IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 5.731
Volume 11, Issue 1, November 2021

Study on the Hazards of Linking the Smartphone to a Public WiFi Network

Rashmi Singh[1], Dhabade Rohan[2], Hankare Sanjana[3]
Asst. Professor[1] and SYBMS[2,3]
Uttar Bhartiya Sangh's Mahendra Pratap Sharda Prasad Singh College of Commerce & Science, Mumbai, Maharashtra

Abstract: *A wireless network is utilized to establish connectivity between different wired infrastructures, enabling seamless mobility for employees within the organization by circumventing the limitations of a physical network. Ensuring the security of the wireless local area network (WLAN) is crucial for a company since it is directly connected to the organization's core network. The proliferation of public wireless access points (hotspots) and the advent of wireless computing devices like tabletop mobiles have facilitated easier internet data access for individuals. The primary objective of this article is to investigate the extent to which users are cognizant of the privacy risks associated with engaging in activities such as internet surfing, computer program querying, and using social networking platforms on publicly accessible hotspots. The primary objective of this study is to aid university decision-makers in evaluating the preferences of public Wi-Fi users about the accessibility of commonly searched sites inside the university's network, and to optimize the allocation of university resources accordingly..*

Keywords: Public Wi-Fi, Privacy, Websites, Leakage, Network

I. INTRODUCTION

In modern times, the internet has become an essential requirement for human existence and is primarily utilized for work-related tasks rather than for leisure. It facilitates various day-to-day activities such as transferring funds, paying bills, making ticket reservations, conducting research, acquiring knowledge, engaging in business transactions, and providing media coverage, among other things. If we had an inclination towards condensing the concept of interconnected networks into a concise statement, it would be "a network of networks referred to as the internet". If we just cite a network, what precisely does it refer to? What is its origin? Consequently, the solution consists of two or more nodes, which are also referred to as systems or PCs.

The prevalence of public Wi-Fi hotspots is steadily rising worldwide. The majority of users opt to connect to hotspots due to their cost-free nature (in contrast to mobile cellular connections) and widespread availability. The global distribution of public Wi-Fi Access Points (APs) has currently reached 94 million and is projected to grow to 549 million by 2022. In the past decade, mobile devices such as smartphones and tablets have become incredibly prevalent. According to the New Zoo Research Organization, more than 3.3 billion smartphones and 230 million tablets were utilized in recent years. Wi-Fi is an essential feature of mobile devices that enables them to establish a connection with the internet.

In the context of computer networks, nodes or hosts refer to devices such as computers, mobile phones, and servers. Each of these devices possesses a distinct code, sometimes referred to as a raincoat address. At first, diversity arises when network providers introduce devices like switches, routers, and other alternatives to the market. In order to avoid the need for physical wiring within a building, it was necessary to develop a technique by which residential, commercial, and communication networks could create connectivity. One such method is the costly and time-consuming approach, which is often regarded as a protracted process. It facilitates the establishment of diverse wireless connections, including WLANs, mobile phone networks, wireless sensor networks, satellite communication networks, and microwave networks.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 5.731
Volume 11, Issue 1, November 2021

II. LITERATURE REVIEW

Wireless networks offer a convenient means for clients to access the internet, and numerous firms find it advantageous to offer complimentary Wi-Fi. In 2016, the United Kingdom has almost 269,000 free Wi-Fi hotspots. Additionally, more than 200 subway stations in London continue to offer free Wi-Fi, enabling individuals to explore alternative transportation alternatives in case of disconnection. Nevertheless, there are inherent security vulnerabilities linked to the utilization of public Wi-Fi. The literature extensively examines the disclosure of privacy in traditional online social networks (OSN), with a particular emphasis on privacy concerns in social networks where users have prior knowledge, such as the analysis of user connections and the profiling of user behaviors. One can combine the privacy information obtained from several websites and analyze the ability to connect this information to the profiles of individual users on external servers. To tackle this problem, numerous measures are being explored to safeguard the privacy of third-party aggregators.

Previous studies have shown that it is feasible to intercept Wi-Fi traffic in order to identify personal information when using public hotspots. The survey indicates that users possess insufficient understanding of the risks associated with Wi-Fi usage and have a misguided sense of safety. Online tracking, a widely used practice in online development, serves several goals such as targeted advertising, identity verification, web analytics, and customisation. Net pursuit strategies are frequently categorized as transient or vagrant.

III. METHODOLOGY

In order to examine the privacy implications of using public Wi-Fi networks, we devised a three-part experiment. The initial phase involved identifying a public Wi-Fi network, followed by the second phase which entailed capturing and analyzing users' network traffic. The last phase involved assessing the data that was collected. Figure 1 illustrates the schematic diagram of the planned experiment.

- **Setting up a public wi-fi network**

We partnered with Minia University's knowledge technology center, which offers extensive Wi-Fi coverage for students, employees, and faculty members. The center's administrator allocated three hotspots for our experiment, designated them as public, and provided them with web service through a dedicated server. In order to monitor and observe people who access the internet using these hotspots, we have installed Wireshark (version 3.0.6, 64 bit) on the Windows server.

- **Acquiring User Traffic**

We have identified our experimental open public Wi-Fi network (consisting of 3 hotspots) at Minia University, which is available at different locations and hours. When users accessed the internet using our public Wi-Fi, Wireshark recorded the data flow from their devices to the internet through our experimental Wi-Fi network. This information was then saved as PCAP files on the Server's permanent memory at regular intervals (twice per day) and retained for a period of 3 days. The data was collected during the course of one month, specifically from the Gregorian calendar month of December 2020. The dataset consisted of 7295 users.

- **Data Collection and Analysis**

In this section, we constructed a model utilizing the Python programming language to analyze the gathered data. This model does data analysis in a two-step process. The initial procedure involves analyzing PCAP files to extract the headers and relevant data of HTTP, DNS, ICMP, SMTP, and POP3 protocols. This data is essential for directing the traffic from the participants' devices to the web. Subsequently, the extracted information is stored in different CSV files, with each file dedicated to a specific protocol, serving as records.

If a device establishes multiple connections to our experimental Wi-Fi network, it is classified as the same user. In the second phase, we analyze the data included in the to identify the visited websites and any potential breach of user privacy.

Wireless network architecture

Wireless access points efficiently cooperate with a radio transceiver to build a connection that enables both the transmission and receipt of radio signals. Consumer gadgets receive these signals and analyze them to form communication channels, which in turn provide enhanced network access. Wireless access points employ the IEEE

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 5.731
Volume 11, Issue 1, November 2021

802.11 protocol, which serves as the prevailing standard for wireless communication in the industry. The primary use of this standard is Wi-Fi, also referred to as WIFI.

Wireless access points efficiently cooperate with a radio transceiver to form a connection that enables the transmission and reception of radio signals. Consumer devices receive these signals and use them to establish extra access to the network through established communication channels. Wireless access points utilize the IEEE 802.11 protocol as the definitive standard for wireless communication. The primary use of this standard is Wi-Fi, commonly referred to as WLAN.

Wireless Protocols and Standards

Wireless refers to the transmission of data using electromagnetic waves instead of physical lines. Morse radiotelegraphy was employed in the early 20th century to operate the earliest wireless transmitters. The field of technology is in a constant state of flux and is progressively assuming a more significant role in the lives of numerous individuals. It has caused a significant number of individuals to become dependent on technology for virtually all kinds of work.

Wireless access technologies are categorized into the following classifications:

1. Wireless Personal Area Network (WPAN) is a type of network that is specifically designed to be used in a variety of applications. IrDA and Bluetooth are two instances. Furthermore, there is a growing trend in the development of other square measurement technologies for this method. 802.15.4a, also known as Zigbee, and 802.15.3c, sometimes known as UWB, are standards that define wireless communication technologies.
2. A Wireless Local Area Network (WLAN) is a type of network that operates within a range of 100 meters and has a maximum speed of 200 Mbps. Wi-Fi, also known as 802.11a/b/g, is a widely used technology for wireless local area networks.
3. The Wireless Metropolitan Area Network (WMAN) technology has the capability to provide a maximum speed of 75 Mbps. The collective term for multiple variants of the 802.16 standard is WiMAX.

Conduct an inquiry into the violation of privacy

We allocated a distinct classification to each device linked to our experimental Wi-Fi networks by utilizing the MAC address and device name. This facilitated our ability to monitor and trace specific users, including their frequent website visits. Unfortunately, their personal information has been compromised, resulting in a breach of privacy. To investigate further, we selected ten users at random and examined the websites they frequently visited.

1.The device with the MAC address HUAWEIY_9a-7346697ffa has the MAC address C6:fe:49:**:** and is used for instant messaging.
2.Device: OPPO Reno2 MAC Address: 6a:3a:b6:f3:**:** Activity: Social Networking
3.The HUAWEI Mate device with the MAC address C4:fe:5b:f:**:** is capable of streaming media and downloading content.
4.The Oppo-F9 device has a MAC address of 44:46:87:4c:**:** and is used for sports activities.
5.The Realme 6 Pro device with the MAC address 44:46:87:fc:**:** is being used
6.Oppo-F11 has the MAC address 00:0c:29:9d:**:** and belongs to the field of Information Technology.
7.Device Name: Galaxy Grand Prime Pro MAC Address: F0:67:28:9d:**:** Category: Business and Finance
8.Oppo-A31 F0:67:28:93:**:** Exploration platforms and data retention
9.The Galaxy-17-2016 with the MAC address 4c:02:20:e9:**:** is used for file sharing and portals.
10.The device model is HUAWEI Y9a Prime 2019 and its MAC address is 00:be:3b:f1:**:**.

Limitations of Wireless Network Connections

While wireless networks have undoubtedly increased our mobility, speed, accessibility, convenience, and connectivity, they are not exempt from limitations. These limitations are inherent in their artistic styles, vocal ranges, or other deficiencies they may possess. Read this material in its entirety to have a deeper understanding of the constraints associated with a Wireless Network.

Here are several limitations of a wireless network:

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 5.731
Volume 11, Issue 1, November 2021

The wired or cabled network enables significantly faster file sharing compared to the wireless network. Wireless networks are limited in their ability to transmit data due to physical and technological limitations. Wireless devices see a decrease in speed when the user goes farther away from the router or Wi-Fi source, in contrast to a cabled connection. The signal strength weakens, and in certain instances, even within a building, the router's signal may become unattainable. This could potentially result in interruptions in data and file transfers, as well as decreased transmission speeds when further away from the router.

Wireless systems can experience signal interference from common household items and interior structures such as refrigerators, window panes, walls, and ceilings. These elements have the potential to deflect or diminish the signals. This may adversely impact wireless systems.

● Establishing a wireless network can be challenging on occasion. This is particularly applicable to individuals who are uncertain or inexperienced with the utilization of wireless devices.

IV. CONCLUSION

In conclusion, wireless networking provides numerous opportunities to enhance productivity and save expenses. Additionally, it alters the entire laptop security risk profile of a firm. While it may not be possible to entirely eliminate all risks connected with wireless networking, it is viable to attain a cost-effective level of security by employing a scientific approach to assessing and managing these risks. This study examined the risks and weaknesses associated with the three main technical elements of wireless networks (clients, access points, and the transmission medium). It also explored various readily accessible solutions that can be utilized to mitigate these risks.

It also highlighted the importance of providing training and education to users on secure wireless networking techniques. Public Wi-Fi can offer numerous advantages; however, it also presents certain risks and worries. VPNs and encrypted connections are the most effective options for ensuring your security when using public networks. Wireless communication has the capacity to enhance overall communication. Nevertheless, there are other technological challenges that need to be resolved.

An individual pie chart query is typically straightforward and uncomplicated for categorizing information. We merely examine each component and determine the percentage that each segment represents. This is a fundamental concept, and you will see that there is one section that is the largest and one that is the smallest. Based on the survey findings, it was found that ty students exhibit the highest level of interest in public wife networks, whilst fee students display the lowest level of interest.

REFERENCES

[1]. Ali, S., Osman, T., Mannan, M., Youssef, A. :On privacy risks of public WIFI captive portals. In: Data Privacy Management, Cryptocurrencies and Blockchain Technology, pp. 80-98 (2019).

[2]. (PDF) Privacy Issues of Public Wi-Fi Networks (researchgate.net)

[3]. Cisco, V.: Cisco visual networking index: Forecast and trends, 2017–2022 White Paper, vol. 1 ,p. 1 (2018)

[4]. Fang, Z., Fu, B., Qin, Z., Zhang, F., Zhang, D.: Private Bus: privacy deification and protection in large-scale bus Wi-Fi___33 system in: Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies, vol. 4 , pp. 1–23 (2020)

[5]. Cheng, N., Wang, O., Cheng, M., Prasant, S., Aruna, : Characterizing privacy leakage of public win networks for users on travel. In: 2013 Proceedings IEEE INFOCOM, pp. 2769–2777 (2013)

[6]. Sumatran, N., Kad Obayashi, Y., Sasse, M., Baddeley, M., Miyamoto, D.: The continued risks of unsecured public Wi-Fi and why users keep using it: Evidence from Japan. In: 2018 16th Annual Conference on Privacy, Security and Trust (PST), pp. 1–11 (2018).

[7]. Klarna, P., Consalvi, S., Jung, J., Greenstein, M., Le Grand, L., Powledge, P., Wetherall, D.: When I am on Wi-Fi, I am fearless privacy concerns & practices in everyday Wi-Fi use. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, pp. 1993–2002 (2009)