IJIRR

International Journal of Information Research and Review
Vol. 03, Issue, 07, pp. 2578-2584, July, 2016

Research Article

EVALUATION OF THE SECURITY CHALLEGES AND VULNERABILITIES OF WIRELESS NETWORK IN NIGERIA AND THE COUNTERMEASURES

*Ikporo Stephen, C.

Department of Computer Science, Ebonyi State University, Abakaliki – Nigeria

ARTICLE INFO

Article History:

Received 15th April 2016
Received in revised form
24th May 2016
Accepted 19th June 2016
Published online 31st July 2016

Keywords:

Access Point,
Wireless Network,
Wireless Security,
Wireless Threats,
WEP,
IEEE 802.11.

ABSTRACT

Nigerians telecom industries are witnessing continuous growth and rapid progress in policy and technological development, which has resulted to increasingly competitive and networked world. Wireless communication systems offer much gain in developing countries including Nigeria. This wireless networks have experienced an explosive growth similar to the internet itself. This is due largely to the attractive flexibility enjoyed by both users and the providers themselves. At present wireless network weakness are on the increase due to the higher demand for wireless access, demand for higher data rates, the emergence of advanced services and the large deployment of the services in Nigeria and indeed the globe. This wireless network has however had daunting security challenges which have made them vulnerable and insecure. And their broadcast nature makes link-layer attacks readily available to anyone within the network layer. This is evident as security issues associated with them are escalating day by day thereby making high-speed wireless network and internet services insecure and defective. The present 802.1x authentication scheme often employed on wireless network is not without flaws, making mutual authentication impossible and open to man-in-the-middle attacks. There are new security issues seen with wireless network that threatens and alters the organizations overall information security risk profile. These threats have also affected the gains offered by wireless network especially in Nigeria where some stringent challenges of wireless network vulnerabilities are quite high. Effective management of the threats requires sound and thorough assessment of risk given the Nigeria environment and development of a plan to mitigate identified threats. This paper explores security issues associated with wireless network, so that a fully secured network could be established in Nigeria.

INTRODUCTION

Wireless network presents many advantages with improved productivity because of increased accessibility to information resources. Some of the benefits includes: network coverage without the cost of deploying and maintaining wires, mobility support and roaming which allows the users to access the network anytime, anywhere, and so on. The level of wireless network usage presently is a testament primarily to their convenience cost, efficiency and ease of integration with other networks and network components. Many organizations are deploying wireless network infrastructure to provide connectivity in places difficult to reach by cable, as a complement to the existing wired network, (Graham and Steinbart, 2006). The emergence of this new technology which can enable truly ubiquitous internet access also creates new threats and alters the existing information security risk profile.

Corresponding author: Ikporo Stephen, C.,
Department of Computer Science, Ebonyi State University, Abakaliki – Nigeria.

Because wireless network communications take place through the air using radio frequencies, the risk of interception is greater than with wired networks. World over, a lot of attentions have been given to the provision of wireless networks solutions and with little attention been given to the provision of adequate security for the network which has made the network prone to unauthorized alterations, destruction and disclosure. This has lead to confidentiality compromise because if messages are not encrypted or encrypted with a weak algorithm, the attackers can intercept and access them, (Graham and Steinbart, 2006). Security of Wireless Network is more concentrated and complex than security of wired networks because wireless their broadcast in nature, making it possible for anyone within the range of a wireless device to interrupt the packets sent without interrupting the flow of data between the wireless device and the access point (Zhu and Ma, 2004). Wireless network security is different from wired network security primarily because it gives potential attackers easy transport medium access. This access significantly increases the threat that any security architecture must address.

However, the earlier 1EEE802.11 standards failed in this regard. (Arbaugh, 2003) Hence the security schemes in wired network cannot be used directly in the wireless network.

The Overview of Wireless Network

The wireless network consists of four basic components. These include: the radio frequencies which transmit the data; the access points that provide a connection to the network; the client device such as laptops, PDAs, etc; and users, (CSI, 2004). See figure 1 below.

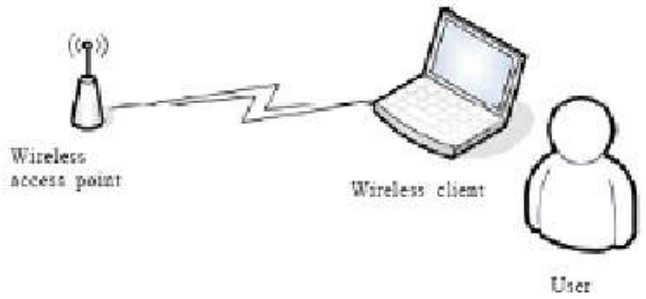

Figure 1. The components of the wireless communication [CSI, 2004]

According to (Finke, 2000), wireless communication is the transmission of message signal through low-energy radio frequency waves using open air, a transmitter and a receiver as the media. The message signal is transmitted to the closest antenna site and delivered via fiber optic cable to a wired telephone or by radio signal to another wireless phone. Wireless enabled devices such as personal computers, video game console, mobile phone, mp3, player or PDAs can connect to the internet. The coverage of one or more interconnected access point (hotspot) can comprise of a few rooms or many miles away as covered by a group of access points with overlapping coverage. Wireless network can also be deployed in mesh configuration, resulting in a wireless mesh network which allows for continuous connections and reconfiguration around broken or blocked paths by "hopping" from one node to another until the destination is reached, (http://www. wirtel.co.uk/ article_africa_2005_q3_001_alvarion.htm). Wireless networks by design have limited range for example a typical wireless router using 802.11b or 802.11g with a stock antenna might have a range of 32m (120ft) indoors and 95m (300ft) outdoors. IEEE 802.11n can exceed double of that range. This range itself also varies with the frequency band. For instance, wireless network in the 2.4 GHz frequency block has slightly better range than that in 5 GHz frequency block. In general, wireless network performance decreases quadratically as distance increases at constant radiation levels, (http//www.itu.int/ITU-D/connect/Africa/2007/ summit/ pdf/ s2_background.pdf retrieved on 23/11/2015).

Wireless Network Security in Nigeria

Nowadays in Nigeria and indeed in the world over, the transfer of information in a safer and secured way over a network has developed into a key challenge for the IT Industries. The security threats facing computer network in Nigeria including wireless have become more technically sophisticated, better organized and harder to detect.

Consequently, the consequences of failing to block these attacks have increased. Apart from the economic consequences of financial fraud through this network, the country is also witnessing real-world attacks that impacts negatively on the reliability of critical infrastructure and national security, (Moore, 2006). The attacks and the network security actions define how using the network security tools, in a better, healthy and safe network can be designed and maintained. The security in wireless network is more complex and as well concentrated than that of wired and with wireless' broadcast in nature, they are more vulnerable as anyone within the range of a wireless device can intercept the packets sent without interrupting the flow of data between the wireless device and the access point, (http://www.wirtel.co.uk/article_africa_2005_q3_001_alvarion. htm). The mobile communication system has increased their security features to include; confidentiality on the air interface, anonymity of the user, and authentication of the user to prevent fraudulent use of the system, (http://www.airdefence.net/products/index.shtm (30 April, 2014).).

The network security employed in wireless is different from that of wired network because wireless gives potential attackers easy transport medium access. This access significantly increases the security threats and vulnerabilities of the network. Unfortunately, the earlier IEEE 802.11 standards did not take note of that. Hence the security schemes in wired network cannot be used directly in the wireless network. The wireless network security issues includes: unauthorized access points, broadcast SSIDs, unknown stations, and spoofed MAC address, (Cisco, 2004).

Types of Wireless Attacks/Security

According (35, 37), basically the security attack been faced by wireless network in Nigeria can be classified into two categories; Passive Attacks and Active attacks.

Passive Attacks: These are attacks with some attributes that involves attempt to disrupt the system by the use of experimental statistics. They include the plain text attacks where both the plain text and the code text are already known to the attackers. They include:

- **Traffic Analysis**: This attacks privacy, or obscurity. It can include trace back on a network, CRT radiation etc.
- **Man-in-the-Middle**: The attacker here entices the computer to log into a computer which is set up as a soft Access Point (AP). Once this is done, the hacker connects to a real access point through another wireless card offering a steady traffic flow through the transparent hacking computer to the real network. With this penetration, the hacker can then sniff the traffic. This can cause "de-authentication attack". This attack forces connected computer to drop their connections and reconnect with the crackers soft AP.

According to 8, 10, 11 and 12, others are:

- **Eavesdropping**: This is the interception and reception of information transmitted over a wireless network illegitimately. This attack is against the confidentiality of the data transmitted over the network and is made possible because the network signals can be received

outside the vicinity of the valid users easily, (8). Hence the attacker can hijack the signal from a distance.

- **Electromagnetic Interference (EMI)**: This is the degradation of the network signal (signal fading) and disruption of wireless signals due to the wide distance between the transmitter and the receiver. This can be described as attenuation. EMI can also be caused by atmospheric conditions or metallic surfaces which can reflect the radio waves or it could be due to the obstacles in the line of sight.
- **Bandwidth Overloading**: This occurs when the wireless internet connection is accessed by an unauthorized user within the network neighbourhood without the consent of the legitimate user thereby allowing access to user more than its designed capacity. This is otherwise known as piggybacking and can also cause service violations, direct attack on the computer and illegal activities by malicious users.
- **Wireless Sniffing**: This is the process by which sniffing tools are used to invade sensitive information such as password, bank account number, credit card details etc. This is possible because many public access points are not secured and with unencrypted traffic (data) as well. Wireless sniffing is similar to shoulder surfing which allows the attackers to directly observe someone's shoulder to fetch information.
- **MAC Spoofing and Session Hijacking (Identity Theft):** This occurs when the attacker illegitimately gain access to privileged data and resources in the network by impersonating the identity of a valid user. This can also occur when crackers are able to listen to network traffic and identify the MAC address of a computer with network privileges. It can be called masquerade. It can be eliminated by ensuring that proper authentication and access control mechanisms are put in place in the WLAN.
- **Rogue Access Point:** This is installed by an attacker to accept traffic from wireless clients to whom it appears as a valid authenticator. The packets so captured can be used to extract sensitive information or be used for further attacks before finally being re-inserted into the proper network.
- **Cafe Latte Attack:** This occurs when intruder has the ability to break into the WEP key of a remote client by sending a flood of encrypted ARP request. The attacker takes the advantage of the flaws in 802.11 WEP and uses the ARP responses to obtain the WEP in just few minutes.
- **Accidental Association**: This attack occurs when a user turns on a computer and it latches onto a wireless access points from another overlapping network within the neighbourhood which the user may not even know that it happened. This brings about security breach as organisation's vital information can be exposed to already existing link from another company as may have been created by this.
- **Ad-hoc Networks**: This is a peer – to - peer networks between wireless computers which do not have access points between them. Ad-hoc networks can pose a great threat to organizations' networks.
- **Non Traditional Networks**: Less attention has been given to non-traditional networks such as personal Bluetooth devices with many not knowing how much such devices are not safe from cracking. In the same manner barcode readers, handheld PDAs, and wireless printers and copiers are not secured. Crackers can capitalize on this oversight and crackdown these devices and access their information.

Active attack: This is the type of attack that allows the attacker to direct data to one or both of the parties, or block the data stream in one or both direction 35, 37). They include:

- **Fabrication**: This is the creation of counterfeit information and inserting same into the network in order to deceive the authorised user into believing on the genuineness of the inserted counterfeits information. This attacks the validity of the network packets.
- **Modification**: This involves the alteration or complete erasure of information contained in the network by an unauthorized user. This attacks the reliability of the network information.
- **Interruption/Denial of Service (DoS):** This occurs when a given network is clogged or bombarded with bogus requests, premature successful connection messages, failure messages, valid or invalid messages enough to affect the availability of the network resources thereby preventing the authorized users' access to the network. This can cause wireless network not to communicate using the radio path or cause a system crash. Since Dos causes network interruption by preventing data transmission, attackers try to observe the recovery process of the network as the initial codes are re-transmitted by the authorized users. The intruder can use any cracking device to record the codes and afterwards use same to gain unauthorized access into the network. This attack mainly relies on the abuse of protocols such as the Extensible Authentication Protocol (EAP).
- **Traffic Redirection**: This is the manipulation of the Media Access Control (MAC) address as well the IP address of a given network by the malicious attacker, thereby allowing the traffic route of such network to be changed to that of the attacker.
- **Malicious Association**: This occurs when the crackers make active wireless devices to connect to the wireless networks through their cracking devices instead of the wireless Access Points (APs). These cracking devices are known as "Soft APs" and are created by crackers when they run some software which makes their wireless network card look like a legitimate access point. The easy access to the wireless network by the crackers through this means makes it possible for them to steal password and launch attacks on the networks or plant virus like Trojan. Again, since wireless networks operate at the layer 2 levels, the network protections such as network authentications and Virtual Private Networks (VPNs) offered in layer 3 cannot prevent these actions of the crackers.
- **Network Injection**: This occurs when network access points which are exposed to non-filtered network traffic are being used to specifically broadcast network traffic such as "Spanning Tree" (802.1D), OSPF, RIP and HSRP. When this occurs, the crackers inject bogus networking re-configuration commands which affect routers, switches, and the intelligent hubs of the given

network. This can cause network failure or crash thereby making such network to require rebooting or reprogramming of all the intelligent network devices.

Security Measures in Wireless Network

Since the nature of wireless communications allow for three basic security threats: interception, alteration and disruption, 802.11b standard according to (12), provides some security measures which include:

- **Service Set Identifiers (SSID):** This is the security feature which ensures that all devices trying to access a particular wireless network must first be configured with the wireless network and verified by access point. Hence no client can communicate with the WLAN without having the same and verified SSID configuration. However, this provides this provides very little security as it is more of a network identifier than a security feature.
- **Wired Equivalent Privacy (WEP):** This is an encryption mechanism standard first introduced by 802.11 to provide security level which will help overcome the security threats in wireless networks. It is an algorithm used to protect wireless network communication against eavesdropping and modification as well as unauthorized access to wireless network. WEP relies on the secret key that is being shared between the wireless station and the access point. This secret key is used to encrypt packets before they are transmitted and an integrity check is used to ensure that the packets are not modified on transmit, (SANS Institute, 2003). The security feature of WEP is based on the fact that they encrypt all information transmitted over the air such that only receivers that are with the same encryption key can decrypt the information, (8). Though WEP uses RC4 encryption algorithm and CRC-32 checksum algorithms as sits stream cipher, there are a lot of growing concern regarding WEP integrity. For example WEP does not provide any forgery protection. Hence masquerading attack is still possible, (Hamid, 2003; Sing, 2012).
- **Media Access Control (MAC) Address Authentication:** Here, the Access Point is configured to accept association and communication request from only those nodes whose MAC addresses are already registered with it. The beauty of MAC address authentication of is that it provides for additional security layer. The problem with this measure is that whenever any node (computer) with registered MAC address is lost, the node will continue to connect (appear) on the network as a legitimate user, (Homeland Security, 2006).
- **Signal-Hiding Techniques**: This allows for the turning off of the Service Set Identifier (SSID) broadcasting by wireless access point, assigning of cryptic names to SSIDs, reducing signal strength to the lowest level that can still provide requisite network coverage or locating of the wireless access points in the interior of the building, away from windows and interior walls. Another effective method here is by using directional antennas to constrain signal emanations within desired areas of coverage or using signal emanating-shielding techniques, sometimes referred to as TEMPEST, 1 to block emanation of wireless signal, (Sing, 2012).
- **Encryption**: One of the best methods of protecting the confidentiality of information transmitted over wireless network is by the use of strong encryption or scramble for all traffics and packets in wireless network. This is also important especially for organization that is subject to regulation. This ensures that the security of the wireless network from intruders and unauthorized users are guaranteed. To ensure this, most wireless routers, access points, and base station have in-built encryption mechanism. To ensure the functionality, they must be turned on, (US-CERT, 2008).

Security Measures for Wireless APs & other Devices

In order to save guard the wireless network and its traffic, the Access Points and other Devices connected to the Network should also be protected. Some measures that can be applied to protect them include;

- **Site Survey and Periodic Audits of Wireless Network**: One of the major ways to avoid or remedy wireless network security problem especially Denial of Service (DoS) include a careful site survey to identity locations where signals from some other network is in existence. This should guide the decision on the siting of the organisation's Access Points. For already located wireless network access points, periodic audits could be applied to check the activities and performances of the network in order to identify the problem areas and devices. During this, the offending device(s) would be identified and removed as a measure to increase the signal strength and coverage within the identified problem area. Network auditing also include scanning and mapping of all access points within the network with some common mapping tools like Netsnumber and Wavelan-tool, etc. Specialized tools such as Airsnort can be used for WEP cracking and auditing of the network for weak keys, key reuse and WEP security setting, (Cisco, 2004).
- **Proper and Secure Configuration of Access Points**: Another way to properly prevent access to wireless network by hackers is to ensure that all the access points are securely configured. Also, the default settings of all the devices connected to the network should be changed, since most of them are well known and can be exploited by hackers. In the same manner, the router and other device identifiers should be changed, (Cisco, 2004).
- **Using 802.1x Authentication Scheme on all the Network Devices**. The best method of combating the threat of rogue access point is by the use of 802.1x on all the devices connected on the network. This will prevent all unauthorised devices and rogue access points from becoming insecure backdoor on the network. (Kelly, 2003).
- **Turning off of the Device Identifier Broadcasting**: Most wireless routers and other devices have mechanism called identifier broadcasting with which they send out signal to any other device in the vicinity indicating their presence. In order to enhance the security of wireless network and its devices, the identifier broadcasting mechanism should be disabled. This will ensure that

hackers don't use them to home in on vulnerable wireless network, (Kennedy, 2004).

Wireless Security Methods/Tools

There are basically two methods in wireless security. They include;

- **Cryptography**: This is the most commonly used tool to secure wireless information and services, (Stallings, 2006). It relies on ciphers which is a mathematical functions used for encryption and decryption of messages in a network.
- **Firewalls**: This is another tool used in securing the wireless network. It is a group of components that collectively form a bridge between two networks. According to (35, 37), firewalls are of three types:
- **Application Gateways**: This is also known as proxy gateway. It is the first firewall in a network and is made up of defender hosts, so they act as a proxy server. Since the application runs at the Application layer of OSI model, clients behind the firewall are categorized and prioritized in order to access the internet services. This has become the most secure measure; because it does not allow anything pass through it by default. Hence programs are written and turned on in order to start the traffic passage as shown in Figure 2 below:

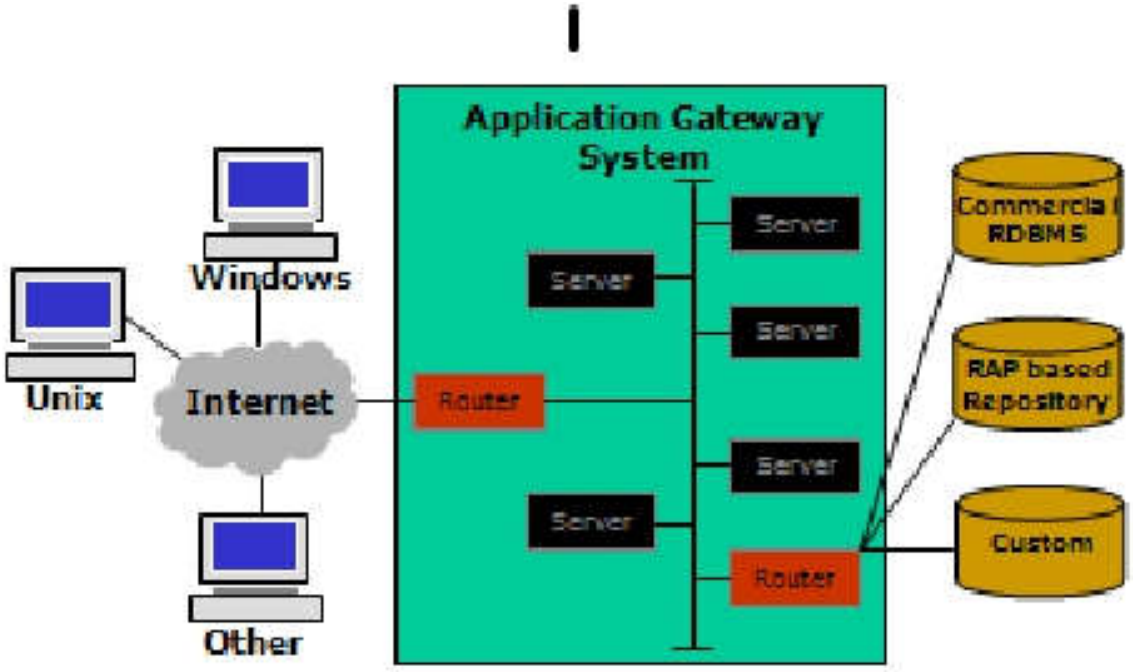

Figure 2: A sample application gateway, [Marin, 2005]

- **Packet Filtering**: This is a technique whereby routers and other devices connected to the network have their Access Control Lists (ACLs) turned on. Routers allow all traffic sent to it to pass by default without any restrictions. ACL defines the sorts of access that is permissible for the outsiders who want to have access to internal network and vice versa. Due to low density and the fact that pocket filter is associated with switches and routers, which optimizes tasks related to networking, packet filter gateway is often much faster than its application layer counterparts.
- **Hybrid systems:** this is the method that combines the features of packets filtering and the application layer gateway to function in the same machine packet filters watches the connection to ensure that only packets that are already authenticated and approved by the application layer gateway are allowed to pas. The benefit here is that, it provides a measure for protecting the users' machine which provides the services to the internet, as well as provide the security of an application layer gateway to the internal network .Additionally, the use of this method ensures that attackers accessibility into system is further restricted as the attacker, in order to access the services on the internal network, will have to break through the access router, the base station and the choke router.

Technological Options in Wireless Network Security

According to (Stallings, 2008), some well-known security vendors offer end - to – end solutions which takes care of some aspects of wireless network security. End- to – end security solutions usually offer a combination of hardware and software platforms including a security management solution that performs multiple functions and takes care of the entire gamut of security on a network.

An integrated solution is one that handles not only a point-security problem (like worm intrusion), but also handles an array of network and application layer security issues. They categorized into the following;

- **SSL- VPN:** Much consciousness of encryption of wired network in the form of SSL and IP-VPNs have always been noticed. People are ever aware of the security risks in transmitting data over the wire in clear text. In addressing this, SSL-VPN has hastened acceptance of VPNs for end

user of both wired and wireless network alike with both being encrypted.

- **ASIC Based Appliances**: This ensures a move from software – based security product which run on unlock platform to purpose built. ASIC based appliance has followed the path of routers advancements in the last decades.
- **Intrusion Detection and Prevention System (IPS):** This combines the best features of firewalls and intrusion detection system to provide a security tool that changes the configurations of network access control points according to the quickly varying threat profile of a network. This introduces the elements of intelligent in network security by adapting to new attacks and intrusion attempts.
- Most organization in Africa and indeed Nigeria evolves in their use of intrusion prevention technology. Some adopt blocking weekly and rapidly expand their blocking as they see the benefits of exact attack blocking. Others tend to start slowly and expand eventually. The key issue here is to constantly detect and stop both known and unknown attacks in real time.

Some Wireless Network Security Control Mechanisms

Notwithstanding the notable risks and vulnerabilities common with wireless communications, a number of control mechanisms can be adopted to checkmate some of the security lapses and limitation as it affects wireless network in Nigeria. These control mechanisms according (Hamid, 2003) are as follows:

- **Regular Change of Default Service Set Identifier (SSID).** The SSID is a unique identifier usually attached to the header of packets sent over wireless network, which acts as a password when a mobile device tries to connect to a particular WLAN. This identifier should be changed as regular as possible and with the use of descriptive name for the SSID or the access point always seen as the best practice, (SANS Institute, 2003). The default password and IP Addresses should be changed regularly.
- **Use of Virtual Private Network (VPN).** VPN is a network technology which creates a secure connection over a public network such as the internet or a private network by service providers. It can connect multiple sites over a large distance like that of Wide Area Network (WAN).
- VPN provides high security for the implementation of wireless network without adding significant overhead to the users. A VPN technology provides three levels of security as follows: Authentication, Encryption and Data Integrity, (SANS Institute, 2003). The utilization of VPN significantly increases the security of the network and enables the network to share from all the levels of security features provided by it.
- **Use of Extensible Authentication Protocol (EAP):** The usage of EAP provides a centralized authentication and dynamic key distribution for the wireless network. This enhances the security features for the network against the penetration of the hackers.
- **Use of Lightweight Extensible Authentication Protocol (LEAP):** LEAP, which was introduced by CISCO in 2000, provides additional security features to EAP. These features include; secure key derivation, Dynamic WEP Keys, Re-authentication policies and Initialization vector changes, (SANS Institute, 2003).
- **V. Minimal Radio Wave Propagation:** As a control mechanism against unauthorized users, radio wave propagation in non-user areas must be minimized by ensuring that antennas are positioned in such a way that they don't cover areas that are outside the physically controlled boundaries of the facilities, (http://www.airdefence.net/products/index.shtm (30 April, 2014).). Also always hard code the MAC Addresses that can connect to the Access point.
- **The use of Temporal Key Integrity Protocol (TKIP) and Wi-Fi Protected Access (WPA and WPA2):** The TKIP is designed to address the flaws associated with WEP, and it implements a message integrity check. Similarly, the security protocols provided by WPA & WPA2 help in no small measure in addressing the deficiencies and limitations of WEP.
- **The use of Secure Socket Layer (SSL):** This is a security protocol developed mainly for internet users. Many websites employ SSL to secure the sensitive areas of their sites, such as user account pages and online checkout, (Sing, 2012). Normally, whenever an internet user log in a website, the resulting page is SSL which encrypts the data being transmitted to avoid being intercepted by hackers. The SSL is the security protocol that keeps users name, address, credit card details, etc between the user and the users' clients.

Conclusion

Wireless network communication provides several opportunities to world over including Nigeria, which increases productivity and cuts costs. This however is associated with some threats which affect the security risk of the organization that uses them. Since wireless network normally allows for expansion of network physical boundaries which gives room for both authorized and unauthorized alike to access the network, they are inadvertently subjected to some vulnerabilities and security issues. Although, it impossible to totally eliminate all security risks associated with wireless networking, it is possible to achieve a reasonable level of overall security by adopting a systematic approach of assessing and managing these risks. Generally, the network security tools for wired and wireless system in the past were command line interface (CLI) based, which are ineffective in the present day wireless network especially. This paper however, discusses some of the security issues, vulnerabilities and threats in wireless network associated with each of the three basic technology components (Clients, Access Point and the Transmission Medium) especially in Nigeria, their counter measures as well as their limitations and control mechanisms. It is recommended that, the WLAN users can protect their networks by exploiting these countermeasures mentioned in this paper ostensibly so as to mitigate the risks of wireless security issues/threats. Finally, a notable best practice for organization using WLAN is that they should have a better understanding of future trends, risks and security threats associated with it. This is to ensure that they are better prepared to make their business as secure as possible, since the inherent security issues and vulnerabilities in wireless communication had made it almost impossible to have a perfect secured

network. This will better prepared them for proper implementation and continued maintenance of the network.

REFERENCES

A beginner's guide to networking security, CISCO systems. http//www.cisco.com/ warp/public/cc/neso/sqso/beggu_pl. pdf, 2001.

AirDefence™, Inc. 'Wireless LAN Security: Intrusion Detection and Monitoring for the Enterprise'. http://www.airdefence.net/ products/index.shtm (30 April, 2014).

Al-Akhras, M. A. 2006. "Wireless Network Security Implementation in Universities". In Proc. of Information and Communication Technologies. ICTTA, 06' Vol. 2, pp. 3192-3198.

Arbaugh, W. A. 2003. "Wireless Security is Different". Magazine of IEEE Computer Society, Computer, Vol. 36. (8), pp. 99-101. http://dx.doi.org /10/1109/MC. 2003. 1220591.

Arbaugh, W., Shankar, N., Wan, Y. and Zhang, K. 2002. "Your 802.11 Wireless Networks Has No Clothes". IEEE Wireless Communication, Vol. 9. (6), pp. 44-51. http://dx.doi.org/ 10/1109/MWC.2002.1160080.

Brenton, C. and Hunt, C. 2002. Mastering Network Security. Second Edition, Wiley.

Chuah, M. and Zhang, Q. 2006. Design and Performance of 3G Wireless Network and Wireless LANs. USA: Springer.

Cisco, 2004. Dictionary attack on Cisco LEAP vulnerability, Revision 2.1, July 19.

Connect Africa Summit 2007, Kigali, Rwanda; http//www.itu.int/ITU-D/connect/Africa/2007/ summit/pdf/ s2_ background.pdf retrieved on 23/11/2015.

CSI. (2004). CSI/FBI Computer Crime and Security Survey.

Du, K. and Swamy, M. N. S. 2009. Wireless Communication System: From RF Subsystems to 4G Enabling Technologies. London: Cambridge University press.

Farrow, R. 2003. Network Security Tools. http//sageweb.sage.org/pubs/whitepaper/ farrow.pdf.

Finke II, L. G. 2000. "Wireless Communication: A modern Necessity". *Journal of Information Technology* 63, (*5*).

Graham, E., Steinbart, P. J. 2006. Wireless Security.

Hamid, R. A. 2003. Wireless LAN: "Security Issues and Solutions".

Homeland Security, 2006. "Wireless Communication Security"

Hopper, D. I. 2002. Secret Service agents probe wireless networks in Washington.

http://www.businessweek.com/ magazine/content/ 11_09/ b4217033849315.htm

http://www.wirtel.co.uk/article_africa_2005_q3_001_alvarion. htm

ISO, 2005. "Information Technology-Security Techniques-Code of Practices for Information Security Management.

Kelly, D. 2003. The X factor: 802.1x may be just what you need to stop intruders from accessing your network. Information Security, 6(8), 60-69.

Kennedy, S. 2004. Best practices for wireless network security. *Information Systems Control Journal* (3).

Khan, F. 2009. LTE for 4G Mobile Broadband: Air Interface Technologies and Performance.

Marin, G. A. 2005. "Network security basics", In security and Privacy, IEEE, Issue 6, Vol. 3, pp. 68-82.

Matt Curtin, 1998. Introduction to Network security. http://www.cs.cornell.edu/Courses/cs519/2003sp/slides/ 15_securitybasics.pdf, March, 1998.

McClure, S., Scambray, J. and Kurtz, G. 2009. Hacking Exposed: Network Security Secrets and Solutions, 6th Edition, TMH.

Miller, K. S. 2001. Facing the Challenges of Wireless Security. Technology News **17**

Mishra, A. and Arbaugh, W. A., (2002). "An Initial Security Analysis of the IEEE 802.1x Standard". Report No CSTR-4328.

Moore, L. 2006. Wireless Technology and Spectrum Demand: Advanced Wireless Services. Congressional Report for Congress.

Nokia. 2003. Man – in – the – middle attacks in tunnelled authentication protocols.

SANS Institute (2003). An overview of Wireless Security Issues.

Siddiqui, M. S. and Hong, C. S. 2008. "Security issues in wireless mesh networks". IEEE Int'l Conference on Multimedia and Ubiquitous Engineering (MUE'08).

Sing, G., (2012). Security Issues in Wireless Local Area Network (WLAN).

Stallings, W. 2006. Cryptography and Network Security, 4th Edition Prentice Hall.

Stallings, W. 2008. Network security essentials: applications and standards, 3rd Edition, Prentice Hall.

US-CERT, 2008. "Using Wireless Technology Securely a government organization". http://www.us-cert.gov/ reading_ room/home-network-security/> (2014).

Yang, H., Ricciato, F., Songwu, L. and Zhang, L. 2006. "Securing a wireless world". The Proceedings IEEE, Vol. 94. (2), pp. 442-454. http://dx.doi.org/ 10/1109/JPROC .2005.862321.

Zhu, J. and Ma, J. 2004. "A New Authentication Scheme with Anonymity for Wireless Environment". IEEE Transaction on Consumer Electronics, Vol. 50, (1), pp. 231-235.

****