SECURING AIRWAVES (PUBLIC WIFI)

SEMINAR REPORT

Submitted for the partial fulfillment of the requirements for the award of the degree of

BSc CYBER FORENSIC

MAHATMA GANDHI UNIVERSITY

KOTTAYAM – 686560

(2021 – 2024)

Submitted by

Gilby Babu

Reg. No: 210021042975

Under the Guidance of

Mrs. Meenu Poulose

ILM COLLEGE OF ARTS AND SCIENCE

METHALA, KEEZHILLAM P.O, PERUMBAVOOR

MAHATMA GANDHI UNIVERSITY KOTTAYAM-686560

ILM COLLEGE OF ARTS AND SCIENCE

METHALA, PERUMBAVOOR

BONAFIDE CERTIFICATE

Certified that the seminar entitled ***"SECURING AIRWAVES (PUBLIC WIFI)"*** *is a bonafide work done by* ***Gilby Babu (Reg.No.210021042975)*** *in partial fulfillment for the requirements for the award of the degree of BSc Cyber Forensic.*

Mrs. Meenu Poulose	**Mr. Ajas E M**	**Prof. George Cherian**
Seminar Guide	**Head of Department**	**Principal**

Submitted for the Viva-Voce Examination held on …….

Internal Examiner	**External Examiner**
……	**……**

DECLARATION

I hereby declare that this project work titled **"SECURING AIRWAVES (PUBLIC WIFI)"** is a record of original work done by us under the guidance of **Mrs. Meenu Poulose**, Assistant Professor, Department of Computer Science, ILM College of Arts and Science, Methala, Perumbavoor and this seminar is submitted for the partial fulfillment of the requirements for the award of degree of BSc Cyber Forensic of Mahatma Gandhi University, Kottayam.

Place: Methala
Date: Gilby Babu

ACKNOWLEDGEMENT

At the culmination of the study, I would like to express my sincere thanks to all who have helped in the completion of the study in different ways. If words are considered as symbols of approval and token of acknowledges then let the word play the heralding role of expressing my gratitude.

First and foremost, I wish to express our profound thanks and gratitude to **Prof. George Cherian**, Principal, ILM College of Arts and Science, Methala, Keezhillam P.O, Perumbavoor, for the guidance and encouragement given during the course of the study. I would like to thank **Mr. Ajas E M**, Head of the Department, Department of Computer Science for his inspiring and commendable support throughout the course and seminar.

I would like to extend our sincere feeling of gratitude to **Mrs. Meenu Poulose**, Assistant Professor, for her valuable guidance and assistance at each stage of this seminar work. I would like to thank all staff members of Computer Science Department for their valuable suggestion and help during course of study. I express our sincere thanks to our parents and friends those who had provide all the support both directly and indirectly.

SECURING AIRWAVES
(PUBLIC WI-FI)

CONTENTS

ABSTRACT

1.1 ABSTRACT

Wireless local area networks are becoming more and more common in the modern world, which is powered by technology and network connections. People are using public WIFI in bus stop, airport, railway station etc. A wireless technology called WIFI enables devices to such as computer, laptops, smart phones to interface with internet to exchange the information with each other. WIFI can be good application for IOT (internet of things) devices. Nowadays, people being almost depend on ECAST, ecommerce. People are quiet interested in using the free WIFI, which could be inconvenient for their privacy. Weak security exists on public WIFI. HTTPS internet traffic using TSL (transport layer security) and is encrypted to given data privacy. By using public WIFI we are simply leaking our privacy. The main objective of this paper is to study the way of data leakage using brute force, WPS pixie attack, krama attack, DOS (denial of services), malware attack. To increase the privacy and reduce the leakage of data process like VPN (virtual private network), increase bandwidth, increase space, fire wall security would be implemented.

INTRODUCTION

2.1 INTRODUCTION

In recent years, technology and network connections have made it possible for more individuals to use the internet, which is a tool that is crucial for daily work. A WIFI is a wireless network protocol that is often used for Internet access and device local area networking. The IEEE 802.11 set of specifications forms the foundation for Wi-Fi. Nearby digital devices may communicate with one other via radio waves thanks to Wi-Fi. These are the computer networks that are utilized the most throughout the globe. In order to link desktop and laptop computers, tablet computers, cellphones, smart TVs, printers, and smart speakers to a wireless router so they can access the Internet, they are used in home and small business networks on a worldwide scale. In wireless access points to provide mobile devices with access to the public Internet in public places including coffee shops, hotels, libraries, and airports. Accordingly, a recent survey indicated that 70% of tablet owners and 53% of smartphone and tablet users, respectively, claimed to have utilized public Wi-Fi hotspots. This suggests that everyone interested in using public Wi-Fi is exposing our privacy in the process. However, as data shared over public Wi-Fi may be readily intercepted, many mobile device and laptop users are endangering their private information, digital identity, and money. Additionally, if their computer or device is not protected by an effective security and anti-malware application, the risks are greatly increased. It's a convenient way to check your emails and stay up to date when you're on the move. social media or use the internet. But con artists regularly snoop on public Wi-Fi networks and eavesdrop on information flowing across the connection. This gives the criminal access to the passwords for users' accounts, their financial information, and other data. social media or use the internet. But con artists regularly snoop on public Wi-Fi networks and eavesdrop on information flowing across the connection. This gives the criminal access to the passwords for users' accounts, their financial information, and other data.

WHAT IS PUBLIC WIFI?

3.1 WHAT IS PUBLIC WIFI

Public Wi-Fi, also known as “open Wi-Fi”, is relied upon by individuals needing an internet connection while out and about. It's common in coffee shops, hotels, airports, and other public places. Public Wi-Fi may be free, but security costs can be high.

A public network is a type of network wherein anyone, namely the general public, has access and through it can connect to other networks or the Internet. This is in contrast to private network, where restrictions and access rules are established in order to relegate access to a selectfew.

PUBLIC WIFI SECURITY CHALLENGES

4.1 Application Layer

The caching, scheduling, and transcoding of video traffic are the primary goals of application-traffic-based optimizers. Statistics and user behavior analytics are simply two applications of an application-based optimizer's architecture. These technologies are employed to build a transparent network of traffic classifiers, load balancers, and the functionality of the application itself. There isn't a standard TCP/IP solution available that Network/transport layer caching and explicit HTTP proxies can communicate with one another. the application layer has problems. Therefore, HTTP/2 is designed to address the present Implementation Difficulty However, this will lead to more issues brought on by the requirement for difficult encryption Knowing application specific features in any of the various network interfaces is an option for establishing interoperability at the new apps, which are developed so they may connect with the "Application layer." the elements that influence switching choices. Every time a socket is opened, the programmed code needs to be updated in order to link the socket to the interface specified by the application. The switching module is used, not the normal interface. Security providing to application-level interoperability is essential to protecting the data of numerous apps. Applications will frequently provide the user with a variety of sensitive services, all of which need to be protected from intrusion. In order to provide comprehensive application-level security that is compatible with a range of networking technologies, new application-level security protocols are being created as part of the standardization of the Internet

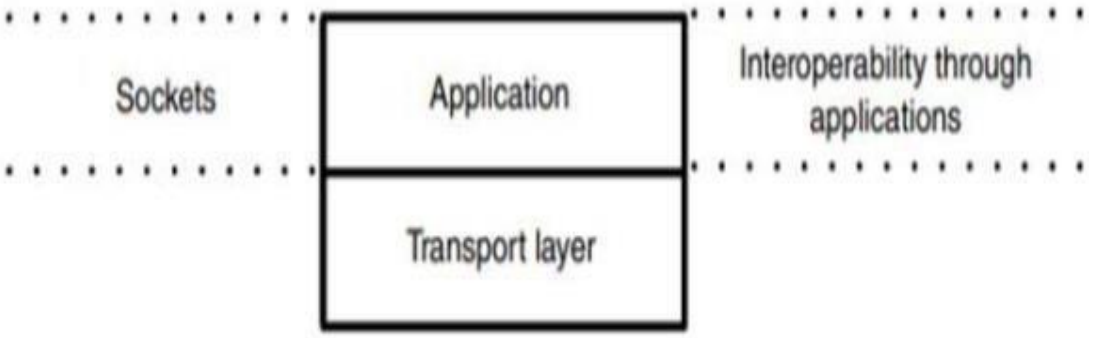


Figure: WiFi interoperability at application layer

4.2 Transport Layer

Maintaining end-to-end TCP connections when switching between various interfaces is the main challenge in establishing interoperability at the transport layer . A TCP connection is made up of four tuples: Source IP, Source Port, Destination IP, and Destination Port. Since different network interfaces have different IP addresses, switching the network interface will sever the end-to-end TCP connection. Redirectable Sockets, often known as RedSocks, are one solution for such issues. With pTCp [10], smooth interoperability at the transport layer can be achieved by aggregating bandwidth, which is done by stripping data across the several TCP connections. Using current TCP proxies, mobile carriers modify network performance to meet desired needs. End-to-end TCP congestion control is currently unable to span heterogeneous networks (cellular and wireless networks). This is due to increased packet loss and end-to-end latency. Furthermore, it is crucial to stress that TCP-based solutions now in use are ineffective especially in mobile networks where the system is actually intended to provide virtual-circuit-like functionality. Therefore, due to significant buffering, variable latency, a lack of AQM, and congestion notification, regular TCP will perform worse in 5G networks. One solution to this issue is to use TCP proxies, which can lower the performance cost of interoperability problems. Additionally, security at the Transport layer interoperability For connection-oriented (TCP) or connection-less (UDP) end-to-end data transmission between the source and the destination, it is crucial to provide the application with data security. The security of transport layer protocols that provide end-to-end service to multiple applications is essential for transport layer interoperability. The introduction of TLS in HTTP/2 will lead to the rapid adoption of end-to-end encryption at the Transport layer

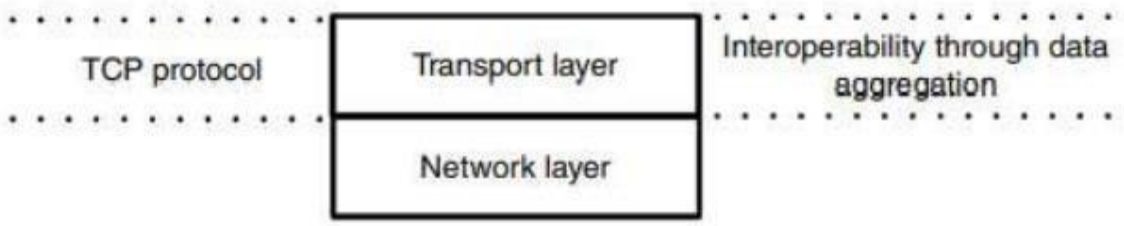


Figure: WiFi interoperability at transport layer

4.3 Network Layer

Existing networks, both wired and wireless, heavily depend on Internet technologies (IP-based networks). A substantial amount of additional hardware must be built in order to support the functions of non-IP based networks. Let's examine a mobility management example. In order to provide "seamless connectivity," 4G networks are deploying an anchor point-based mobility approach through tunnelling. This can be accomplished via proxy-MIP- or GTP-based technology. This type of solution's centralized design suffers from the usual efficiency, scalability, and security problems. As a result, work on creating novel solutions to satisfy the needs of internet access, such as Selected Traffic Offload, began. The most prevalent use case for mobile Internet connectivity is outlined in [9], and it is not required to have perfect IP connectivity. A challenge to achieving interoperability at the network layer is the maintaining of a single static IP address (IPv4 or IPv6) for the mobile device across several network interfaces. The concept of optimized Mobile IP allows for the creation of a single mobile device with a static IP address. A mobile device is considered to have left the home network and entered a foreign network each time it switches to a new network interface. It is easy to ensure that a "source IP address" is used to provide end-to-end communication employing encapsulation and tunnelling. However, both Wi-Fi APs and cellular BSs need to support Mobile IP protocol for this strategy to function (tunneling and encapsulation at Foreign Agents). Protecting the security of L3 data is crucial for interoperability at the network layer (IP packets). Mobile IP, a network layer technology, provides global Internet connectivity using IP-in-IP encapsulation and L3 tunnelling. A thorough security architecture has been created by contemporary research to protect L3 data using IP security (IPsec). Using mobile IP with IPsec is one way to secure application data (IP packets) at the network layer. Optimized Mobile IP is made to select the optimal packet traversal path between source and destination. A mobile device could be made using the concept of optimized Mobile IP. It is considered to have left the home network and entered a foreign network once it switches to a new network interface. Utilizing tunnelling and encapsulation makes it straightforward. It is necessary to guarantee the use of a "source IP address" for end-to-end communication. However, for this strategy to function, both Wi-Fi APs and cellular BSs must support the IP protocol for mobility (tunneling and encapsulation at Foreign Agents).

Protecting the security of L3 data is crucial for interoperability at the network layer (IP packets). Universal and Anywhere Internet connection is provided by Mobile IP, a network layer protocol, via L3 tunnelling and IP-in-IP encapsulation. Modern research has created a thorough security strategy to deliver the IP security that safeguards the L3 data (IPsec). Mobile IP is one way to provide network-layer security for application data with IPsec (IP packets). The goal of Optimized Mobile IP is to select the best packet traversal path between the source and the target location.

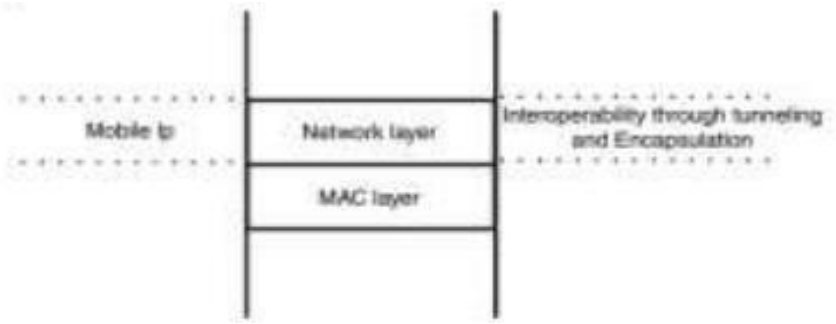


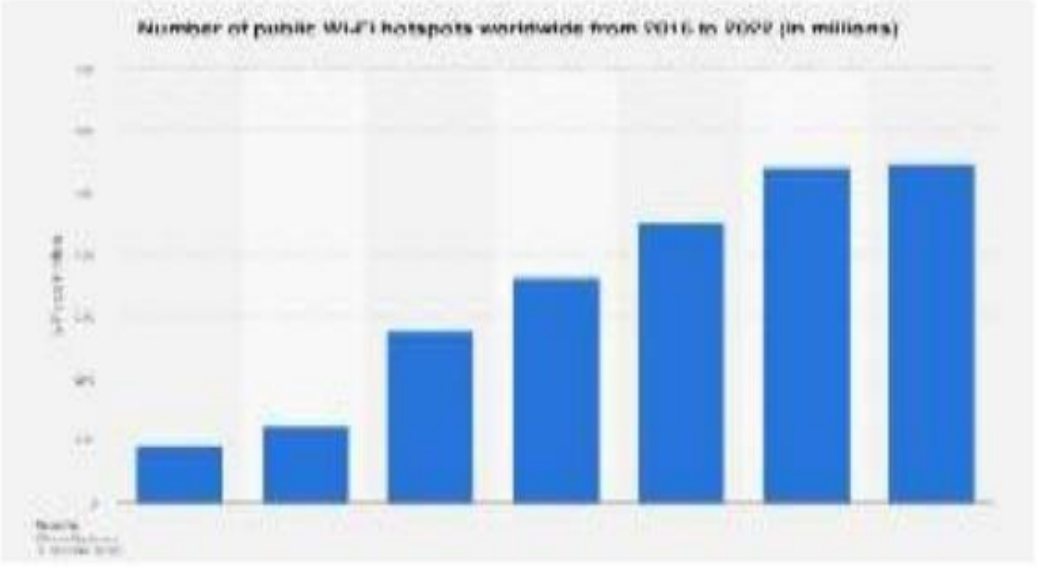
Figure WiFi Interoperability at the Network Layer

4.4 MAC Layer

AMAC is a member of the Adapt Net protocol family. Here is a two-layered MAC protocol that can let cellular and wireless networks communicate with one another. The master sublayer equivalent of a virtual cube. modifying the module to offer user-based interoperability. It is essential to guarantee the security of the application data when switching between packets (or frames) of different connection technologies (Wi-Fi). Protect the data from intruders. Generally speaking, changing the data is easy for hackers. when it comes to interoperability, the L2 packet switch needs to be able to communicate with a variety of technology protocols. Consequently, to ensure application data protection at "Network Interface" switching, it is critical for network designers to consider MAC level interoperability security considerations

METHODOLOGY

The Indian Government, as well as Governments throughout the world, have launched plans for providing public Wi-Fi because they recognize the internet as a necessary tool for day-to-day work and have made it easier for people to use it in recent years]. However, privacy hazards associated with utilizing public Wi-Fi have also been raised nationally and will be covered in this study. This case study aims to analyze the privacy policies of two Internet service providers in India, Tata Docomo and D-VoiS, which provide public Wi-Fi services in Bangalore city against the indicators listed under the Ranking Digital Rights project[4], as well as the Information Technology (Reasonable security practices and procedures and sensitive data) [Reasonable security practices and procedures and sensitive data] [Reasonable security practices and procedures] [Reasonable security practices and procedures and sensitive data Rules, 2011 (personal data or information) (personal data or information) [5. Based on this analysis, this paper will provide significant recommendations for these ISPs to adhere to in order to guarantee sound privacy policies and practices and to build a framework and ecosystem that are balanced with respect to crucial privacy considerations, particularly those related to public Wi-Fi.



SECURITY ISSUES FACED BY PUBLIC WI-FI

Security Issue Type	Security Issue Description
Interception	By intercepting information through control and data signalling without altering or erasing it, the attacker violates the victim's right to privacy, which is violated by both the subscriber and the network operator
Reply attacks	Depending on the objective and type of physical access, the intrusion could bring bogus things into the system (such phoney messages). erroneous subscriber data or incorrect service logic
Data leakage	The intruder uses open entry points to collect private information. the specific user data
Analysis of the traffic flow	The intrusive party records the length, rate, time, source, and destination of the traffic flow in order to ascertain the user's location.
DOS attack	An attempt to disable a computer system or network so that its intended users cannot access it is known as a denial-of-service (DoS) attack. DoS attacks do this by bombarding the target with traffic or data that makes it crash.
Brute force attack	Application applications utilise a brute-force attack as a trial-and-error technique to decode encryption keys and login information in order to use them to enter systems without authorization. It is exhausting to use brute force instead of using intelligent techniques.
DDOS attack	A DDoS attack is a sort of cyberthreat that involves making excessive requests to a website or other online resource, which takes it offline. To exert this pressure, the attacker makes use of a sizable computer network, frequently by exploiting "zombie" workstations that malware has taken control of.
Traffic jamming	The intrusion attempts aggressively utilize the WLAN's bandwidth.to overwhelm legitimate traffic with false messages, through transmissions with a high radio frequency. These types of assaults fall into this category: Spam attacks: By flooding with spam, the intrusive party will using wireless communication networks to spread spam. Attacks using denial of service (DoS): the intrusive party prevents the legitimate User traffic is flooded with high frequency to reach the receiver. radio transmissions or phone communications;
MAN IN THE MIDDLE	Man-in-the-middle (MiTM) attacks on computers include the attacker covertly intercepting and relaying communications between two parties who think they are communicating directly to one another. When someone is assaulted, they are eavesdropping in the sense that they hear what is being said and then have complete control over it.
Network injection	Packet injection is a term used in computer networking to describe the process of altering an existing network connection by creating fake packets that appear to be a regular part of the data stream (also known as forging packets or spoofing packets)..

Table-2 Based on methodologies used to cause the attack

attacks using service logic	The 5G communication's data is the target of the hacker. harming the system by altering, incorporating, or deleting the data stored there
data-based attacks	By simply assaulting the service logic of the various network pieces, the intrusive party seeks to do significant damage.
Message-based attacks	Stopping the flow of control and data transmission to and from the Wi-Fi network by integrating, swapping out ping, replaying, and other forms of attacking the Wi-Fi architecture.

HOW PUBLIC WI-FI NETWORK GET HACKED?

7.1 HOW PUBLIC WI-FI NETWORK GET HACKED

- EVIL TWIN ATTACK
- MAN IN THE MIDDLE ATTACK
- PASSWORD CRACKING ATTACK
- PACKET SNIFFING ATTACK
- SECURITY VULNERABILITIES/MISCONFIGURATION

7.1.1 EVIL TWIN ATTACK

- Setup malicious hotspots with trustworthy names.

STEPS:

1. Looking for right location
2. setting up Wi-Fi access point
3. Encourage victim to connect
4. Setting up a captive portal
5. stealing data

PROTECTION:

i) check warning notifications

ii) Disable auto connect

iii) Avoid login into private accounts

iv) multifactor authentication

v) use VPN and HTTP websites

7.1.2 MAN IN THE MIDDLE ATTACK

- Criminals break into network and eavesdrop on data as it travels between device and Wi-Fi

PREVENTION:

i) Use VPN

ii) WAP encryption

iii) public key pair authentication

7.1.3 PASSWORD CRACKING

- Use software that automatically tries huge volume of usernames and password.

TECHNIQUES

i) Phishing

ii) malware etc

TOOLS:

- John the Ripper
- Cin and Abel
- ophcrack,
- THC Hydra
- Hash cat
- Air Cracking

7.1.4 PACKET SNIFFING

- Capture data units sent across the network then unpack to extract individual login details, financial information etc.

PREVENTION:

i) Encrypting data

ii) Trusted Wi-Fi

iii) Scanning network for dangers.

METHODS:

* Password Sniffing

* DNS Poisoning

* JavaScript card sniffing

PREVENTION:

i) Adopt sniffer detection applications like Anti-sniff, Neper, ARP Watch, Snort etc.

ii) implement intrusion detection system

iii) Avoid using unsecured network

7.1.5 SECURITY VULNERABILITIES/MISCONFIGURATION

- Sometimes default router settings allow criminals to log in as admin, and can plant malicious software to device.

DANGERS OF USING PUBLIC WI-FI

8.1 DANGERS OF USING PUBLIC WI-FI

- Identity theft via online victim profiling
- Infecting your device with malware
- Stealing your passwords
- Snooping for confidential data
- Business Email Compromise
- Ransomware attacks
- Session Hijacking
- Taking over your online accounts
- Targeting you with phishing attacks
- Gaining remote control of your device

8.1.1 IDENTITY THEFT THROUGH ONLINE VICTIM PROFILING

- Hackers could easily discover enough information about you to create targeted cyberattacks.
- Hackers can snoop you over public Wi-Fi and discover:
    - Location data about where you've been recently.
    - Personal information such as your interests, job, and marital status.
    - Detailed financial information about your bank and credit accounts

How to keep your data safe on public Wi-Fi:

- Strong encryption
- Use a virtual private network (VPN) when connecting to any Wi-Fi hotspot**.**

8.1.2 INFECTING YOUR DEVICE WITH MALWARE

- It is easy for attackers to sneak malicious software (malware) into your device Scammers, can inject an infected ad into a seemingly safe website.
- Trick you into filling out a phishing form, or even fool you into installing a fake app that records everything you type

How to protect your devices against malware:

- Anti-malware
- VPN service

8.1.3 STEALING YOUR PASSWORDS

- Some hackers use specialized tools that search for passwords.
- Tools include
  - John the Ripper
  - Cain and Abel
  - ophcrack etc

For example, tech giant Cisco got hacked when an employee's personal Google account login credentials were compromised.

How to protect your passwords:

- A VPN will help hide your passwords from snooping scammers.
- It is also a good idea to securely store all of your credentials in a password manager.

8.1.4 SNOOPING FOR CONFIDENTIAL DATA

- Public Wi-Fi networks are notoriously vulnerable to surveillance by bad actors looking for sensitive documents such as confidential contracts, invoices, and two-factor authentication (2FA) codes.
- An online session over public Wi-Fi can lead to an NDA (non-disclosure agreement) breach or to endangering your colleagues' work.

How to keep your sensitive documents safe:

A strong cyber security suite that protects you and your employees is essential. So is avoiding sending, receiving, and talking about confidential information over open hotspots.

8.1.5 TAKING OVER YOUR BUSINESS ACCOUNTS (Business Email Compromise)

- In Business Email Compromise (BEC) scams, fraudsters target your work email and send fake messages pretending to be someone you know.
- They may ask you to change payment information or send wire transfer to fake "clients."

How to protect yourself:

- Scammers will spend significant time and money to try and trick you. It's essential that you learn how to tell if an email is from a scammer.
- Digital security education helps you become more cautious. It also trains you to develop safer reflexes, such as double-checking transactions.

8.1.6 RANSOMWARE ATTACKS THAT DISRUPT LIVES AND BUSINESS

- Cyberattacks against open Wi-Fi networks also seek entry points into data storage platforms. Once bad actors have access to your sensitive data, they can blackmail you for its release.
- Ransomware attacks grew 80% in 2022.

How to protect yourself:

- Don't log into sensitive file-sharing services over public Wi-Fi.
- Make sure you're using tools like a VPN to encrypt your data.
- Always keep a backup of your most important data somewhere safe, ideally disconnected from the internet Cyber criminals.

8.1.7 SESSION HIJACKING

- Malicious hackers take over the connection between your device and the website or app that you are using.
- This gives them the same rights that you have as a legitimate,logged-in user.

For example, they could break into an online store and use your stored credit card information.

How to avoid session hijacking:

- For safe online shopping, *never* store your credit card details in your online account.
- And for added security, choose an always-on, all-in-one protection plan that combines device and online security with identity and financial fraud protection.

8.1.8 TAKING OVER YOUR ONLINE ACCOUNTS (email, social media, etc.)

- Account takeovers happen when bad actors gain unauthorized access to your accounts and take full control of them.
- Financial institutions hardened their authentication measures, cybercriminals have been focusing on account take-over tactics that get around these measures, such as tricking you into providing 2FA codes.

How to protect yourself against account takeover fraud on public Wi-Fi:

- Always use a VPN to encrypt your data *whenever* you need to log into sensitive accounts (banking, online shopping, email, etc.).
- It also helps to know if your personal data including
  i) passwords
  ii) Social Security number (SSN) has been leaked in data breaches.

8.1.9 PHISHING ATTACKS

- Phishing is a form of social engineering attack that uses deceptive messages to get victims to release sensitive information. This can include passwords, authentication codes, documents.
- By hacking into Wi-Fi hotspots, attackers can intercept network traffic and inject phishing attacks in the form of phishing emails, text messages, and voicemails.

How to avoid phishing attacks over public Wi-Fi:

- Use a robust security solution like Aura that includes a VPN and antivirus protection.
- Keep your software up to date.
- Turn on multi-factor authentication (MFA), which confirms your identity via face ID, fingerprint, or one-time codes.

8.1.10 GAINING REMOTE CONTROL OF YOUR DEVICE

- In the worst-case scenario, hackers may even be able to infect your device with malware that gives them remote access — or control — of it.
- This malware is often hidden inside infected ads on websites that hacker's control**.**

How to protect your devices from remote access malware when on public Wi-Fi:

- Multi-layered digital security
- An ideal digital security suite *must* include five essential components:
    i) Device security
    ii) Data protection
    iii) Personal information monitoring
    iv) Expert support for guidance
    v) Identity theft insurance

HOW TO STAY SAFE ON PUBLIC WI-FI

9.1 HOW TO STAY SAFE ON PUBLIC WI-FI

- Before connecting to public wi-fi.
- While using public hotspots.
- After disconnecting from a public wi-fi**.**

9.1.1 Before connecting to public Wi-Fi:

- Turn on your VPN.
- Clear your browsing history and cache.
- Check that your antivirus is up and running.
- Turn off Bluetooth discoverability settings to avoid others forcing your device to connect to theirs.
- Make sure you've turned on two-factor or multi-factor authentication (2FA or MFA) for your most important accounts.
- Disable auto-connect to avoid having your device linked to public Wi-Fi networks

9.1.2 While using public hotspots:

- Only connect to networks offered by entities you can tie to a physical location.
- Log out of any account that you don't need to use while online.
- Close and/or quit applications that you don't plan on using.
- Store all your passwords in a password manager and use it to autofill your login data
- Avoid filling in sensitive information (passwords, credit card details, SSN, home address, etc.) while connected to public networks.
- Keep your list of saved Wi-Fi networks limited to only those you truly trust.

.

9.1.3 After disconnecting from a public network:

- Scan your devices for malware with antivirus software.
- Restart your device — This can help break the connection between it and a potential attacker.
- Purge networks you don’t need from your preferred network list.
- And, if you have the option, use your mobile hotspot instead of public Wi-Fi.

9.2 Ten ways to check if a Wi-Fi network is safe to use:

1. You’ve confirmed with the establishment’s owners that the name of the network you want to use is the one that *they* set.
2. You have to enter an annoyingly complex password to use it.
3. Your VPN is turned on and working.
4. Your antivirus software is up to date and running in the background.
5. Your antivirus has traffic and content filtering capabilities.
6. Your operating system, browsers, and other apps are up to date.
7. You’ve quit any unnecessary programs, tabs, and applications.
8. You’ve logged out of accounts you don’t need.
9. You’re using a password manager to automatically fill in your credentials and multi-factor authentication (MFA) for accounts that support this feature.
10. You have an ad blocker that works across browsers and apps.

TOOLS USED FOR HACKING WIFI

10.1 SOME TOOLS ARE USED TO HACKING THE WIFI

TOOLS	TOOLS FOR WIFI HACKING
Aircracking	Air crack-ng, a dangerous suite of tools used for wireless hacking, is well-known in today's online world. The utilities can be used with Linux and Windows operating systems. It's important to remember that Air crack-ng uses other tools to first gather data about its targets.
Wifite	Wep or WPA-encrypted wireless networks can be audited using the tool Wifite. The tools air crack-ng, pyrit, reaver, and tshark are used to do the audit. This programme can be automated and is trustworthy enough to operate unattended with just a few basic settings. Wep or WPA-encrypted wireless networks can be audited using the tool WIFI. The tools air crack-ng, pyrit, reaver, and tshark are used to do the audit. This application is dependable when used unattended and can be used to automate activities with a small number of parameters.
WIFI phisher	A security programme included in this package launches automated phishing attacks against WiFi networks in an effort to gather user credentials or secret passphrases. It is a social engineering approach that, in contrast to previous strategies, does not use brute force. It is a simple method for acquiring login information via captive portals, external login sites, or WPA/WPA2 secret passphrases.
nSSIDer	nSSIDer Office is a tool for optimising and debugging Wi-Fi. It looks for wireless networks with the aid of your Wi-Fi adaptor so you can examine their signal quality and channel usage. It also offers a lot of interesting information about each network.
Wireshark	Wireshark is capable of capturing any kind of data that is transmitted over a network, including usernames, email addresses, confidential information, pictures, videos, and anything else. As long as we are able to monitor network traffic, Wireshark can sniff the credentials that are being transmitted across the network.
Cowpatty	While auditing WPA-PSK or WPA2-PSK networks, this tool may be used to discover weak passphrases that were used to build the PMK. Give a dictionary file with potential passphrases, a libpcap capture file containing the 4-way handshake, and the SSID of the network.
Air crack	To assess the security of a Wi-Fi network, utilise the Air crack-ng toolkit, which is part of Kali Linux. It is capable of breaching, monitoring (by gathering packets), and attacking wireless networks. The password-protected WPA/WPA2 Wi-Fi network will be compromised using Air crack-ng in this post.
Airgeddon	An extensive menu-driven third-party tool wrapper for wireless network inspection is called Airgeddon.
omnviews	ommView for Wi-Fi is a popular wireless monitor and packet analyzer application. Its graphical user interface is simple to use. It works flawlessly with 802.11 a/b/g/n/ac networks. Every packet is recorded, and a list of the most significant data is displayed. You may receive crucial information such as access points, stations, signal strength, network connections, and protocol dispersion. To decode packets that have been captured, employ user-defined WEP or WPA keys. The main target audience for this product is software developers who are making wireless network software, Wi-Fi network managers, security specialists, and home users who want to monitor their Wi-Fi traffic.

CONCLUSION

11.1 CONCLUSION

When it comes to everyone, anything, and anything connection, security concerns are essential. The ISPs must have a strong Privacy Policy in place to satisfy the many worries people have about privacy and security when using public Wi-Fi. The Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011, requirements for the security of personal information, and improving the policies in accordance with those requirements will significantly contribute to protecting freedom of expression and ensuring the privacy of user information. Due to the growth of free and public Wi-Fi services in India, it is more crucial than ever to ensure adherence to the country's current data protection laws. This is because privacy and security issues are becoming more and more of a worry. Taking appropriate steps, such as getting consent before collecting the commitment of firm leaders to uphold individual rights, the adoption of security standards, raising public knowledge of security issues, etc. by such corporations must all be taken into account to secure the safety of personal information and lessen the possibility of a data breach. To achieve the standards established by the Ranking Digital Rights initiative and demonstrate dedication to the protection of users' rights to freedom of speech and privacy.

REFERENCE

1. Lee, J., Kim, J., & Seo, J. (2019, January). Cyber-attack scenarios on smart city and their ripple effects. In 2019 International Conference on Platform Technology and Service (Platicon) (pp. 1-5). IEEE.

2. Golbeck, J. (2020, October). User concerns with personal routers used as public Wi-fi hotspots. In 2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON) (pp. 571-576). IEEE.

3. Anamalamudi, S., Sangi, A. R., Alkatheiri, M., Muhaya, F. T. B., & Liu, C. (2018). 5G-Wlan security. A Comprehensive Guide to 5G Security, 143-163.

4. Oliveira, L., Schneider, D., De Souza, J., & Shen, W. (2019). Mobile device detection through Wi-Fi probe request analysis. IEEE Access, 7, 98579-98588.

5. Yeboah-Ofori, A., Islam, S., & Yeboah-Boateng, E. (2019, May). Cyber threat intelligence for improving cyber supply chain security. In 2019 International Conference on Cyber Security and Internet of Things (ICSIoT) (pp. 28-33). IEEE