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 o application-traffic-based optimizers. Statistics and user behavior analytics are simply tw applications of an application-based optimizer's architecture. These technologies are employe to build a transparent network of traffic classifiers, load balancers, and the functionality of th application itself. There isn't a standard TCP/IP solution available that Network/transport laye caching and explicit HTTP proxies can communicate with one another. the application layer ha 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 fo establishing interoperability at the new apps, which are developed so they may connect with th "Application layer." the elements that influence switching choices. Every time a socket i opened, the programmed code needs to be updated in order to link the socket to the interfac specified by the application. The switching module is used, not the normal interface. Securit providing to application-level interoperability is essential to protecting the data of numerou apps. Applications will frequently provide the user with a variety of sensitive services, all o which need to be protected from intrusion. In order to provide comprehensive application-leve security that is compatible with a range of networking technologies, new application-leve security protocols are being created as part of the standardization of the Internet

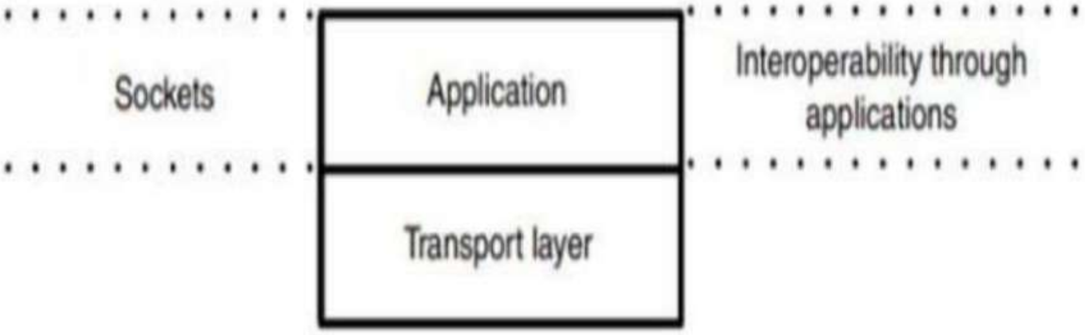

Figure: WiFi interoperability at application layer

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

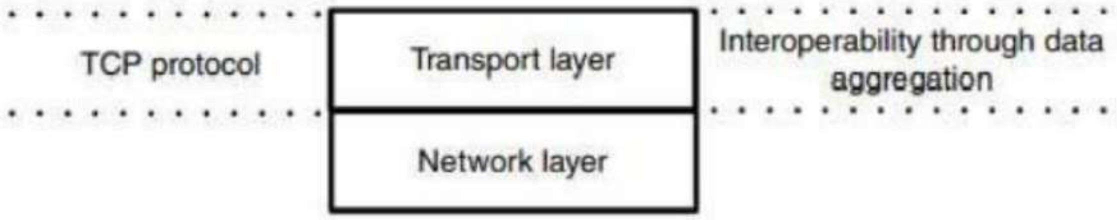

Figure: WiFi interoperability at transport layer

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.

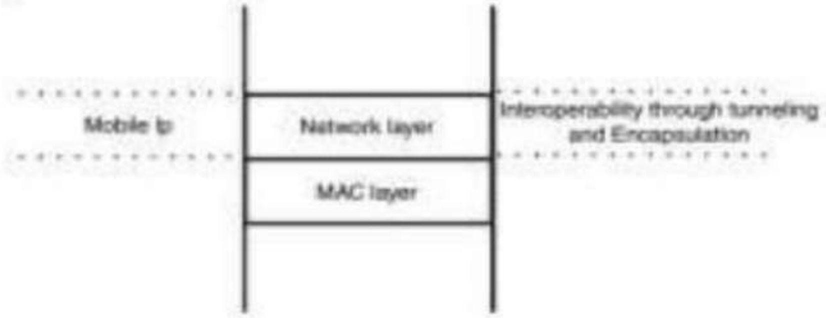

Figure WiFi Interoperability at the Network Layer

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