RUNNING HEAD: SECURITY IN PUBLIC WI-FI HOTSPOTS

Security in Public Wi-Fi Hotspots

Harish

[Name of the institution]

Table of Contents

[Literature Review: 3](#_Toc5366355)

[**Wired Equivalent Privacy in Wi-Fi Networks:** 3](#_Toc5366356)

[Flaws in WEP: 6](#_Toc5366357)

[**Wi-fi Protected Access (WPA):** 8](#_Toc5366358)

[Flaws in WPA: 10](#_Toc5366359)

[**Wi-Fi Protected Access Two (WPA2):** 11](#_Toc5366360)

[**Wi-Fi Protected Setup:** 12](#_Toc5366361)

[Methodology: 14](#_Toc5366362)

[Experiments: 17](#_Toc5366363)

[Results Analysis: 19](#_Toc5366364)

[Recommendations and Conclusion: 21](#_Toc5366365)

[References 23](#_Toc5366366)

Security in Public Wi-Fi Hotspots

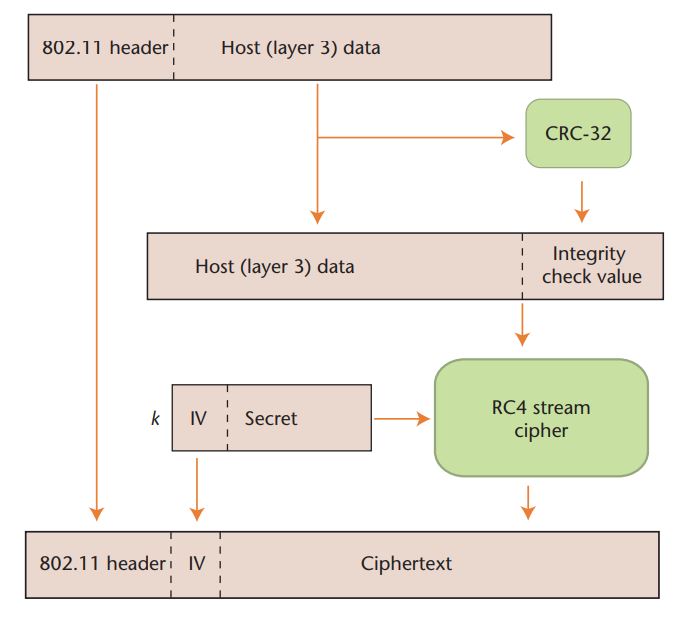
# Literature Review:

## **Wired Equivalent Privacy in Wi-Fi Networks:**

With the exponential increase in the popularity of Wifi networks, researchers are always trying to secure communication between client device and wireless access point in a wifi network. Attacks on wireless networks are not only increasing in number but in complexity as well. As wireless networks are prone to eavesdropping and man in the middle attacks it is inevitable to protect the confidentiality and integrity of the information being shared in such networks. One way of securing information in transit is to encrypt the data before transmission. Data encryption is an important step in securing communication not only in wireless networks but in all types of networks. As a general perspective, it was considered that a wired network is more secure as compared to the wireless network. In a wireless network, anyone can capture the signal and analyse it using specialized tools. Therefore, researchers started to look for different ways of securing wireless communications especially wifi networks using encryption. Encryption techniques have evolved over time.

The simplest example of an encryption algorithm is Caser cipher. In encryption, a cipher is applied to a plaintext message resulting in a ciphertext. In Caesar cipher, each letter of a plain text message is replaced with a corresponding third letter from English alphabets. Such as in a plain text message each "A" will be substituted with a "C". As in this case, the key of encryption is three as the letters are rotated up to three spaces. This is the simplest form of encrypting any message to ensure confidentiality. To retrieve the message exact procedure is need to be reversed resulting in original message form ciphertext. Such encryption schemes using the same key for encrypting and decrypting the data are known as symmetric encryption algorithms. More complex and sophisticated encryption algorithms have been designed and implemented to secure communication in wifi networks. The idea behind the use of encryption in wifi networks is to encrypt the data before sending it to the wireless access point. Researchers identified that mitigation of one security flaw in wireless networks often leads to a new security hole in the system that can be exploited by the attackers in future (A. Sanatinia et al., 2013). The idea of encrypting the information before transmitting it over an insecure wireless channel was considered to be a good step towards making wifi ecosystem more secure. However, any encryption system is as secure as the key associated with it because an attacker cannot extract the original message if the key of encryption is not known.

Implementation of encryption in wifi networks to provide wired equivalent privacy created other challenges of securing the key of encryption used to encrypt the data. Wired equivalent privacy (WEP) protocol was designed by Institute of electrical and electronics engineers (IEEE) as a standard when they discovered that wireless medium is shared between clients in wifi networks and privacy of one client can be easily breached by other clients sharing the medium. WEP was designed to protect the data at the link layer of the open system interconnection model. WEP was based on symmetric stream cipher known as RC4 to encrypt the network traffic in wifi networks (A. Sanatinia et al., 2013). WEP system works on the basis of a shared secret key that is transmitted to all of the connecting clients out of the band. Most of the times the preshared key or password of the wireless access point for authentication is manually shared between the participating nodes. Anyone not having the password cannot connect to the wifi network as it is currently applicable in modern day networks as well. Working of RC4 algorithm for wifi networks is explained in the figure below (A. Sanatinia et al., 2013);



*Fig: RC4 in wi-fi networks*

RC4 algorithm uses the pre-shared key to generate a stream of pseudorandom characters of equal size and perform a bitwise exclusive OR operation of that stream with the plaintext information producing the ciphertext. Due to the simplicity of implementation of the RC4 stream cipher, it was quickly adopted by the device and access point manufacturers and they started incorporating it into their devices. Almost 90% of modern devices and wireless access points currently deployed at public places still use the WEP protocol to secure the connection. However, as the algorithm is a symmetric algorithm so the sender and receiver must produce the same string of pseudorandom characters to decrypt and encrypt the information. That is considered to be the extreme weakness of the protocol as the same information will generate the same ciphertext for repitive conections as well (Watanabe et al., 2017). The fact provided an opportunity to the attackers to analyze a certain amount of network packets to figure out the key of encryption leaving the entire implementation of cryptography useless. To overcome the challenge, an initialization vector (IV) value was added in the WEP packet structure. WEP now use a 24-bit IV value along with a 40 to 104-bit shared secret to produce the key of encryption (Potter, 2003). IV value is transmitted by the sender along with the ciphertext packet so, that the receiver can generate the same key of decryption.

### Flaws in WEP:

It was considered at the time of implementation as a breakthrough in providing confidentiality to wifi networks but the attackers proved it wrong with their sophisticated attack methods. Dictionary attacks are considered to be the most common attack technique of hackers to compromise passwords of public wifi networks. However, modern attacks are known as brute-force attacks that are similar to dictionary attacks because the attackers are required to try a different combination of keys but using a vast collection of strings as compared to a simple dictionary attack. Inherent flaws in RC4 algorithm allowed the attackers to compromise any wifi hotspot using WEP encryption to protect the confidentiality of the data being transferred (Tews and Beck, 2009). By design WEP use an IV value of relatively small size that is 24-bits result in a total possible combination of 224 key values. An attacker can build a dictionary of all related keys for a single IV value in a manageable size of 40 Gbytes.

As early as in 2001, researchers explained the flaws in RC4 key scheduling algorithm allowing the attackers to compromise the network in significantly less time. An attacker only requires to intercept 4 million packets in a public wifi network using any wireless packet sniffing device to figure out the encryption key. The attacker will then have complete access to wifi hotspot without even knowing the exact password of the network. A breakthrough advancement in the research was made in 2008 when researchers were able to crack a 104-bits WEP encrypted connection in just three seconds (Reddy et al., 2010). The required number of packets can be captured in less than a second and the analysis can be performed to crack the encryption code in one second using a core i-7 intel processor for mobile devices. The requirement of minimal computing effort to compromise WEP connection has made it possible for attackers to compromise public wifi hotspots in real-time while walking through an area using a mobile phone. A paper was published by the Tews, Ralf-Philipp Weinmann and Andrei Psyhkin demonstrating the attack. They further elaborated that only 40,000 packets are required for a success rate of 50% and 85,000 captured packets can ensure a success rate of 95% (Tews et al., 2007).

Demonstration of flaws in RC4 implementation in WEP protocol convinced many device manufacturers to mitigate the risk of brute force and dictionary attacks on their access point devices. One method of mitigation was to filter the weak IV values form packets destined to the access point. The filtering operation for each packet subsequently reduced the efficiency of the wireless access point devices. As the vendors have now to choose between eth security and usability of their devices there exist a tradeoff between the security and usability of wifi devices for public hotspots. Some of the vendors decided to block a subset of IV values from being used in the network potentially giving rise to IV reuse and smaller dictionary size for attackers. This way, mitigation of one risk given rise to a more sophisticated risk more quickly as previously possible (Realpe et al., 2018). Given the fact that WEP is not an efficient protocol for providing the confidentiality and integrity of information, its use is not recommended. However, most of the public hotspot devices still use WEP encryption to secure the network, in fact making it vulnerable to a plethora of attacks compromising the confidentiality of data. Severe flaws in WEP forced researchers to design new and improved algorithms to secure public wifi as well as wifi networks in general.

## **Wi-fi Protected Access (WPA):**

Due to the flaws discovered in the initial wifi security protocol known as WEP, researchers spent a lot of time and money to develop new and sophisticated protocols to secure the wifi networks especially public wifi hotspots. Wireless protected access also known as WPA protocol was introduced as a replacement of WEP to overcome security flaws. WPA provides efficient key management as compared to the WEP protocol which does not provide any such facility. WPA was designed and introduced as a standard by wi-fi alliance (Abo-Soliman and Azer, 2018a). The technology was designed to ensure backward compatibility with existing devices supporting WEP protocol. A new protocol to encrypt the data was introduced known as the temporal key integrity protocol (TKIP). As it is evident by the name the protocol was designed to provide improved integrity along with the confidentiality of the transmitted data. The integrity of encryption keys is provided using hashing technology (Agbeboaye et al., 2018). A hash function is a function that operates on an arbitrary piece of information and generates a fixed length random value.

The strength of the hashing function lies in the fact that the original key cannot be reconstructed from a hash value of the key. An important quality of a hash function is that it must not compute same has value for two different input strings but must create the same has value for the same input all the time. If any hash function computes the same hash value for two different inputs then the problem is defined as a hash collision. TKIP also adds integrity checking feature to the data packet so, that it can be verified at receiver's end that the encryption key is not tampered with. TKIP is a hashing function widely adopted by the manufacturers of wifi access points as it does not require implementation of specialized hardware into existing designs (Wen and Liu, 2018). TKIP uses the RC4 algorithm for encryption and decryption but fortifies the process with a 128-bit key and IV value of 48-bits. The key of encryption is known as the temporal key and IV is used as a counter in transmission for packets. Therefore, the participating clients and the access point have to perform a 2-phase key generation that is known as a per-packet key also known as PPK.

WEP was lacking the facility of user authentication on the wifi access point. Whereas WPA provides authentication using extensible authentication protocol (EAP). EAP allowed the wireless access points to authenticate users of the network using the MAC address of the clients. As it was thought at that time that masquerading a MAC address is not an easy job, the implementation of EAP was regarded as a strong security mechanism in public wifi protection. Introduction of EAP and authentication features with the WPA technology allowed the administrators and access point to allow only authenticated devices to connect to the network. Although the feature can increase the security in a home network environment but useless in public wifi hotspots as it will kill the basic purpose of a public wifi hotspot (Esser and Serrao, 2018). Most of the time public hotspots are not managed by any system administrator. Even in case of a managed public hotspot controlled access will not be a manageable task regarding user authentication coupled with MAC address filtering.

### Flaws in WPA:

WPA was designed and implemented to support devices, previously configured for WEP security. Backward compatibility allows devices such as wireless access points to operate in a mixed mode to provide connectivity to the clients using WEP. However, in actual tests, it was discovered that the mixed mode provides only WEP equivalent protection to all users regardless of the configuration of the client device. Which effectively means that a public wifi hotspot advertised as supporting WPA security may not actually provide an enhanced level of security and privacy protection (Dawood et al., 2018). As TKIP itself is not an encryption protocol it just makes sure that each transmitted packet over the network must have a unique encryption key, the attacks against WPA are also successfully tested. Researchers discovered that breaking WPA encryption provides access to the information contained in the internet packet but it does not provide complete control of the network. It was discovered that an ARP packet captured from the public access network can be opened and decrypted in just 14 minutes. Although WPA provides a good feature set as compared to the WEP as it is difficult to control the entire network but the flaws in the protocol allow man in the middle attacks to be successful (Čisar and Čisar, 2018). Based on the findings researchers suggested to use the wifi routers for public wifi hotspots with the security level set to WPA-EAP instead of WPA-PSK. As the WPA-PSK mode is only recommended for home users with a preshared key mechanism of security.

## **Wi-Fi Protected Access Two (WPA2):**

To overcome security flaws discovered in the WPA protocol a new protocol based on different encryption algorithm was introduced in 2004, known as WPA2. In 2001, the national institute of standards in technology accepted advance encryption standard as a standard of encryption even for classified government communication as well. AES was introduced in place of the data encryption standard. With the new encryption standard for general purpose security, researchers decided to implement it into wifi networks for increased security and privacy. AES encryption was built into WPA2 in place of TKIP as found in WPA (Terkawi and Innab, 2018). AES encryption is much stronger as compared to the TKIP and DES encryption algorithms. It provides authentication of users based on transport layer security based on the extensible authentication protocol intended for enterprise and public wifi hotspots. It provides data integrity verification using counter mode cipher block chaining message authentication code protocol. It also operates in two modes WPA2-PSK mode is intended for home users because it requires a pre-shared key as it was the case with WEP and WPA previously (Azeez and Chinazo, 2018). WPA2 allowed the use of preshared keys with up to 64 ASCII characters. However, use of such a long passphrase is not feasible even in home networks because users will prefer usability instead of security if they are required to remember fairly long passwords for their network.

As with the case of public wifi hotspot security WPA2 offers server-side authentication using a RADIUS server. The security is based on an 802.1x industry standard that is introduced by the Institute of electrical and electronics engineers. WPA2 with AES encryption is considered to be the best security measure to ensure confidentiality and integrity of wifi networks not only in corporate environments but in public wifi hotspots as well (Dey et al., 2018). It provides 128-bit strong encryption that is not purely immune to attacks but requires a considerable amount of computing resources to break the encryption. The computing resources required to break WPA2-AES key are not currently feasible in real-world scenarios. There are no direct attacks reported by the researchers directly targeting WPA2-AES encryption key. However, insider attacks are possible even in a WPA2-AES secured network because a group transient key is broadcasted to each client connected to the network.

Therefore, a client already connected to the public wifi hotspot can compromise the security of other devices on the network but an intruder cannot directly have access to the network. Due to the possibility of having the same group key for one or more clients the network can provide an opportunity to an insider for ARP spoofing. ARP spoofing is a type of attack in which a device connected to the network send fake address resolution requests. Attacks can authenticate multiple IP addresses with a single target's MAC address. A successful ARP spoofing attack can bring the overall network down as well. In public wifi hotspots, an attacker can use ARP spoofing to initiate a denial of service attack (Abo-Soliman and Azer, 2018b). In which the access of legitimate users to the wifi router will be blocked due to the congestion on the network links created by the attacker (Gunawan et al., 2018). Despite having flaws in the security protocol implementation of WPA2, it is still considered as the most secure mechanism for public wifi hotspots.

## **Wi-Fi Protected Setup:**

Wi-fi protected setup is another security protocol designed to make wifi communications in enterprise and public hotspot environments more secure. It was also designed by the Wifi alliance in 2007. The standard defines two methods of authenticating devices with a wireless access point supporting the WPS protocol. The first method requires the use of a PIN code for device authentication and second requires a physical push button to be pressed on the access point to authenticate the device on the network (Zisiadis et al., 2012). Push button setup method is not provided in all of the devices supporting the WPS protocol. It also defines two out of the band authentication methods known as the use of universal serial bus devices and NFC tags. But these authentication methods are not used in common access point devices. Stefan Viehbock was a researcher who discovered severe vulnerabilities in the WPS protocol. The vulnerabilities make the brute force attacks a real problem in access points configured for WPS protocol.

Design flaws present in the WPS protocol allows an attacker to compromise the PIN code of the public wifi network. As it is the most suitable method for setting up a public hotspot using a wireless access point router. Push button standard cannot be used in public wifi hotspots. PIN code authentication mechanism of the WPS can be hijacked using social engineering tactics. In most of the practical scenarios, the PIN code will be publicly available and the attacker will not have to design a social engineering attack to obtain the PIN code (Petiz et al., 2013). As per the scenario, the PIN code is readily available to the attacker and the attacker can connect to the public hotspot. After successfully connecting to the network, the attacker may gain full control of the network and in the worst case scenario can re-flash the firmware of the wifi router. Re-flashing the public wifi hotspot router with a custom Linux kernel firmware will allow the attacker to intercept all of the traffic being routed through the access point. All of the logical measures will be useless in the prevention of these attacks (Orukpe et al., 2013). Any router with a malicious firmware installed allows the attackers to intercept voice over internet protocol calls as well, significantly breaching individual privacy. The primary motive of cyber-attacks in public wifi hotspots is to compromise the security and privacy of connected devices (A. Sanatinia et al., 2013). Attackers steal banking credentials and authentication credentials for various online platforms such as social media networks and then trade compromised credentials in dark web markets for monetary benefits.

# Methodology:

Cyber-attacks are turning into a profitable industry. The primary motive of cyber-criminals is to use information technologies for monetary benefits by employing illegal, often dangerous methods. Exponential penetration of mobile devices in human lives and reliance on social media have made it compulsory to have an active internet connection. The advent of wi-fi networks solved the connectivity problem of these mobile gadgets. Cloud computing era has created an enormous pressure on wifi networks and network service providers to ensure connectivity and minimize the service downtimes. Quality of service to maintain the requirement of high availability is managed through the introduction of public wifi hotspots. Originally the purpose of deployment of the public wifi hotspots was to facilitate the end users and to meet their connectivity requirements. As the internet itself was not designed with much security in mind, any service offered at the top of an existing infrastructure of the internet will be inherently insecure such as public wifi hotspots. As discussed in the literature review, public wifi hotspots pose a serious risk to the security and privacy of users while they are using the network.

Freemium model of public wifi hotspot service and the temptation of the public to use the service has made it a paradise of cyber-criminals. They are always on their toes to compromise public wifi networks as the valuable information that can be extracted by compromising a public hotspot is worth the effort for criminals. Moreover, it is not as much difficult to hack a public wifi router due to security design flaws as compared to hack a server having strict security controls. Public wifi hotspots provide a direct link of interaction with the public. Therefore, qualitative research methodology is best suitable to analyze the behaviour of people using public wifi hotspots and threats encountered by them. The methodology employed in the research study involves the analysis of published case studies and qualitative reviews of published qualitative reports providing insight into the threats experienced by the public hotspot users. Qualitative method is chosen for research as it provides granular visibility and maximum details of an event. It provides independence to the researcher analyzing a data source. If valuable information is not available via one source the researcher can freely choose another source of data providing valuable information about the issues. Experimental results are analyzed by various researchers from their qualitative publications to understand the broad range of targeted threats to public wifi hotspots and recommendations are made to make the public wifi ecosystem more secure in general.

A case study of public wifi network secured using WPS security by the researchers Amirali, Sashank, and Guevara revealed many flaws and their possible exploitation techniques. They conducted tests on public wifi networks in an urban area compromising of at least twenty public wifi hotspots (A. Sanatinia et al., 2013). All of the routers installed in public hotspots being studied were configured to use PIN code authentication with WPS security protocol. As per the previously discovered flaws in WPS security design such routers can be used in various forms of attacks such as the man in the middle attacks, phishing, DNS pharming etc. All of such attacks are possible due to the compromised firmware flashing vulnerability present in WPS protocol. During their study, they successfully flashed custom firmware in routers present in public wifi hotspots. Custom flash allowed them to analyze traffic being forwarded through the network. Majority of people connecting to such wi-fi networks use handheld devices such as mobile phones. Android is the most popular mobile device operating system was found to be installed in almost 85% devices connecting to the compromised access points.

Capturing all of the network traffic revealed that 8% of applications installed on android phones connected to the compromised access points were prone to man-in-the-middle attacks. Applications using transport layer security can be tricked into sending malicious traffic to other users even outside of the compromised network. They discovered that even an antivirus application installed on the mobile device can be tricked into accepting false security updates. They intercepted the communication of antivirus applications installed on the mobile devices and manipulated the received packets at the compromised router (Amirali Sanatinia et al., 2013). They forwarded the antivirus definition packets to the mobile antivirus applications and applications were fooled into accepting the packets as legitimate updates. The user ended up infecting their device with malicious code that can allow remote control of handheld devices as well while having a false sense of security (Leroy et al., 2011). The security application reported the user as their device is secure. The design flaw of WPS can be manipulated in many ways and allow direct control of not only the access point but the client devices as well.

In another study, researchers discovered many severe flaws in public hotspots. Most of the analyzed public wifi routers and access points were not configured for user authentication to provide simplicity and usability. As discussed in the literature, there exists a strong tradeoff between security and usability of any device. A device that is not connected to anything including the power source can be considered as more secure in comparison to a network connected device. On the other hand, the same device will be limited in functionality that it can provide to the user and will turn into a useless piece of the machine (Cheng et al., 2013). Therefore, security is about finding a unique trade-off between reasonable security without significantly compromising on the usability of the system. Security researchers deployed a wifi access point at a public place with port mirroring to their command and control server. All of the traffic from client devices was routed through their command and control server analyzing the traffic. They discovered that none of the connected clients was configured to use any type of encryption for data security. Packet contents were easily decrypted and analysed exposing vulnerabilities in connected mobile devices applications. It was hard for the attackers to decrypt packets transmitted from the laptop as they were encrypted using transport layer security (M. Li et al., 2016). There exists a unified opinion that public wifi networks no matter how secure they are claimed to contain severe vulnerabilities compromising privacy and security of connected clients.

# Experiments:

Experiments are an ideal way of understanding the situation in any particular scientific problem. During the research study to verify the claims of security vulnerabilities and threats to public wifi networks three limited experiments were performed. In one of the experiments, an open wifi connection was made available to the public without any requirement of user authentication. For simplicity purpose, all of the wifi access points were configured in the same public place with different SSID's broadcasted to nearby devices and with different security protocols of authentication. The goals were to identify what is the behaviour of the general public regarding the use of public wifi hotspot networks. All of the network through the access points was monitored using packet sniffers and a dedicated computer for software packet analysis. The first access point was configured for open connection and was configured to allow a maximum number of stations to be linked with the router (Santoso and Vun, 2015). The traffic was forwarded to a software configured router that was performing traffic analysis.

A controlled instance of the machine running the analysis program was also used to deliver a malicious payload to connected devices. It was a step taken towards measuring the security implementation of mobile devices using different operating systems. The method helped in identification of operating system vulnerabilities as well but most of the vulnerabilities were platform dependent. The largest number of connections were made to the open public wifi hotspot device leaving the other two devices. Ransomware payload was successfully delivered to the connected devices using man in the middle packet analysis and modification attack. Packet contents were changed and optimized for malicious attacks independent of the host application. In the case of the second wifi hotspot device WPA2-PSK encryption was used (Sathiaseelan et al., 2013). The key to connect with the wifi connection was also made public so, that people can configure their connections. Phishing, man in the middle traffic analysis, and malware spreading attacks were carried out using this network as well.

In the case of a third wifi hotspot, the access point was configured to use WPA2-AES encryption with extensible user authentication protocol. The access point was configured to warn the connected devices if they are not using the virtual private network. The goal was achieved by inspecting the received packets from the client device connecting to the network. The connection to the access point was not terminated even if the client device does not have the virtual private network available. The experimental setup was configured in this way to understand the behaviour of the general public regarding the use of free internet available to them in the form of public hotspots. User behaviour is an important factor in the security of any system either a public wifi network or a corporate network having strict security controls (Y. Li et al., 2016). Most of the time dangerous activity is initiated with the permission of user as the devices are not able to authenticate any forged request. The possibility of malicious activity cannot be completely ruled out as there are various techniques actively used by the criminals to make this happen. However, an informed decision will subsequently reduce the risk of compromised information even in public wifi networks.

# Results Analysis:

During the experimental stage of study three different types of access points were configured for the general public. The results of the experiments were completely in accordance with the reports studied in the literature review. As per the general public behaviour of using public wifi hotspots, there were many factors affecting the user decision. Most of the handheld devices of today such as mobile phones and tablet computers have high-speed cellular connections having third and fourth generation of network connectivity. However, people tend to connect to public wifi hotspots due to high speed and low price of free connectivity. Regarding laptops, there is a trend being popular between the device manufacturers that they have gradually removed the possibility of wired connections on laptops. Therefore, there is no other option for people than using a wireless connection such as freely available public wifi hotspot.

As in the case of the experiment, most of the clients were connected to the open network not protected with any type of authentication as similar is the case with almost 48%public wifi hotspots. It was due to the fact that most of the people do not bother to turn off their wifi connections on their devices even if they are not actively using the connection. Users of such devices are more prone to cyber-attacks associated with public wifi hotspots as compared to other users. During network analysis, all of the users having an automatic connection to the open access point were infected with adware (Hooper et al., 2016). Adware is a type of malicious software that tricks users into the installation of fake products and compromises the privacy of the user. Many users were using or checking their bank account details without even noticing that they are connected to an unknown network automatically. Banking credentials of the majority of users along with their personal messages sent from applications not supporting an end to end encryption were obtained.

Even if the devices were not configured to auto-connect to the available network all the time people preferred to connect to the open network. In comparison, almost 76% of devices were connected to the open wifi hotspot potentially allowing attackers to compromise their data. A low percentage of only 22% of users opted for the password protected network. Thus making their connections more secure as compared to the people using the open network. Their network communication was encrypted using transport layer security but the man in the middle attacks was still possible. As the initial authentication messages between the access point and the client device were intercepted by the attacker (Dalton et al., 2014). An attacker having such information can spoof the MAC address of the device and even breach the security of WPA network as well. Potential vulnerabilities of the protocol identified in literature were found to be completely exploitable with no fix or patch available to users.

Only a fraction of two per cent people connected to a secure network using WPA2 with AES encryption enabled. However, when they received warning that their connection is not secure and their information can be compromised by an attacker they immediately switched to open network. Therefore, the security and usability tradeoff altered the decision of the user in this particular case. User switched to a less secure network due to a poorly designed warning. Moreover, most of the mobile devices support software-defined access points. Any malicious actor can turn his device into a secondary or rogue access point for a wifi network in an attempt to harvest user credentials (Durbin, 2016). All these vulnerabilities and attacks combined to make the wifi infrastructure more insecure. As most of the common gadgets are being connected to the internet forming an internet of things without considering usable security we will be building an internet of threats instead of the internet of things.

# Recommendations and Conclusion:

The features that make a public wifi hotspot attractive to the users also make it paradise for cyber-criminals. Despite having a data plan for cellular broadband network connections, users still tend to use public wifi hotspots as they are usually provided free of cost. However, as per the research findings, a free public wifi hotspot is not entirely free. It is certainly free as there are no monetary fees associated with it, but the users have to pay through their security and privacy while using a public wifi hotspot. Public wifi hotspots devices often disable recommended security features to increase the usability for end users compromising the security and confidentiality of private data. Public wifi networks are prone to phishing, malware attacks, hacker attacks, DNS spoofing, phishing and spamming (Taha and Shen, 2012). All these threats and their corresponding tools are used by criminals to harvest personally identifiable information of users.

The only way of making public wifi hotspots safe to use is through following precaution and safe browsing habits. User education is inevitable to make public wifi hotspots secure enough to be used for the financial transaction. All of the public wifi hotspot routers must be configured for WPA2 with AES encryption to protect the confidentiality, integrity, availability, and non-repudiation of data. Although there are flaws in the WPA2 security protocol as well those flaws cannot be exploited by hackers with ease as compared to other security protocols. A simple way of securing a public wifi hotspot is to disable WPS on the access point (Srinivasan and Wu, 2018). Most of the modern devices are preconfigured to use WPS for ease of use. Unfortunately, some devices do not even provide a configuration option to turn it off. While deploying a public wifi hotspot device it must be disabled for WPS. Users must be advised to use virtual private networks while they are using public wifi hotspots. It must be ensured that information is being transmitted on a public wifi network using a secure sockets layer connection that makes it difficult for hackers to intercept the communication.

It has been observed that people keep there wifi connection active even if they are not using it. The problem with such configuration as it is explained in the experiments that it will connect to available networks regardless of their security condition. The security on public wifi networks is interrelated for the deploying person and for the users of the service as well. The person deploying a public wifi hotspot must make sure that it is configured for WPA2 with AES to ensure the security. On the other hand, the user must ensure the security of their device and must avoid the use of financial services while on public wifi networks. Those are the only recommended measures that can help in securing public wifi networks. Otherwise, public wifi hotspots are security and privacy hazards and must be avoided at all costs.

# References

Abo-Soliman, M.A., Azer, M.A., 2018a. Enterprise WLAN Security Flaws: Current Attacks and relative Mitigations, in: Proceedings of the 13th International Conference on Availability, Reliability and Security. ACM, p. 34.

Abo-Soliman, M.A., Azer, M.A., 2018b. Tunnel-Based EAP Effective Security Attacks WPA2 Enterprise Evaluation and Proposed Amendments, in: 2018 Tenth International Conference on Ubiquitous and Future Networks (ICUFN). IEEE, pp. 268–273.

Agbeboaye, C., Akpojedje, F.O., Okoekhian, J., 2018. SECURITY THREATS ANALYSIS OF WIRELESS LOCAL AREA NETWORK. Compusoft 7, 2773–2779.

Azeez, N.A., Chinazo, O.J., 2018. ACHIEVING DATA AUTHENTICATION WITH HMAC-SHA256 ALGORITHM. Comput. Sci. Telecommun. 54.

Cheng, N., Wang, X.O., Cheng, W., Mohapatra, P., Seneviratne, A., 2013. Characterizing privacy leakage of public wifi networks for users on travel, in: 2013 Proceedings IEEE INFOCOM. IEEE, pp. 2769–2777.

Čisar, P., Čisar, S.M., 2018. ETHICAL HACKING OF WIRELESS NETWORKS IN KALI LINUX ENVIRONMENT. Ann. Fac. Eng. Hunedoara 16, 181–186.

Dalton, C., Lioy, A., Lopez, D., Risso, F., Sassu, R., 2014. Exploiting the network for securing personal devices, in: Cyber Security and Privacy Forum. Springer, pp. 16–27.

Dawood, O.A., Hammadi, O.I., Asman, T.K., 2018. Developing a New Secret Symmetric Algorithm for Securing Wireless Applications, in: 2018 1st Annual International Conference on Information and Sciences (AiCIS). IEEE, pp. 152–158.

Dey, B., Vishnu, S.S., Swarnkar, O.S., 2018. An efficient dynamic key based EAP authentication framework for future IEEE 802.1 x Wireless LANs, in: Proceedings of the 2nd International Conference on Digital Signal Processing. ACM, pp. 125–131.

Durbin, M., 2016. Apparatus, method, and system for securing a public wireless network. Google Patents.

Esser, A., Serrao, C., 2018. Wi-Fi network testing using an integrated Evil-Twin framework, in: 2018 Fifth International Conference on Internet of Things: Systems, Management and Security. IEEE, pp. 216–221.

Gunawan, T.S., Lim, M.K., Kartiwi, M., Malik, N.A., Ismail, N., 2018. Penetration Testing using Kali Linux: SQL Injection, XSS, Wordpres, and WPA2 Attacks. Indones. J. Electr. Eng. Comput. Sci. 12, 729–737.

Hooper, M., Tian, Y., Zhou, R., Cao, B., Lauf, A.P., Watkins, L., Robinson, W.H., Alexis, W., 2016. Securing commercial wifi-based uavs from common security attacks, in: MILCOM 2016-2016 IEEE Military Communications Conference. IEEE, pp. 1213–1218.

Leroy, D., Detal, G., Cathalo, J., Manulis, M., Koeune, F., Bonaventure, O., 2011. SWISH: secure WiFi sharing. Comput. Netw. 55, 1614–1630.

Li, M., Meng, Y., Liu, J., Zhu, H., Liang, X., Liu, Y., Ruan, N., 2016. When CSI meets public WiFi: Inferring your mobile phone password via WiFi signals, in: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. ACM, pp. 1068–1079.

Li, Y., Zhou, L., Zhu, H., Sun, L., 2016. Privacy-preserving location proof for securing large-scale database-driven cognitive radio networks. IEEE Internet Things J. 3, 563–571.

Orukpe, P.E., Erhiaguna, T.O., Agbontaen, F.O., 2013. Computer Security and Privacy in Wireless Local Area Network in Nigeria, in: International Journal of Engineering Research in Africa. Trans Tech Publ, pp. 23–33.

Petiz, I., Rocha, E., Salvador, P., Nogueira, A., 2013. Detection of WPS attacks based on multiscale traffic analysis. Recent Adv. Commun. Netw. Technol. Former. Recent Pat. Telecommun. 2, 127–139.

Potter, B., 2003. Wireless security’s future. IEEE Secur. Priv. 99, 68–72. https://doi.org/10.1109/MSECP.2003.1219074

Realpe, L.F.E., Parra, O.J.S., Velandia, J.B., 2018. Use of KRACK Attack to Obtain Sensitive Information, in: International Conference on Mobile, Secure, and Programmable Networking. Springer, pp. 270–276.

Reddy, S.V., Ramani, K.S., Rijutha, K., Ali, S.M., Reddy, C.P., 2010. Wireless hacking-a WiFi hack by cracking WEP, in: 2010 2nd International Conference on Education Technology and Computer. IEEE, pp. V1-189-V1-193.

Sanatinia, A., Narain, S., Noubir, G., 2013. Wireless spreading of WiFi APs infections using WPS flaws: An epidemiological and experimental study, in: 2013 IEEE Conference on Communications and Network Security (CNS). Presented at the 2013 IEEE Conference on Communications and Network Security (CNS), pp. 430–437. https://doi.org/10.1109/CNS.2013.6682757

Sanatinia, A., Narain, S., Noubir, G., 2013. Wireless spreading of WiFi APs infections using WPS flaws: An epidemiological and experimental study, in: 2013 IEEE Conference on Communications and Network Security (CNS). IEEE, pp. 430–437.

Santoso, F.K., Vun, N.C., 2015. Securing IoT for smart home system, in: 2015 International Symposium on Consumer Electronics (ISCE). IEEE, pp. 1–2.

Sathiaseelan, A., Rotsos, C., Sriram, C.S., Trossen, D., Papadimitriou, P., Crowcroft, J., 2013. Virtual public networks, in: 2013 Second European Workshop on Software Defined Networks. IEEE, pp. 1–6.

Srinivasan, A., Wu, J., 2018. VOUCH-AP: privacy preserving open-access 802.11 public hotspot AP authentication mechanism with co-located evil-twins. Int. J. Secur. Netw. 13, 153–168.

Taha, S., Shen, X., 2012. A link-layer authentication and key agreement scheme for mobile public hotspots in NEMO based VANET, in: 2012 IEEE Global Communications Conference (GLOBECOM). IEEE, pp. 1004–1009.

Terkawi, A., Innab, N., 2018. Major Impacts of Key Reinstallation Attack on Internet of Things System, in: 2018 21st Saudi Computer Society National Computer Conference (NCC). IEEE, pp. 1–6.

Tews, E., Beck, M., 2009. Practical attacks against WEP and WPA, in: Proceedings of the Second ACM Conference on Wireless Network Security. ACM, pp. 79–86.

Tews, E., Weinmann, R.-P., Pyshkin, A., 2007. Breaking 104 bit WEP in less than 60 seconds, in: International Workshop on Information Security Applications. Springer, pp. 188–202.

Watanabe, Y., Iriyama, T., Morii, M., 2017. Proposal of WEP Operation with Strong IV and Its Implementation. J. Inf. Process. 25, 288–295.

Wen, Y., Liu, T., 2018. WIFI Security Certification through Device Information, in: 2018 International Conference on Sensor Networks and Signal Processing (SNSP). IEEE, pp. 302–305.

Zisiadis, D., Kopsidas, S., Varalis, A., Tassiulas, L., 2012. Enhancing WPS security, in: 2012 IFIP Wireless Days. IEEE, pp. 1–3.