Digital Innovations & Contemporary Research in SCIENCE, ENGINEERING & TECHNOLOGY
Vol. 8. No. 2, 2020

Article Citation Format
Afolabi S., Bello O. A. & Aweh O. (2020): Minimizing the Vulnerability of Transmitted Data in Wireless Local Area Networks Using Appropriate Security Protocols. Journal of Digital Innovations & Contemp Res. In Science., Engineering & Technology. Vol. 8, No. 2. Pp 11-28

Article Progress Time Stamps
Article Type: Research Article
Manuscript Received: 21st May, 2019
Review Type: Blind
Final Acceptance:: 11th June, 2020

Minimizing the Vulnerability of Transmitted Data in Wireless Local Area Networks Using Appropriate Security Protocols

Afolabi S., Bello O. A. & Aweh O.
Department of Computer Science
Afe Babalola University
Ado-Ekiti, Ekiti State, Nigeria
E-mails: psafolabi@gmail.com, boniyide@gmail.com, opaniaweh@abuad.edu.ng

ABSTRACT

Wireless local area networks (WLANs) transmission channels are vulnerable to man-in-the-middle related attacks. Meanwhile, it is enjoying a boom owing to the huge investments in them by businesses, homes and institutions angling to leverage their inherent benefits. In this study, it was observed that some businesses whose transactions depend substantially on their WLANs connected to the internet are apparently oblivious of their risks exposures to cyber related attacks. Majority also have a lukewarm attitude towards risks of cyber-attacks. Therefore, to demonstrate how vulnerable their transmission channels, and by extension their businesses, are to attacks, this study tested the relative levels of security provided by the two most popular WLAN security protocols of Wireless Equivalent Privacy (WEP) and Wi-Fi protected Access (WPA) (and its various modifications with encryptions) against the most used traffic types of Hypertext Transfer Protocol (HTTP), Domain Name System (DNS) and Internet Mail Access Protocol/Simple Mail Transfer Protocol (IMAP/SMTP) using a widely available, open source, easy to install and use packet sniffing tool (Wireshark). The results showed that the transmission channels were vulnerable to varying degrees for all protocols, but most importantly, it showed that particular protocols equipped with particular encryption schemes provided better security to designated traffic types. For example, while WPA-PSK (TKIP) provided better security for HTTP and DNS traffic types, WPA-PSK (AES) was the better option for SMTP/IMAP traffic types.

Keyword:: Wireless Local Area Networks (WLANs), WLANs Security Protocols, WLANs Traffic Types, Wireshark, Network Packet Sniffing.

1. INTRODUCTION

Wireless Local Area Network

Wireless local area network (WLAN) technology is experiencing tremendous growth which is mainly due to the increased bandwidth made possible by the IEEE 802.11 standard (Tom and Les, 2008, Rathod & Deepak, 2015). A WLAN is a group of wireless networking nodes within a limited geographic area that is capable of radio

communications. It is usually implemented as extensions to existing wired local area networks to provide enhanced user mobility (Frankel *et al,* 2007). A WLAN enables access to computing resources for devices that are not physically connected to a network. WLANs mainly operate over a fairly limited range, such as an office building or campus.

WLAN enables a user to connect to a local area network (LAN) through a wireless (radio) connection system that is governed by the IEEE 802.11 standards that provides for usage and security mechanisms required route data over vulnerable wireless medium (Latha & Vasantha, 2014). WLANs allow greater flexibility and portability when compared to traditional wired local area networks. Tom and Les (2008) articulates the benefits of WLAN to compass user mobility, rapid installation, flexibility and scalability. WLAN has two fundamental architectural components. These are the station (STA) and the access point (AP) (Frankel *et al*, 2007). While the STA comprises of computing devices with wireless network interfaces, the AP contains the components for performing the wireless-to-wired bridging functions in addition to other functions. AP's logically connect STAs with a distribution system (DS), which is mainly an organization's wired infrastructure.

Protecting WLAN Communication Channels

The protection of wireless network communication channels remains a great challenge partly because of the vulnerabilities inherent in providing users with wireless access to file sharing applications. The other causes can be ascribed to the absence of standard rules for matching provided security protocols to routed traffic types, and downright negligence on the part of some category of users of such networks. Ordinarily, numerous algorithms, certificates and protective mechanisms (including protocols) have been defined and adopted in providing security for WLAN. (Aleksandar *et al,* 2015).

WLAN Security Protocols

The main security protocols in WLAN are wired equivalent privacy (WEP), Wi-Fi protected access (WPA), and Wi-Fi protected access II (WPA2) (Thaier *et al*, 2012; Ezedin & Mohammed , 2007, Babita and Neha, 2016 and Vipin and Hitesh, 2014). And because WLANs are highly prone to attacks some designated measures are expected to be carried out to minimize risks. These measures are:

i. Using Authentication: authentication is used to ensure that only authorized users can access or make use of the wireless network. It involves the use of authentication or access control measures such as unique usernames and passwords. Sometimes additional schemes are added to provides a more reliable and secure authentication. For example, schemes that support authentication on a per-user, per-session basis or mutual authentication between the user and the authentication source are advocated.

ii. Checking For Rogue Access Points: this involves checking for rogue access points plugged in to the network jack to gain unauthorized access. Plugging rogue access points are grave security threats to WLANs whose access points are not properly configured. The process of checking for rogue access points is carried out using specific application/tools and a wireless computer or a special management appliance. They are used to collect data from access points by scanning for new wireless access points. It is often carried out by the network administrator

iii. Using Encryption: encryption is used to make sure that data is unreadable and is protected from the possibility of alteration as it is transmitted between an access point and a wireless device. Encryption requires that both the sender and receiver have a key to decode the transmitted data. Secured encryptions uses very complicated keys, or algorithms, that change regularly.

Preliminary Investigation and Findings

Adherence to these designated measures designed to minimize the risks of attacks by some categories of WLAN owners or users whose businesses can be classified as low to medium scale, was undertaken as a preliminary investigation in this study. This preliminary investigation was aimed at gauging the level of risks exposure awareness of these categories of users and it was accomplished through the administration of some simple structured set of questions. The population for this investigation was selected based on some predefined criteria. First, the members of the population were to be elites whose businesses, or some aspects of their businesses relied on the use of a WLAN. Second, the members of the population, were presumed to have some knowledge, no matter how vague, of cyber related attack risks. Third, for representation, the population was selected to cover a broad range of businesses or services spanning merchandizing, legal services, financial services, engineering services, survey/estate management services and medical services or clinics. And for ease of executing the preliminary investigation, locations with high concentration of the selected businesses, most of who actually shared the same building complexes as office were selected.

The investigation was straight forward. The presence of a wireless network was detected using a mobile phone, and the owners or managers, and in some cases, a few functionaries of some of the firms were approached to respond to a few questions. And the same set of questions were administered to those who obliged. The first question was on the setup of their local network, and its management. And the response to this question was expected. It was done by a third party, who invariably tuned it to run on only one security protocol for all traffic types, and the third party was responsible for fixing (managing) the network any time it had issues. The second sets of questions concerned the use of the network to access the internet, the common traffic types routed on the network and the conduct of sensitive internet based transactions on the network. The responses to these questions were expected as well. Virtually all the networks were connected to the internet, and sensitive internet based transactions like card not present payments and transfers were done regularly by some of the firms and their functionaries. And within the business confines, sensitive trade data and client or customer information (patient health information for clinics) are routed freely across the network.

The third set of questions were based on the second sets of questions and they were on their vulnerability to cyber-attack, the possibility of sniffing (stealing) client or customer or patient or payment card information from the network. The response to these questions was in the affirmative, but the succeeding questions on why no deliberate measures were put in place to check or prevent them from occurring was baffling. Ruefully, it reflects the mindsets of the owners, managers and functionaries of these businesses and indeed, majority of communication network users. There is this scary believe that it just cannot happen, apparently based on the belief that only the big firms are prone to attack.

The two core findings from this preliminary investigation are the absence of standard rules for matching provided security protocols to routed traffic types and downright negligence on the part of some categories of WLAN users. This outcome provided impetus to demonstrate the risk exposure of these category of businesses who route sensitive information and conduct internet based financial transaction using WLAN. And the study conducted this demonstration by using one of the most common and very easy to use network sniffing attack tool (Wireshark). The study then provided some guidelines for selecting security protocols based on traffic types, to minimize the vulnerability of the routed traffic to sniffing attack using the most used WLAN security protocols of Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA).

2. RELATED LITERATURE

WLAN Security Issues

WLAN is required to address various security concerns (Frankel *et al*, 2007). The core concerns being confidentiality, integrity, access control and availability. WLAN threats involves an attacker gaining access to the radio link between a STA and an AP or between two STAs, and it typically entails (Frankel *et al*, 2007):

I. Denial of Service: Attacker prevents or prohibits the normal use or management of networks or network devices.
II. Eavesdropping: Attacker passively monitors network communications for data, including authentication credentials.
III. Man-in-the-Middle: Attacker actively intercepts the path of communications between two legitimate parties, thereby obtaining authentication credentials and data. In the context of a WLAN, a man-in-the-middle attack can be achieved through a bogus or rogue AP, which looks like an authorized AP to legitimate parties.
IV. Masquerading: Attacker impersonates an authorized user and gains certain unauthorized privileges.
V. Message Modification: Attacker alters a legitimate message by deleting, adding to, changing, or reordering it.
VI. Message Replay: Attacker passively monitors transmissions and retransmits messages, acting as if the attacker were a legitimate user.
VII. Traffic Analysis: Attacker passively monitors transmissions to identify communication patterns and participants.

WLANs typically suffers from packet sniffing attacks. Packet sniffing involves monitoring packet that passes through the network using either a piece of software or hardware that examines the network traffic. Some packet sniffers have the ability to capture all incoming and outgoing traffic and packets (Inderjit *et al*, 2014; Anas, 2016; Praful & Sandeep, 2017).

There are so many commercial and non-commercial tools available for executing sniffing attacks. Ordinarily, packet sniffing is important in network monitoring to troubleshoot and to log network activities and traffic and they play an integral role in securing any network, hence they are also referred to as network analyzer or protocol analyzer (Charu *et al*, 2014). The sniffing process is divided into three steps (Inderjit *et al*, 2014; Anas, 2016; Charu *et al*, 2014), and the core components of packet sniffers are given by Aruna and Swathi (2016).

There are many packet sniffing tools. Some of them are as described as follows (Inderjit *et al* , 2014):

I. **Wireshark:** Wireshark is an open source packet filter and analyzer that has a rich set of filtering and sorting options (Charu *et al*, 2014). Wireshark is a tool that “understands” the structure of different networking protocols and is capable of capturing packets sent and received on the network and to decode such packets for analysis.
II. **Tcp-dump**: Tcp-dump is an open source sniffing/monitoring tool used for packet capture, network monitoring and protocol debugging. It is the oldest and most commonly used command line tool. It can be used to read live capture or already captured log file. The advantage of TCP-DUMP over other packet sniffers is that it can be used remotely and it has the least overhead. Hence it is preferred some users who like to work from a different network
III. **Nmap**: Nmap stands for network mapper. Nmap is an open source tool used to explore and audit networks. It can determine the hosts that are available on the network, the services enabled, the operating system running on the hosts, the type of firewalls put in place and many other aspects of the network using raw IP packets. Nmap is a command line tool. Besides its use for network scanning and monitoring, it is also a tool used by attackers for stealing personal information.

IV. **Zenmap**: Zenmap is similar to Nmap. It is an open source tool that is easy to use when compared to Nmap because it has a graphical user interface (GUI). The main difference between Nmap and Zenmap is that Nmap is a command line tool while Zenmap is GUI based. Zenmap stores and sorts all the information gathered from any scan performed and uses this information to build up a picture of the network. For example, a simple ping scan will display all the devices that are alive on a network.
V. **Kismet**: Kismet application is an open source wireless network analyzer that run on Linux, UNIX and Mac operating systems. Kismet is a passive sniffer used to detect any wireless 802.11a/b/g protocol complaint network, even when the network has a non-broadcasting hidden secure service set identifier. Kismet detects and logs the internet protocol (IP) range of any detected wireless network and reports it signal and noise levels. It can sniff data packet from detected network. Kismet can be used to troubleshoot and optimize signals strength for access points and clients, as well as detect network intrusions. Kismet runs on GUI mode so it is very easy to use.
VI. **Caspa**: Capsa supports most of the features of Wireshark as it runs on GUI. It assists the user in the specification and in the analysis of cryptographic protocols. Caspa provides an editor for protocol specifications and offers a quick loading procedure for the protocols specified in underlying protocol libraries. It also offers a convenient parsing procedure for user defined protocol specifications and it has a graph management tool that automatically generates and displays graphs. Caspa gives the user a fully mechanized analyzer that verifies secrecy and authenticity properties on a given graph and displays the results.
VII. **Ntop**: Ntop is a network traffic tool that provides information regarding the usage of the current network. Ntop provide information on the network status by displaying the list of the hosts that are currently using the network, their IP addresses and the traffic generated by each host.
VIII. **Dsniff**: Dsniff is a password sniffer and a network traffic analysis tool. It automatically detects each application protocol. Basically DSNIFF is a tool for auditing the network and for penetration testing.
IX. **Cain and Abel**: Cain and Abel is basically a password recovery tool for Windows operating system. It is used to recover passwords by sniffing the network. It can also be used to crack encrypted passwords using cryptanalysis or brute force attack. It is a powerful tool that helps to decrypt tough algorithms. Cain and Abel can also be used to capture and monitor the network traffic.
X. **Etherape**: Etherape is an open source packet filter and traffic analysis tool developed to be compatible with UNIX1. It displays the network traffic graphically in color-coded nodes linked with the most used protocols. When a node or link is selected a detailed information about the protocols and network traffic for that node are automatically generated and presented.

WLAN Security Protocols

WLANs faces common security threats, such as eavesdropping, injection of bogus messages, jamming, replaying attacks and Denial of Service (DoS) attacks (Nisbet, 2012). And to minimize or check the incidence if these attacks, security mechanisms and specifications are evolving into security protocols. The three most popular ones are highlighted next.

Wired Equivalent Privacy (WEP)

WEP was the first IEEE 802.11 specification attempted to provide security for wireless communication channels in 1999 by the Wi-Fi alliance. The primary aim was to make wireless networks as secure as wired local area network and not to achieve absolute security (Lashkari *et al*, 2009; Lashkari & Towhidi, 2009; Maple *et al*, 2006). The WEP project was aimed at providing access control to the network and message confidentiality/integrity. The WEP was flawed from onset owing to its one way authentication mechanism and the weak key used to implement its encryption scheme (Reddy *et al*, 2010; Maple *et al*, 2006). WEP is susceptible to passive attacks (based on traffic statistical analysis), active attacks (based on traffic injections and impersonation) and also dictionary-building brute force attacks.

Wi-Fi Protected Access (WPA)

Due to a number of apparent vulnerabilities in WEP, WPA was formally adopted in 2003 as the replacement. WPA was implemented as WPA-Pre-Shared Key (PSK), which uses keys of length 256bits, a significant change from the 64 and 128bit keys that were used in WEP implementations. Encrypted message integrity checks (MIC) were also incorporated in WPA to ascertain if an attacker had captured or altered data packets between the communicating node and the access point thus reducing the chance of a denial of service (DoS) and spoofing type attacks. The encryption algorithm was equally improved to the Temporal Key Integrity Protocol (TKIP) which supplied each connecting host with a much longer unique key that gets rotated at a configurable interval (Lashkari *et al*, 2009; Selim *et al*, 2006). TKIP uses a per-packet key, which dynamically generates a 128 bit key for each packet. Despite the significant improvements in WPA over WEP, WPA still had numerous vulnerabilities in its design. For example, it was proven that nearly all traffic going towards a WPA enabled WLAN client can be decrypted by using fragmentation and injection of an arbitrary amount of packets in the data stream.

Wi-Fi Protected Access 2 (WPA2)

WPA2 is the most recent of the wireless encryption algorithms and has been in existence since 2004. Also known as IEE802.11i-2004, it provides much stronger data protection and network layer access control than WEP and WPA (Li *et al*, 2011). One of its major significant changes has been the mandatory use of the Advanced Encryption Standard (AES) algorithm and counter cipher mode with block Chaining Message Authentication Code Protocol (CCMP), which together has replaced TKIP (Kolahi *et al*, 2011). WPA2 provides wireless security ranging from small home installations to government grade security on large implementations.

WPA2 by default provides support for WPA mechanism. It provides strong authentication and encryption support for both infrastructure and ad-hoc implementations. There is also support for key caching. A mechanism that reduces overheads on network nodes that are roaming between different access points. In addition, WPA2 supports pre-authentication, that is, it is capable of completing an authentication exchange between a wireless node and an access point prior to initiation of roaming. The security provided by implementing WPA2 is robust. This has been achieved by using an authentication services that uses a four-way handshake mechanism to authenticate wireless stations and nodes during the first stage of the communication process.

The increase in the use of wireless networks and the exponential growth in the use of mobile devices shows clearly that wireless technology is a very suitable means of communication amidst its security issues (Aruna et al, 2013). It can be blatantly stated that the most critical concern for WLANs is security. The justification for this position is articulated by Ajah (2014) who affirms that securing wireless networks is difficult because they consist of radio transmitters and receivers, and anybody can listen, capture data and attempt to compromise it. And to provide this elusive security in WLAN's, several security protocols have been developed to support authentication and encryption. Some of these security protocols are WEP, WPA, WPA2 and robust security network (RSN) (Vipin & Hitesh, 2014). However, the two most popular WLAN security protocols are WEP and WPA2 and selecting the appropriate security protocol that will not impair the performance of the WLAN at material points in time is a great challenge (Vipin & Hitesh, 2014).

This challenge stems from the complexity inherent in the task of modeling WLAN security protocols to gain better insight in to how security can be better addressed (Chao et al, 2011, Deepika, 2014). And current literature search has not provided a concise concrete or conceptual framework for evaluating the performance of WLAN security protocols in general or their performance with specific traffic types in particular. To achieve higher levels of security in WLANs, Aleksandar *et al,* (2015) believes that it is crucial to pre-evaluate the parameters that affect the security of the wireless network in the course of building a security model. This believe accords with the study of Nidal & Shadi, (2010) who provided a guide that tried to answer certain questions such as: what should be the right security level and network architecture for a particular network applications and particular type of users.

The findings of Pandikumar & Mohammed (2017) corroborates the earlier findings of Omar (2011) on the unreliability of WLAN WEP. Omar (2011) demonstrated the vulnerability of WEP protocol using the trio concerns of confidentiality, integrity and availability, and showed that an attacker can readily access a WLAN using WEP protocol. In addition, he also showed that an attacker could use the services supported by the WLAN with ease. He then canvassed for the addressing of these concerns as an approach to ensuring tighter security. Pandikumar & Mohammed (2017) on their own part showed that it was easier to break the security of WEP, in comparison to WPA and WPA2. And based on their findings, they recommended that if WEP cannot be avoided on a network the implementation of longer keys (128 bit) should be used for encryption to enhance its security. In an identical comparative analysis of WEP, WPA and WPA2 Saurabh *et al,* (2017) showed that WEP was the most vulnerable WLAN protocol.

On their part, Poonam & Brahmjit, (2014) thinks beyond just ensuring tight security in WLANs. Based on their knowledge of the role of algorithms and encryptions in secure protocols design, they expressed their fears about performance. And they proceeded to demonstrate the fact that there is always a tradeoff between the security capabilities of a protocol and network performance. In the study, they provided a quantitative analysis of the security strength and the overheads associated with each protocol, and showed that a robust security protocol can improve network performance.

Another dimension is introduced into the WLAN security protocols discuss by Saurabh e*t al*. (2017) who arges that owing to the various and diverse traffic types that WLANs are required to support, a multiplicity of security issues are bound to arise. And under this circumstances, those responsible for making the decision regarding which security protocol to use, have an onerous task that requires appropriate information for good decision making.

In another twist to the WLAN security protocols conundrum, Richa *et al,* (2015) are of the view that amidst the availability of strong and weak security protocols, it becomes increasingly difficult to provide security in a WLAN as the number of nodes increases. It is therefore apparent that the quest to improve security in WLANs, raise security awareness, and provide easy to comprehend and use security schemes for owners, managers and users of the technology, remains an active and highly desirable domain of study.

3. MATERIALS AND METHODS

The methodology adopted in this study was an empirical evaluation of the two core security protocols in WLAN for securing data transmission. The security protocols used were:

I. WEP (Wireless Equivalent Privacy)
II. WPA (Wi-Fi protected Access)

This security protocols were used to route the most commonly used traffic types used in wireless networks. These traffic types include:

I. Simple Mail Transfer Protocol (SMTP): this protocols is commonly used for mailing or email services
II. Internet Message Access Protocol (IMAP): this is the protocol used for retrieving messages from email servers. It works with SMTP
III. Hypertext Transfer Protocol (HTTP): this is the most commonly used protocol in web applications
IV. Domain Name System (DNS): This helps in providing a critical link between human users and internet locations by mapping host names to IP addresses.

To carry out this empirical investigation a packet analyzing/sniffing tool was used to execute the sniffing attack on a WLAN setup for this investigation. The specific tools used in this investigation includes:

I. Wireshark: version 2.6.3 (v2.6.3-0-ga62e6c27) network protocol analyzer. The choice was informed by its ease of access and use. And the intent was to highlight how a readily available tool could be used with ease to breach the security of the WLANs of most businesses (who take security for granted) heavily dependent upon.
II. Router (TP-link TL-MR3220): this was used to propagate the WLAN environment and to implement the security protocols to be evaluated in this study. The two main security protocols were supported by the router which made it the selected choice for this study.
III. Computer Devices: this comprise of three computers. Two of this computers were configured to route traffic while the third device was configured as the attacking device/computer.

Experiment scenario setup

Table 2 shows the detailed specification of the hardware used to setup the stage for the experiment while Table 3 depicts the detailed computer systems configurations and protocols specifications

Table 2: Detailed Specification of the Hardware Used to Setup the Experiment

WLAN Client and Attacking Devices Specifications	
Network card	Integrated10/100BAS
Wireless connectivity	802.11b/g/n (1*1)
Access point / Router Specification	
Supported Security features	AES encryption, TKIP, WEP, WPA-PSK,WPA2-PSK
Model Name and Number	TP-Link TL-MR3220
Standards	IEEE 802.11 b/g/n
Frequency range	2.4GHz
Coverage range	250 meters

Table 3. Detailed Computer Systems Configurations and Protocols Specifications

Configuration of Computer Systems (Client Devices)	i. Client device A: (Windows 10 Pro, Intel Core i3, 2.4Ghz, 8GB of RAM) ii. Client device B (Attacking Device): Windows 10 Pro, intel(R) Celeron processor, 1.60Ghz, 4GB of RAM iii. Client device C: Windows 10 Pro, Intel Core i7, 2.6 GHz, 8 GB of RAM)
Protocols Specifications	i. WEP security protocol: Hexadecimal, 64-bit key, open system ii. WPA PSK (AES encryption, PSK password) iii. WPA PSK (TKIP encryption, PSK password) iv. Traffic protocol (HTTP, DNS and SMTP/IMAP)

Figure 1 depicts the experimental scenario setup using the tools designated for the empirical experiment. The setup shows the two client communicating computers, the computer configured with the attack tool and the router used for the generation and propagation of the WLAN, the WLAN security protocols and the various traffic types.

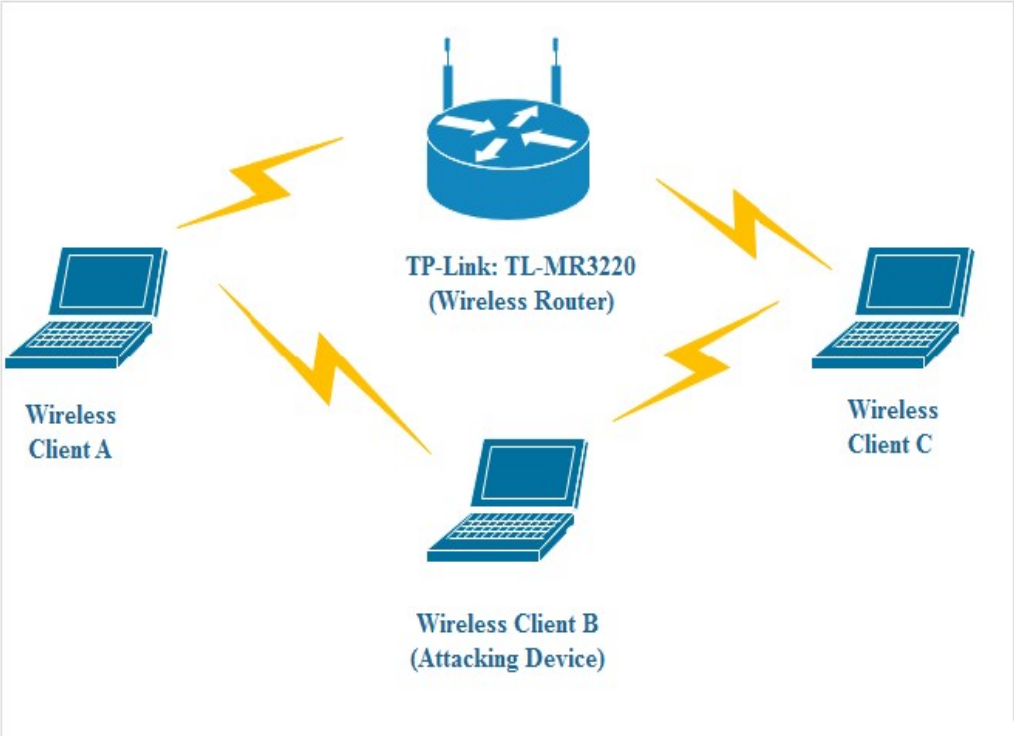

Figure 1: Experimental Scenario Setup / Topology

This study employed a sniffing attack which is a variation of the man-in-the-middle attack to evaluate WLAN security protocols provided by the router employed in the propagation of the wireless media used to interconnect the various systems. The generation of the various traffic types and the protocols used to route them were configured on the router.Wireless Client A in figure 1 was the sending device (sender) and it was used to route various traffic types (HTTP, DNS and SMTP/IMAP) to the receiving device. Wireless client B was used as the attacking device to execute the sniffing attack aimed at intercepting the various traffic routed from the sending to the receiving device. And the sniffing device which contained the Wireshark application was setup and running on the advanced option mode.
Wireless client C was used as the receiving device (receiver) in this experiment. It was configured to receive the various traffic types routed by the sender using the different protocols

Having setup the evaluation environment, the different security protocols were used to route various traffic type data successively from sender to receiver, while the attacking device executed it traffic capture mission. This procedure was carried out repeatedly until a consistent pattern that produced the same set of results for each traffic types routed with specific protocol types were achieved. Having achieved the traffic captures of the consistent pattern for the various traffic types for all the protocol types, the display filters facility on Wireshark was used to display the packets for the different traffic types for each protocol types.

The input/output graph generated for each traffic type for specific protocol type by Wireshark was used for the results evaluation. The input/output graph presented detailed information oo the total packets received per second and the total number of seconds used to execute the sniffing attack. And to fully understand the level of security provided by each WLAN security protocol in the course of this experiment, the peak packet captured per second was identified and compared to other results obtained for different traffic types and security protocol types.

4. RESULTS PRESENTATION/DISCUSSION

The presentation and discussion of the results obtained in this study is presented using the generated input/output graph for each security protocol type routing the different traffic types.

WEP routing HTTP, DNS and SMTP/IMAP Traffic Types

The presentation and discussion starts with WEP routing HTTP, DNS and SMTP/IMAP traffic types. Figures 2, 3 and 4 shows the respective input/output graphs of the traffic types followed by their brief interpretations.

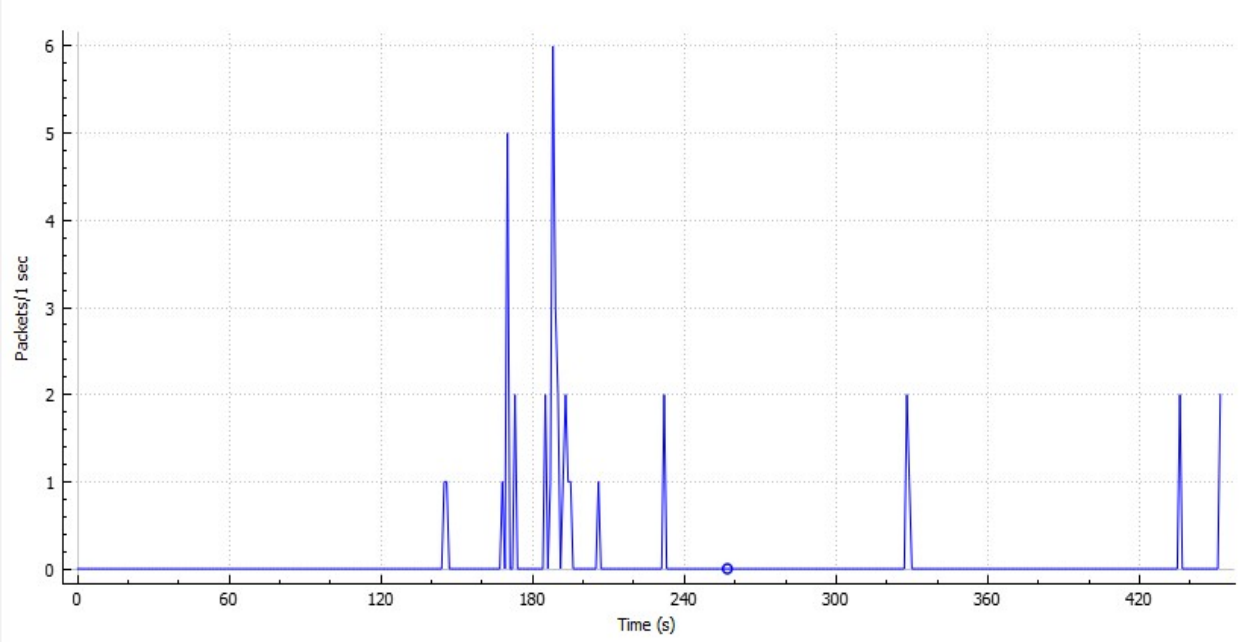

Figure 2: Graph for WEP Security Protocol Routing HTTP Traffic

From Figure 2 it can be seen that there no activity in the first 140 seconds and the peak packet captured was 6 packet per second in an attack that lasted 320 seconds.

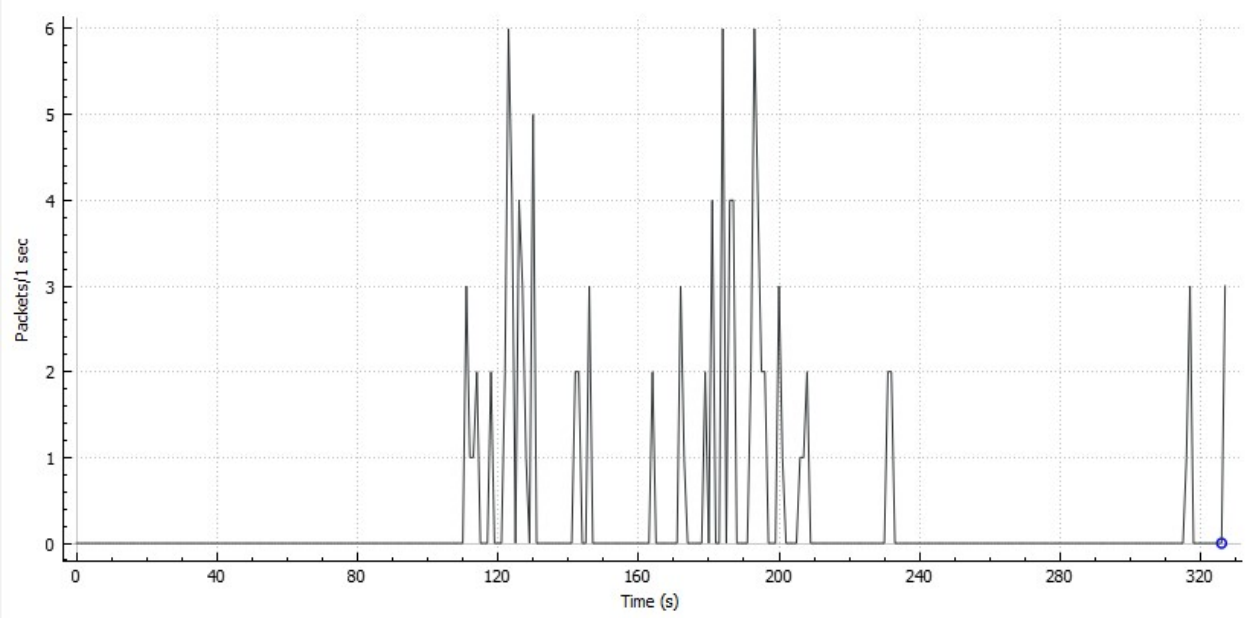

Figure 3: Graph for WEP security protocol routing DNS Traffic

From Figure 3 there was no activity on the network for 109 seconds after which the packets captured increased to between 3 and 6 packets per second for 100 seconds and evened out at 316 seconds. The graph showed 6 packets per second as the peak packet captured during the entire sniffing attack.

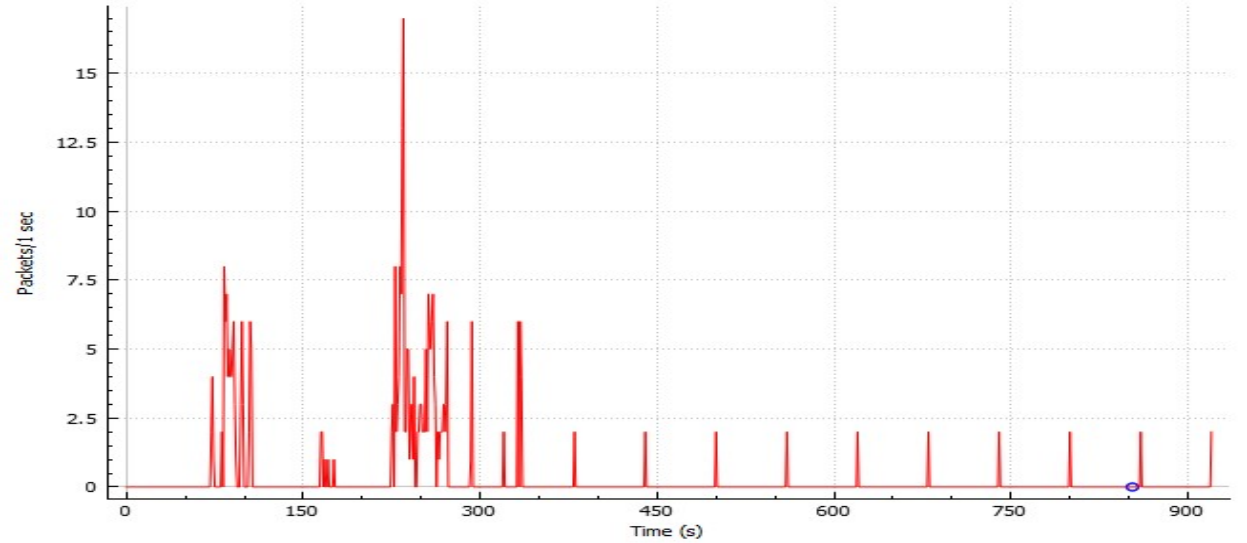

Figure 4: Graph for WEP security protocol routing SMTP/IMAP Traffic

Figure 4 showed that there was no activity for approximately 70 seconds, and then, all of a sudden, there was a packets captured rate of 8 packets per second at approximately 83 seconds, then a peak packet capture of approximately 16.9 packets at 235 seconds, before dropping down a minimal level of approximately 1.9 packets per second between 325 seconds to 900 seconds.

WPA-PSK Routing HTTP, DNS and SMTP/IMAP Traffic Types

The next set of results presentation and discussion is for WPA-PSK routing HTTP, DNS and SMTP/IMAP, traffic types. We have two sets of scenarios here. The first set is WPA-PSK (AES Encryption) routing HTTP, DNS and SMTP/IMAP traffic types which are depicted by their respective input/output graphs in Figures 5, 6 and 7 while the second set is WPA-PSK (TKIP encryption) routing HTTP, DNS and SMTP/IMAP traffic types. Figures 8, 9 and 10 contains the respective input/output graph generated for the various traffic types.

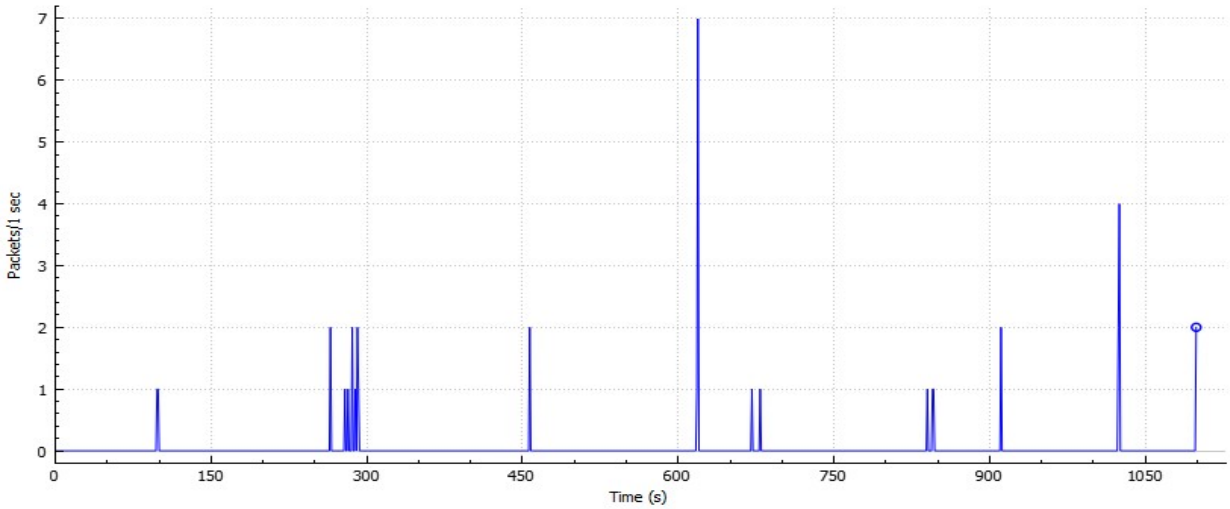

Figure 5: Input /Output graph for WPA-PSK Security Protocol (AES Encryption) Routing HTTP Traffic

From Figure 5 no activity was noticed for until the 100 seconds approximately, and the average packets captured per second was between 2 and 4 packets/ second, while the peak packet captured was 7 packets per second at approximately 625 seconds.

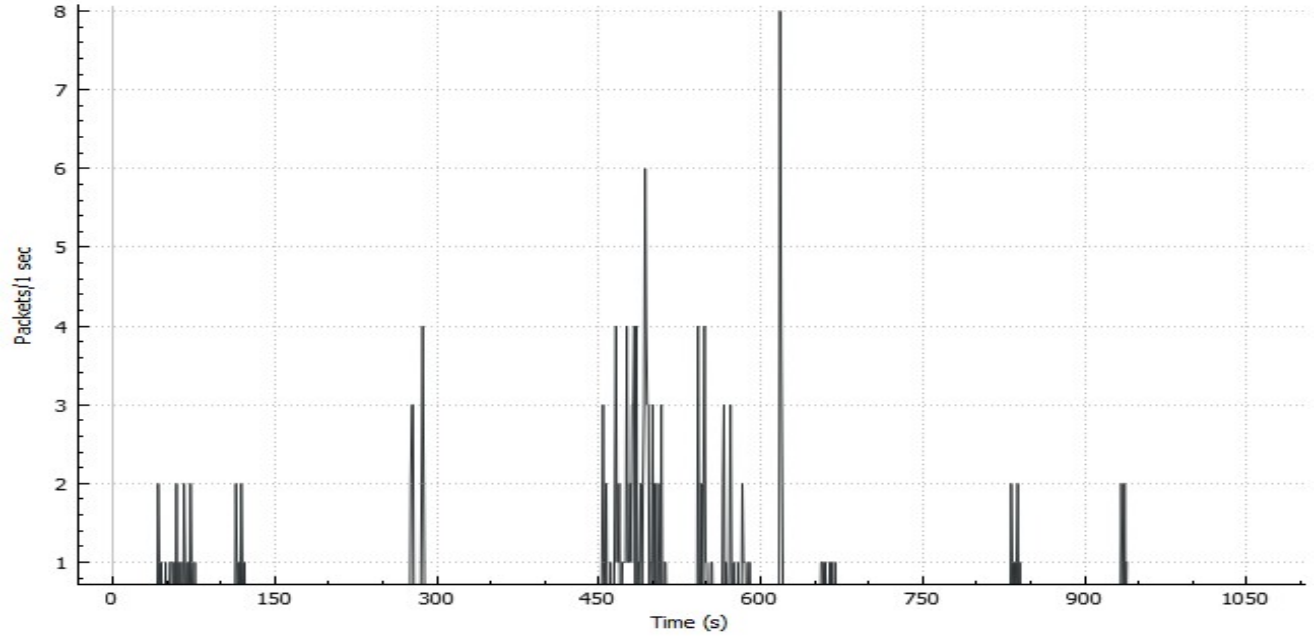

Figure 6: Graph for WPA-PSK (AES) Security Protocol Routing DNS Traffic

Figure 6 indicates that attack activity became noticeable at around 40 seconds approximately with between 1 and 2 packets captured per second for a period of 80 seconds. The peak packet capture was between 450 seconds to 900 seconds, with the peak packet captured standing at 7 packets per second between exactly 620-625 seconds.

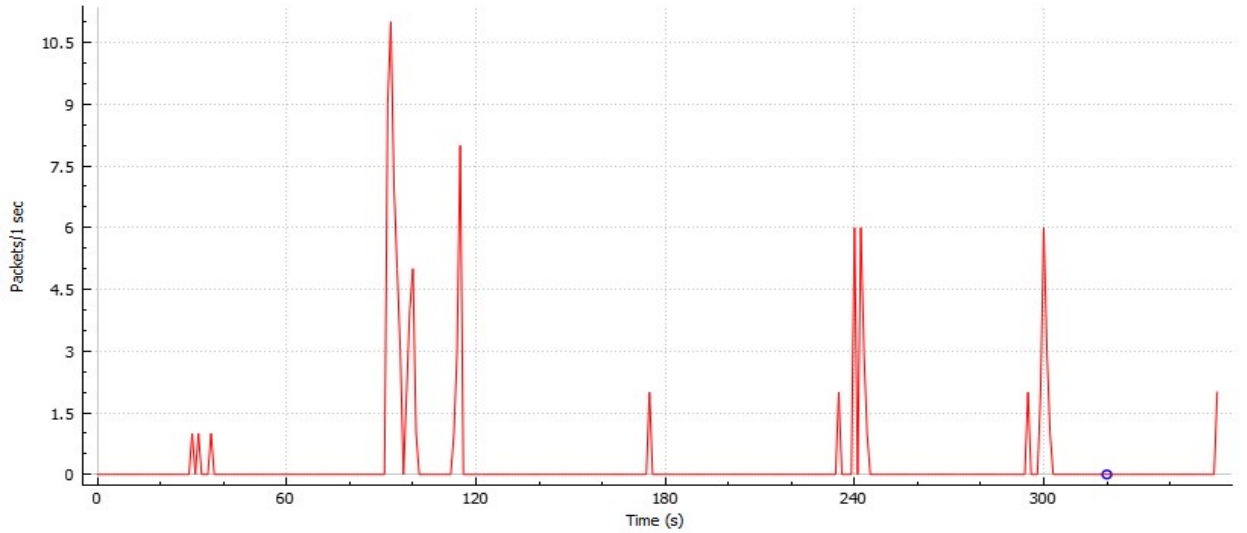

Figure 7: Input / Output Graph for WPA-PSK (AES Encryption) Security Protocol Routing IMAP/SMTP Traffic

In Figure 7, no activity was noticed for the first 30 seconds after which little activity was noticed for 20 seconds. The peak packet interception was between 95 and 155 seconds. Another noticeable observation was that for about approximately 55 seconds interval after there was packet capture, there was inactivity.

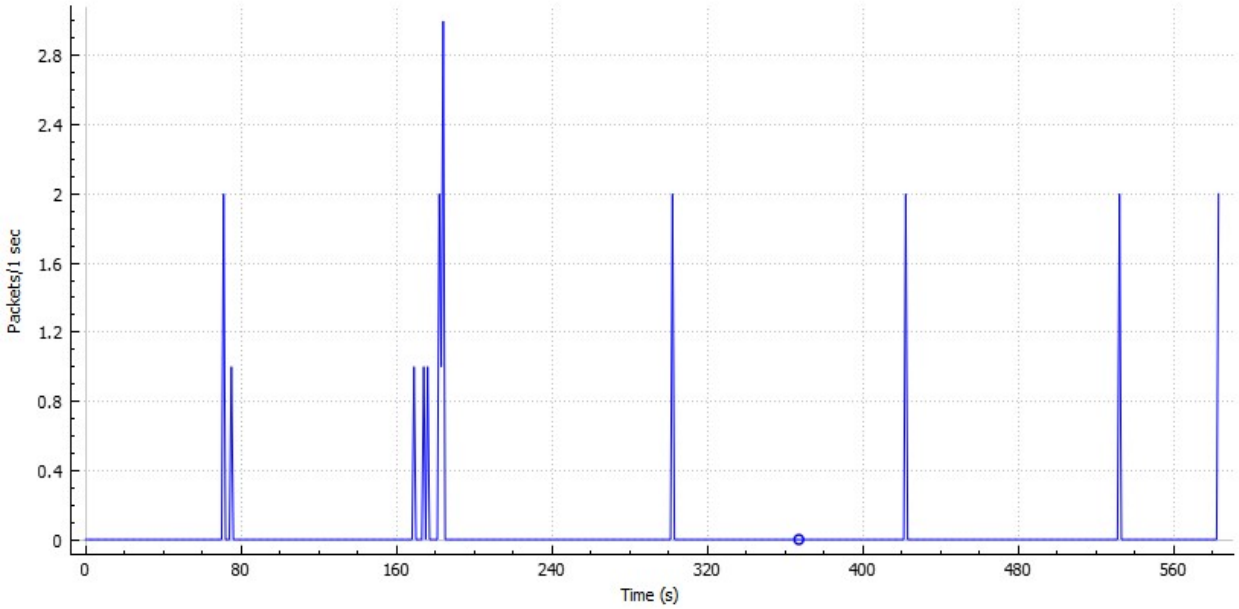

Figure 8: Graph for WPA-PSK (TKIP) security protocol Routing HTTP Traffic

For approximately 70 seconds no activity was displayed by the input/output graph as depicted in Figure 8. However, from 71 seconds, there was capture activity at the rate of 2 packets per second. There was an average of 100 seconds inactivity interval between each packet captured until traffic capture activity was halted.

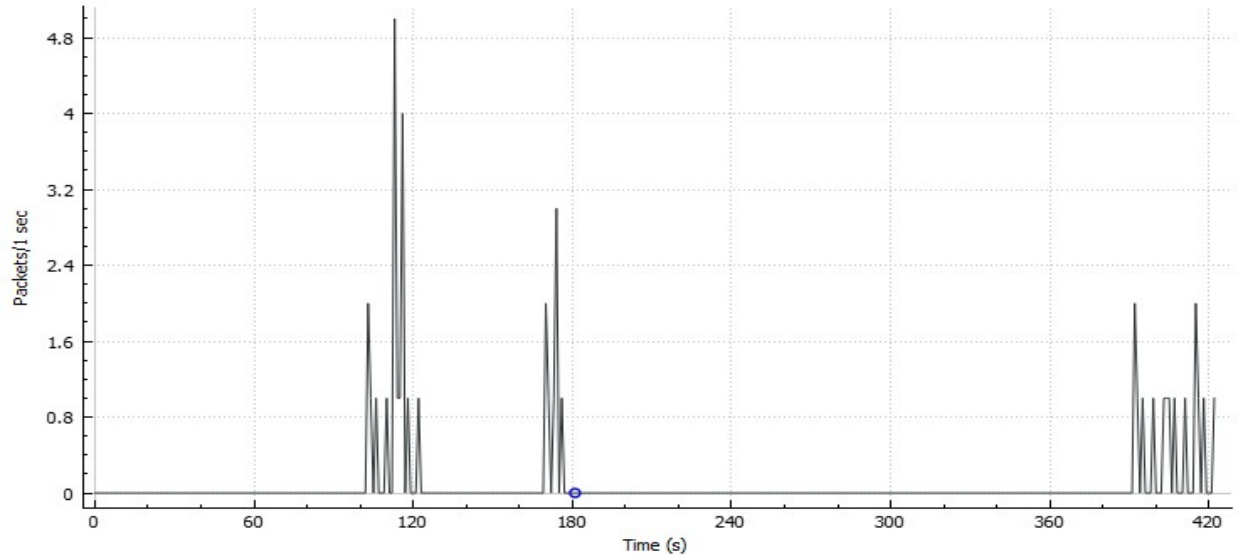

Figure 9: Graph for WPA-PSK (TKIP) Security Protocol Routing DNS Traffic

Figure 9 gives a representation of the input / output graph which shows no activity for 100 seconds. After which there was noticeable activity for 320 seconds. The peak packet captured was 4.9 packets per second between 112 and 117 seconds and it lasted for 420 seconds before it was halted.

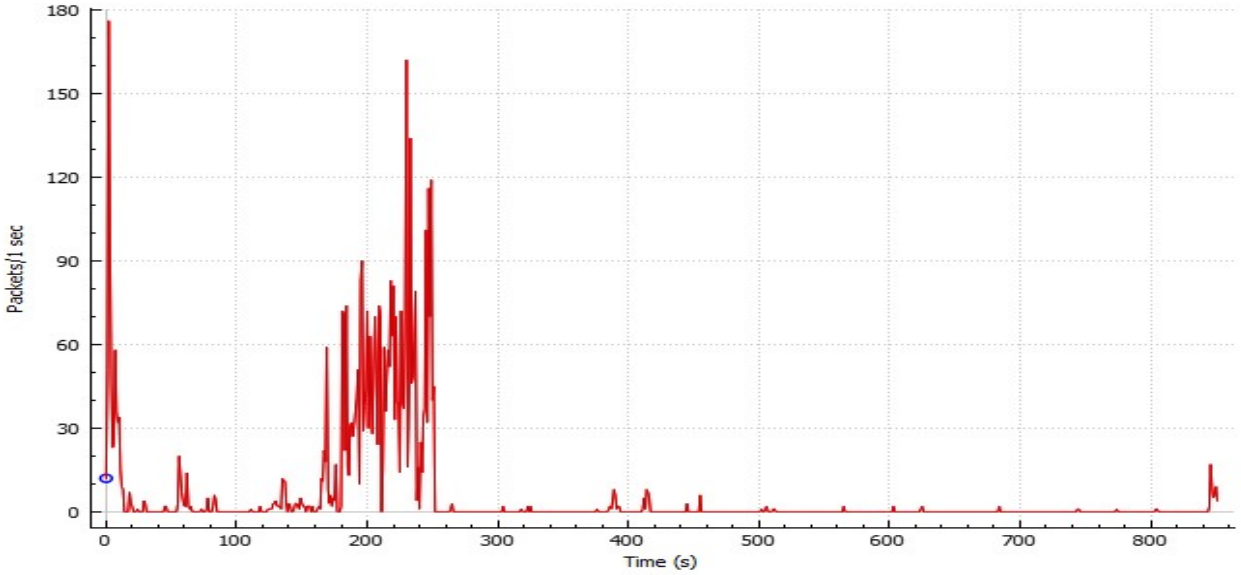

Figure 10: Graph for WPA-PSK (TKIP) Security Protocol Routing SMTP/IMAP Traffic

Figure 10 shows that the period of high activity was the first 250 seconds with a peak packet captured of approximately 178 packets per second for about 10 seconds. Then, activity returned to a minimal level at exactly 254 seconds, at it remained at that level until it was halted at 800 seconds

A detailed analysis of the results for the various security protocols routing various traffic types are presented in Table 4.1 for ease of comparison.

Table 4: Summary and Comparison of Results

Security Protocol/ Traffic Type	Active Time in (Seconds)	Peak Packet Captured/Second	Recommended Security Protocol
WEP: (HTTP)	143 – 227	6	
WPA-PSK (AES): (HTTP)	220 – 1100	7	
WPA-PSK (TKIP): (HTTP)	70 – 583	2	WPA-PSK (TKIP)
WEP: (DNS)	110 – 233	6	
WPA-PSK(AES): DNS	450 – 650	8	
WPA-PSK(TKIP): DNS	100 - 178 395 – 420	5	WPA-PSK(TKIP)
WEP: SMTP/IMAP	70 – 340	17	
WPA-PSK (AES): SMTP/IMAP	86 – 305	11	WPA-PSK (AES)
WPA-PSK (TKIP): SMTP/IMAP	0 -265	178	

Table 4 shows summary of the results obtained from the input/output graph generated by the security protocols for the various traffic types. The recommended security protocol was derived based on the peak packet size captured per second. From Table 4, for HTTP type traffic, WPA-PSK (TKIP) is the preferred option because at the peak packet capture period, only 2 packet per second were intercepted. The same applies to DNS traffic type, because with WPA-PSK (TKIP), the packet capture rate was 5 packets per second. However, for SMTP/IMAP traffic type, WPA-PSK (AES) provided the best result of 11 packets per second

5. CONCLUSION

The current level of investment in WLANs is soaring as more businesses, homes and institutions join the league of others who are already leveraging the benefits inherent in computer networks. Most businesses already boast of running a near paperless office, which implies that most of their business related transaction documents are distributed and stored as soft copies. While this development is welcomed, the need to understand the security risks incidental to the investment in WLANs needs to be emphasized so that appropriate security risks counter measures could be put in place to safeguard these huge investments. The preliminary study conducted in the course of this study showed that most business owners, managers and other users of WLANs have a lukewarm attitude to the security risks they face in this contemporary times that there is a mushrooming of cyber related attacks.

This study has demonstrated the vulnerability of data in WLANs transmission channels by using a widely available, free (open source), easy to install and use network sniffing software (Wireshark) to illustrate the risks exposure of the businesses who currently have a lukewarm attitude to cyberattack risks. From the results obtained based on the two popular protocols of WEP and WPA (WPA-PSK (AES) and WPA-PSK (TKIP)), it is apparent that, though the two protocols (and their variations) are vulnerable to attack, they are vulnerable to remarkable varying degrees. Therefore for routing HTTP and DNS traffic types, the router should be set to the WPA-PSK (TKIP) security protocol, while for SMTP/IMAP traffic type it should be set to WPA-PSK (AES) security protocol option.As an ad-memoir, businesses running very sensitive transactions on their WLANs which are connected to the internet, must take additional security cautions. It is apparent that the core traffic types are: HTTP/HTTPS (web Browsing), IMAP/SMTP (emailing) and DNS (map an address to a name or name to an address).

As a suggestion to further improve on security, the router setting should always avoid the HTTP option as much as possible. This is because HTTP leaves a network vulnerable to man-in-the-middle related attacks and denial of service attacks. And also, secure HTTP (HTTPS) should be used instead of HTTP to access applications or information to leverage its encryption. Regarding DNS traffic, users are advised to use the business network to connect to only trusted websites to avoid DNS poisoning attacks at its dire consequences. And very importantly, businesses should invest in data encryption mechanism, intrusion detection schemes and perimeter fencing schemes (firewalls).

REFERENCES

1. Ajah , A. I. (2014). Evaluation of Enhanced Security Solutions in 802.11-Based Networks. International Journal of Network Security & Its Applications (IJNSA), 6(4), 29-42.
2. Aleksandar , S., Bozidar , K., & Edvard, T. (2015). Wireless Network Security recommendations Using the Application for Security Evaluation. INFuture, 287-297.
3. Anas, B. (2016). Crowd Mobility Analysis Using WIFI Sniffers. International Journal of Advanced Computer Science and Applications, 7(12), 374-378.
4. Aruna , D. P., Rani, L. S., & Sathiyavaishnavi, K. (2013). A Study on Network Security Aspects and Attacking Methods. International Journal of P2P Network Trends and Technology-, 3(2), 97-103.

5. Aruna, V., & Swathi, P. (2016). Comparative Study of Packet Sniffing tools for HTTP Network Monitoring and Analyzing. IJCSET(www.ijcset.net), 6(12), 406-409.
6. Babita , D., & Neha , G. (2016). Integrating Enhanced Security Measures in WEP/WPA/WPA2-PSK (Review Paper). International Journal of Innovative Research in Computer and Communication Engineering, 4(2), 1240-1245.
7. Chao, Y., Jiafeng, M. A., & Xuewen, D. (2011). A New Evaluation Model for Security Protocols. Journal of Communications, 6(6), 485-494.
8. Charu, G., Gaurav, S., Rishi, P. G., Pupul, S., & Bhavya, K. S. (2014). Packet Sniffer – A Comparative Study . International Journal of Computer Networks and Communications Security, 2(5), 179-187.
9. Deepika , D. (2014). WLAN Security Issues and Solutions. Journal of Computer Engineering, 16(1), 67-75.
10. Ezedin, B., & Mohammed , B. (2007). On The Impact of Security on the Performance of WLANs. Journal of Communications, 2(4), 10-17.
11. Frankel , S., Bernard, E., Les , O., & Karen, S. (2007). Establishing Wireless Robust Security Networks: A Guide to IEEE 802.1I. Gaithersburg: National Institute of Standards and Technology.
12. Inderjit , K., Harkarandeep , K., & Gurjot , S. (2014). Analysing Various Packet Sniffing Tools. International Journal of Electrical Electronics & Computer Science Engineering, 1(5), 65-69.
13. Kolahi, S., Narayan, S., Nguyen, D., & Sunarto, Y. (2011). Performance monitoring of various network traffic generators. The 13th IEEE International Conference on Computer Modelling and Simulation (UKSim), 501-506.
14. Lakshari, A., Mansoor, M., & Danesh, A. (2009). Wired Encryption Privace (WEP) versus WIFI Protected Access (WPA). International Conference on Signal Processing Systems, 445-449.
15. Lashkari, A., Towhidi, F., & Hosseini, R. (2009). Wired equivalent privacy (WEP). the International Conference on Future Computer and Communication (ICFCC), 492-495.
16. Latha, P. H., & Vasantha, R. (2014). Review of Existing Security Protocols Techniques and their Performance Analysis in WLAN. International Journal of Emerging Technologies in Computational and Applied Sciences (IJETCAS), 7(2), 162-171.
17. Li, p., Kolahi, S., Safdari, M., & Argawe, M. (2011). Effect of WPA2 Security on IEEE802.11n Bandwith and Round Trip Time in Peer-peer Wireless Local Area Networks. the IEEE Workshops of International Conference on Advanced Information Networking and Applications (WAINA), 777-782.
18. Luis , W. C. (2005). An Overview of 802.11 Wireless Network Security Standards & Mechanisms. SANS Institute, 1-18.
19. Maple, C., Jacobs, H., & Reeve, M. (2006). Choosing The Right Wireless LAN Security Protocol for the Home and Business User. The1st International Conference on Availability, Reliability and Security (ARES), 1-8.
20. Nidal, T., & Shadi, M. (2010). RECOMMENDATIONS GUIDE FOR WLAN SECURITY. The International Journal of ACM Jordan, 1(1), 18-27.
21. Nisbet, A. (2012). A tale of four cities: Wireless security and growth in New Zealand. The International Conferenceon Computing,Networking and Communications (ICNC), 1167-1171.
22. Omar, A. H. (2011). Mosul University WLAN Security: Evaluation, Analysis and Improvement. Iraq J. Electrical and Electronic Engineering, 7(2), 138-143.
23. Pandikumar, T., & Mohammed , A. Y. (2017). Wi-Fi Security and Test Bed Implementation for WEP and WPA Cracking. International Journal of Engineering Science and Computing, 7(6), 13571-13576.
24. Poonam , J., & Brahmjit , S. (2017). Quantitative Analysis of the Security Performance in Wireless LANs. Journal of King Saud University- Computer and Information Science, 29, 246-268.
25. Praful, S., & Sandeep, K. S. (2017). Analysis of Network Traffic by using Packet Sniffing Tool: Wireshark. International Journal of Advance Research, Ideas and Innovations in Technology, 3(6), 804-808.
26. Rathod, M. P., & Deepak, C. K. (2015). Performance Measurement of WEP and WPA2 on WLAN Using OpenVPN. International Conference on Nascent Technologies in the Engineering Field (ICNTE), 1-4.

27. Reddy, S., Sai, R. K., Rijutha, K., Ali, S., & Reddy , C. (2010). Wireless hacking - a WiFi hack by cracking WEP. The 2nd International Conference on Education Technology and Computer (ICETC), 189-193.
28. Richa , G., Hamid, A., Munendra, K. D., & Shalini, C. (2015). An Evaluation of "Security Services" schemes For IEEE 802.11 Wireless LAN's Using Qualnet. International Journal of Innovative Research in Science, Engineering and Technology, 4(1), 18931-18936.
29. Saurabh, M., Aishwarya, R., Rohan, P., & Aastha, S. (2017). Research on Wi-Fi Security Protocols. International Journal of Computer Applications, 164(3), 975-983.
30. Seliim, G., El-badawy, H., & Salam, M. (2006). New Protocol Design for Wireless Networks Security. The 8th International Conference Advanced Communication Technology (ICACT), 4-776.
31. Thaier, H., Samer, K., Bassam , J., & Awni , I. (2012). Analyzing the Impact of Security Protocols on Wireless LAN with Multimedia Applications. The Sixth International Conference on Emerging Security Information, Systems and Technologies, (pp. 169-175).
32. Tom, K., & Les, O. (2008). Wireless Network Security; 802.11, Bluetooth and Handheld Devices. Gaithersburg: National Institute of Standards and Technology.
33. Vipin , P., & Hitesh , C. (2014). A COMPARITIVE ANALYSIS OF WIRELESS SECURITY PROTOCOLS (WEP and WPA2). International Journal on AdHoc Networking Systems (IJANS), 4(3), 1-7.
34. Vishali, R. (2014). Security in Wireless Local Area Networks. International Journal of Computer Science and Information Technology Research, 2(2), 472-483.