyber criminals. It will also discuss what privacy rights are at risk in the usage of public hotspots, and argue that the risks presented by public hotspots are too great to not receive heightened protection by way of the law.This report will next explore possibilities as to what can be done to assist in keeping consumers safe from harmful computer crimes that invade their privacy.

1 Introduction

Unknown wireless fidelity (Wi-Fi) networks are public open networks whose identification is unknown.Many, if not all, consumers nowadays carry an internet-enabled gadget with them, whether it's a phone, laptop, tablet, or other device.. To get online, and avoid extra expenses by using a cellular connection, many opt to use free Wi-Fi internet connections which are often widely available.Although public Wi-Fi makes connecting to the internet quick and convenient, it does not ensure a safe network environment.Although much of the traffic on public networks is unencrypted, many public wi-fi users, many of whom are unaware of the hazards, continue to log in to email accounts, Facebook accounts, bank accounts, and other domains that hold sensitive personal information.Once logged into these networks, public Wi-Fi users tend to check their email accounts, access social networks, shop online, and even access their bank accounts. Unfortunately, since many of the public Wi-Fi networks are unencrypted and allow for an easy distribution of malware, man-in-the-middle attacks, and hijacking connection, they pose serious risks to their users' security and privacy. Acknowledging these risks. An environment like this, where a high number of users exchange sensitive data via an unencrypted network, might be a hotspot for nefarious hacker activity.
Recognizing these dangers, the Federal Trade Commission (FTC) advises users of public Wi-Fi networks to tread cautiously when accessing these networks.[1]

Users are advised to utilize encrypted Wi-Fi networks, provide personal identifying information only on secure websites, connect to a Virtual Private Network (VPN), and avoid sending emails containing personal information, among other things. Few experts go so far as to say that, because criminals can easily set up fraudulent Wi-Fi networks to deceive people into logging in, users should avoid doing online banking or accessing sensitive data while using a public Wi-Fi network, even though the websites are encrypted. Unfortunately, despite ongoing attempts to raise public Wi-Fi users' knowledge of these risks and the security precautions that may be taken, they are nonetheless vulnerable. Unfortunately, despite the continued efforts that are being made to improve public Wi-Fi users' awareness of these hazards and the security measures that they need to take, consumers still lack understanding of how common self-protective behaviors are among public Wi-Fi users.[4]

---

2 Privacy and Data Leakage

The internet today allows users to easily access a wide range of personal data. Consumers favor convenience despite the danger of online data theft, as seen by the continued rapid expansion of ecommerce, online banking services, and social networking. The expansion of public-wi-fi hotspots into practically every public space is due to this need for convenience. Users recognize the advantages of public wi-fi, but many are unconcerned about, or even aware of, the threats that an open public wi-fi network poses the frequency of attacks on an open network that even a beginner cracker could carry out,there is a legitimate risk that personal information may get into the hands of a malicious third party. Bank account information, personal

emails and contact lists, credit card numbers, passwords, and private messages are among the types of information collected. Once data has been stolen, it cannot be retrieved, and users will almost never know who took it, how it happened, or when it happened. The data might be used in a variety of ways by the attacker, including selling credit card details, getting access to a user's online accounts, and sending spam messages to contacts.

---

3 Attack Vectors

Several attack tactics for open wifi networks are described in this section. It is extremely difficult, if not impossible, to identify an attack in many circumstances.This is due to the open nature of public-wi-fi hotspot connections. Two main properties of public wi-fi provide attackers with relatively easy access to other users' data: (1) the unencrypted nature of public networks; and (2) the lack of a physical barrier to receiving all packets on the network.With neither of these security guards in place, an attacker can join the network anonymously, sniff packets intended for other users, redirect traffic to the attacker's computer, or otherwise disrupt network services.Furthermore, these attacks are virtually untraceable and difficult to detect in most situations, making public wi-fi hotspots an even more appealing target for criminals.The rest of this section goes over the most common attacks on public Wi-Fi networks, but it by no means covers all possible flaws.

3.1 Sniffing and Scanning

Sniffing By far the easiest and stealthiest method of intercepting other users' data is known as "packet sniffing."Software sniffers allow hackers to passively intercept data sent between a web browser and web servers on the Internet.On an open, unswitched network such as most public wi-fi hotspots, data packets intended for a specific user are actually sent unencrypted to all other users connected to the network. There are several popular tools that will perform packet sniffing with the click of a button, like Wireshark, tcpdump, and Cain and Abel. Once sniffed, packets can be analyzed to find username/password pairs, files, instant messages, or any other unencrypted data sent over the network.An attacker can infer trends in another user's web browsing just by looking at HTTP data, which can help them launch further, more complex attacks. Packets can also provide information about a user's identity, such as the device names sent from iPhones.Because packet sniffing is a purely passive process, there is very little protection against it on an open network. The unexpected recipient is only required to listen and not to change the network flow in any manner. This also makes it impossible to identify a sniffer using technological methods.

Scanning is a technique for locating other hosts on a network. An attacker can scan the network for vulnerable holes, even if scanning has numerous legal uses.

Scans are notoriously difficult to detect, and most public hotspots lack the capacity to keep track of them. Scanning methods vary, but they all follow the same fundamental premise of sending specific sorts of packets to all possible IP addresses on the network and analyzing the responses. From those responses, an attacker may be able to identify, or "fingerprint", specific information about machines, such as operating system or open ports. Armed with this knowledge, an attacker may be able to propagate malware, use another host in a denial-of-service attack, or perform some other form of illicit behavior.

3.2 Man-in-the-Middle Attack

Man-in-the-middle (MITM) is a designation for an attack in which a third party intercepts communications between parties involved. A man-in-the-middle (MITM) attack is a significantly more complicated type of attack, but it allows for more options.Another element breaks the relationship between client and the server, preventing data from being transferred directly. The uninvited cyber-criminal then gives you access to their own version of a network, complete with their own unique messages.

Attackers' ability to modify the address resolution protocol (ARP), which links IP addresses to ethernet addresses, is used in this attack. All hosts on the network communicate using ARP and preserve a table of all other hosts' link layer addresses. Because any host can declare that it is associated with any IP address, the vulnerability exists, allowing a host to impersonate another. ARP spoofing is the term for this method, and there are several tools that can be used to carry it out.

A man-in-the-middle attack is potentially deadly for anyone who consumes public

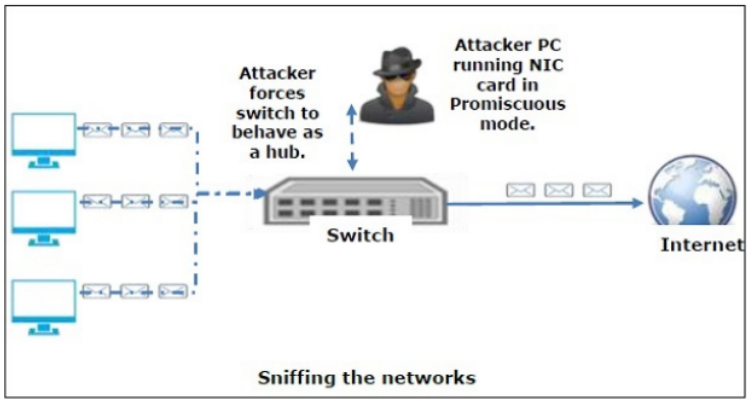

Figure 1: Man-in-the-Middle Attack

Wi-Fi. It's not just the hotspot that's exposed to the public; it's also your data, because all of the data transmitted is unencrypted. It's similar to taking sweets away from a toddler, except that in this situation, the users of these networks are

the ones who are in danger. A hacked router can accumulate a lot of sensitive and confidential information. By hacking into your emails, cybercriminals can acquire access to your passwords, usernames, and private messages/pictures.[3]

There are measures in place to protect against these assaults, but they are often ineffective. A certificate authority will be used by many SSL servers to validate the SSL connection's identity. In many cases, however, the user is pretty much given an unorthodox message about certificates, which many users will unwittingly accept.

3.3 WIFIPHISHER or Evil Twin

The "Evil Twin" is another name for type of MITM attack. This cyber-attack approach scrambles user data as it flows via a public Wi-Fi hotspot, bypassing any security protocols in place. As previously stated, setting up a fake access point (AP) is rather simple and well worth the time and effort for hackers. Hackers may set up an AP with the same name as a legitimate hotspot using any device with internet capabilities, such as a laptop, tablet, or smartphone. Any data submitted after joining a phony network is forwarded straight to a cybercriminal. One of the more common spots for WIFIPHISHER or Evil Twin is the free airport hotspot.

3.4 Side jacking

Side Jacking is a way of stealing a session cookie holding usernames and passwords from a number of websites, such as Facebook or LinkedIn, using a packet sniffer, a tool that may intercept or capture information travelling across a digital network.Because the session cookie already provides access to the website's content, sidejacking allows the bad actor to spoof the user.

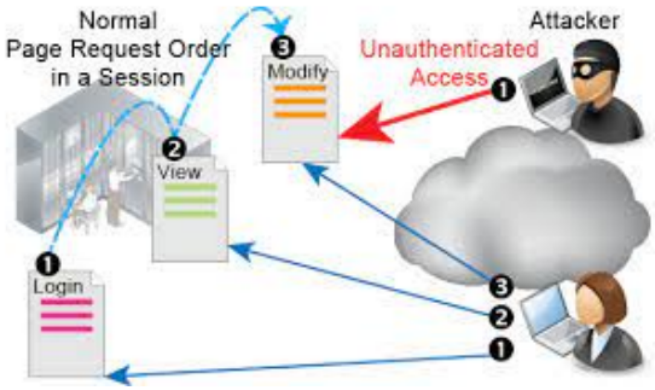

Figure 2: Side Jacking

The bad actor does not have access to the user's password when they utilize side-jacking. The bad actor loses access once the session is turned off and authentication is required to log in. SSL access helps prevent passwords from being discovered, however many websites do not encrypt data after login, leaving them vulnerable to this sort of security flaw.

3.5 Rogue Access Points

An attacker pretends as an access point (AP) designed to seem like a real AP in this type of attack. When a user connects to this AP, the attacker gains total control over all network connections made by that user. Rogue access points are the result of a newly formed connectivity paradigm: consumers expect to be able to connect to the internet for free, no matter where they are. Since a result of this requirement, verifying an access point's legitimacy is a tough task, as it might obstruct a user's capacity to link to an AP swiftly and transparently in any situation.The attack is motivated by the ease that public internet connections provide to mobile device users. In this attack, a user would connect to the phony AP, but no data requests would be sent. Due to the fact that most smart phones block broadband access in favor of a wi-fi connection, the phone is unable to receive data. This is only one of numerous attacks that may be carried out via mobile connection, which is becoming increasingly prevalent.

3.6 Denial of Service

A denial of service (DoS) attack seeks to prevent a user's (or a group of users') device from receiving service. A DoS attack can be carried out via the spoofing and MITM techniques outlined before, or simply flooding the network. An attacker can use spoofing to deceive other network users into requesting access to the attacker. The attacker only has to not send the request packets to the intended receiver to cause a denial of service. A user would lose access to the router at a public wi-fi hotspot, and all network activity would appear to stop.

Wireless spying is possible on almost any public Wi-Fi network. Many users believe that if they pay for an open Wi-Fi network at a mall or airport, the connection would be as secure as their home or business network. It is hard for a novice to control the security of a public Wi-Fi network and detect those that are unsafe and expose users to hackers. Unfortunately, today's Wi-Fi users are responsible for protecting themselves from such dangers. It's critical to raise awareness about the dangers of susceptible assaults, and every Wi-Fi user should be aware of what's going on behind the scenes.

4 Protection Practices and Strategies

There is a tradeoff between privacy protection and user convenience, that is why public wifi hotspots are insecure. Finding the correct balance between the two may

be challenging, and many public networks cater to users' desires for simple, speedy access by providing little to no security.This section offers some recommendations for precautionary steps that implementers and users of these networks can take.

Providers When it comes to network security, public wi-fi hotspot providers take a "use at your own risk" approach. A user's browser will be sent to a "terms of service" page by most public wi-fi suppliers, that must be accepted before the client may join. A"captive portal" is a type of redirection that may be used to verify user authentication or charge for connectivity.While this technique gives consumers some indication that the site is unsafe, it falls short of adequately warning them about the risks. Instead, most users will likely reject this page without reading a long legal contract that protects the seller from data loss responsibility.

Although public vendors may not be ready to give up convenience for security, implementing encryption on their networks would dramatically reduce the risk of data loss. Though encryption can not totally secure data on a network (for example, an attacker who knows the network password might still decode the data), it does provide a degree of complexity that may induce an attacker to search elsewhere.

Users When using public wi-fi hotspots, users may take numerous actions to guarantee that their personal data is sufficiently safeguarded. The ideal safety mechanism, of course, is not to send any piece of data that the does not want monitored. However, this implies that the user must trade expediency for security, such as making a payment in a coffee shop. If private information must be transferred over HTTP from a public network, the customer should utilize a secure socket layer (SSL) or transport layer security (TLS) to encrypt all transactions for the length of the remote connection. In some circumstances, an attacker may still be able to spoof secure protocols, but the time and complexity needed may deter the attacker from doing so. [2]

VPN When it comes to staying secure when using public Wi-Fi, VPNs are essential. When connecting to your business over an unprotected connection, such as a Wi-Fi hotspot, a Virtual Private Network (VPN) connection is required. The amazing thing about VPNs is that even if a cyber-criminal manages to place himself in the midst of your connection, your data will be securely protected. Because computer hackers are looking for simple targets, they are more likely to dump stolen data rather than putting it through a lengthy decryption procedure. Encryption prevents unauthorized parties from viewing the data you're sending and receiving.The majority of cyber-criminals are seeking for an obvious hole in your system, and if they notice that users are using a secure channel, they will go on to the next target who does not have a VPN. Overall, the main reason why hackers are snooping around public Wi-Fi networks is that they are not encrypted.

Turn off sharing When using the Internet in a public setting, it's unlikely that you'll wish to provide any personal information.Depending on the operating system, users can disable sharing through system preferences or Control Panel settings. If

they're running Windows, the first time you connect to an unprotected network, Windows will basically turn "sharing" off for you by picking the "Public" option.[3]

When you're not using Wi-Fi, turn it off Even if users haven't made a strong connection to a public network, the laptop's Wi-Fi hardware is nevertheless transmitting data to any wireless network within range. Although not all wireless routers are created equal, professional cyber-criminals may be highly resourceful when it comes to backdooring or exploiting any given vulnerability in your system. One blunder might signal the start of a security breach. Overall, if you're simply using your laptop or smartphone to work in Microsoft Word or PowerPoint, turn off the Wi-Fi because these apps can be used without it.

5 Conclusion

Public Wi-Fi hotspots are here to stay. Consumers will see public wi-fi as the standard rather than the exception since more mobile devices reach the market. If a venue does not provide internet access, the modern customer is more inclined to patronize one that does. As a result, public wi-fi sellers stand to benefit just as much as consumers from safeguarding public networks, and a greater role for vendors would assist to create a safe and secure internet for everyone.Unfortunately, the more you take your gambles with a free network connection, the greater the likelihood that you will suffer some type of security breach. There is a popular saying in the cybersecurity industry which states "There are three types of people in the world. Those who have been hacked, those who will be hacked, and those who are being hacked right now and just don't know it yet". All in all, the better you protect yourself, the greater your chances of minimizing the potential damage.There are several initiatives that suppliers should take in the future for safeguarding their networks, whether through improved encryption technologies, VPN tunneling, or simple educational campaigns. This isn't to suggest that users aren't accountable for the information they communicate across public networks. The rise in online financial, medical, and commercial activities necessitates the development of more secure public networks. The only question is whether public wi-fi security will be the result of proactive planning or reactive disaster.[3]

References

[1] Emmanuel W Ayaburi, James Wairimu, and Francis Kofi Andoh-Baidoo. Antecedents and outcome of deficient self-regulation in unknown wireless networks use context: An exploratory study. *Information Systems Frontiers*, 21(6):1213–1229, 2019.

[2] Dave Mancinelli. Public wi-fi: Friend or foe. 2014.

[3] Jean Muhammad. Does connecting to public wi-fi have an effect on your personal information and privacy.

[4] Ellie Shahin. Is wifi worth it: The hidden dangers of public wifi. *Catholic University Journal of Law and Technology*, 25(1):7, 2017.

BFH1925002F

ORIGINALITY REPORT

48%	35%	7%	35%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to University of Northumbria at Newcastle Student Paper	18%
2	tuftsdev.github.io Internet Source	15%
3	docplayer.net Internet Source	4%
4	link.springer.com Internet Source	2%
5	www.usenix.org Internet Source	2%
6	Submitted to Waltham Forest College Student Paper	2%
7	v1.overleaf.com Internet Source	2%
8	hbr.org Internet Source	1%
9	global.oup.com Internet Source	1%

10	e-channelnews.com Internet Source	1%
11	Submitted to UT, Dallas Student Paper	<1%
12	www.coursehero.com Internet Source	<1%

Exclude quotes	On	Exclude matches	Off
Exclude bibliography	On		

BFH1925002F

PAGE 1

Article Error You may need to use an article before this word. Consider using the article **the**.

PAGE 2

Prep. You may be using the wrong preposition.

PAGE 3

Article Error You may need to use an article before this word.

Proofread This part of the sentence contains a grammatical error or misspelled word that makes your meaning unclear.

Run-on This sentence may be a run-on sentence. Proofread it to see if it contains too many independent clauses or contains independent clauses that have been combined without conjunctions or punctuation. Look at the "Writer's Handbook" for advice about correcting run-on sentences.

PAGE 4

Run-on This sentence may be a run-on sentence. Proofread it to see if it contains too many independent clauses or contains independent clauses that have been combined without conjunctions or punctuation. Look at the "Writer's Handbook" for advice about correcting run-on sentences.

Missing "," You may need to place a comma after this word.

Missing "," You may need to place a comma after this word.

Article Error You may need to use an article before this word. Consider using the article **the**.

Article Error You may need to remove this article.

PAGE 5

Article Error You may need to use an article before this word.

Article Error You may need to use an article before this word.

Article Error You may need to remove this article.

PAGE 6

Article Error You may need to use an article before this word.

Article Error You may need to use an article before this word.

PAGE 7

Missing "," You may need to place a comma after this word.

P/V You have used the passive voice in this sentence. Depending upon what you wish to emphasize in the sentence, you may want to revise it using the active voice.

Article Error You may need to use an article before this word.

Article Error You may need to use an article before this word.

Possessive This word may be a plural noun and may not need an apostrophe.

Possessive This word may be a plural noun and may not need an apostrophe.

Article Error You may need to remove this article.

PAGE 8

Prep. You may be using the wrong preposition.

Article Error You may need to use an article before this word.

Word Error Did you type "**the**" instead of "**they**," or have you left out a word?

Article Error You may need to use an article before this word.

Proper Noun If this word is a proper noun, you need to capitalize it.

PAGE 9

PAGE 10