Evaluating the Challenging Issues in the Security of Wireless Communication Networks in Nigeria

Ijemaru Gerald Kelechi, Udunwa Augustine Ikenna, Ngharamike Ericmoore Tochukwu, Oleka Emmanuel Uchendu

***Abstract*— Despite the gains offered by wireless communication systems, developing nations like Nigeria have been facing some stringent challenges in the security of wireless communication systems. Although Nigeria's Telecom industry has experienced continuous growth and rapid progress in policy and technological development, thus resulting in an increasingly competitive and networked world, it has however been encumbered with many security challenges. At present, wireless communications weaknesses are on the increase due to the higher demand for wireless access, demand for higher data rates, the emergence of advanced services, the need for roaming, and the large deployment of services across the globe. Consequently, this has created challenging issues in the security of wireless systems and applications operating in wireless environments.**

Nigeria witnessed stages of technological advancements in her information-dissemination techniques. Most of the techniques, such as post office, public switch telephone network, telegram and so on, are now becoming obsolete and therefore necessitate the use of other communication mediums which are not only faster, cheaper, portable, contemporary, more efficient and reliable but also have the gains and potentials of accelerating economic development as well as enhancing the lives of individuals. Consequently, the wireless communication systems such as the Global System for Mobile communication (GSM) and the internet, which are operative in Nigeria at present, have brought convenience, mobility and portability in the information and communication process. And with these, people can now transact a wide range of services formally. It is true that security of wireless networks is a global issue that needs to be addressed; the Nigerian case has more to it owing to the diverse nature of the country vis-à-vis its ethnic and religious diversities and therefore requires a critical evaluation, especially now that deregulation of the sector has taken its success.

***Key Words*— CDMA, GSM, TDMA, WLAN, Wireless Security, Wireless Communication Networks.**

I. OVERVIEW OF WIRELESS COMMUNICATIONS

Electronic communication is described as a type of communication that uses electronic circuits to transmit, receive and process information. Information itself is the knowledge or intelligence that is being communicated.

Information technology deals with the ability to electronically input, process, store, output, transmit and retrieve data and information, including text, graphic, sound and video. According to the Information Technology Association of America (ITAA), information technology is "*the study, design, development, implementation, support or management of computer-based information systems, particularly software applications and computer hardware*". Information technology increases efficiency and effectiveness of business operations. Wireless communications is thus a type of information technology that enables us to communicate anytime and anyplace. According to [4], wireless communication is the transmission of message signal via 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 is delivered via optic-fiber cable to a wired telephone or by radio signal to another wireless phone.

II. WIRELESS EVOLUTION & ADVANCEMENTS

The birth of wireless communications is credited to M.G Marconi in the late 1800s, when he successfully pioneered a work of establishing a radio link between a land-based station and tugboat [2]. This was succeeded by Fessenden in 1906 which saw the invention of amplitude modulation (AM) for music broadcasting, and 1933 saw the invention of frequency modulation (FM) by Edwin H. Armstrong [3]. Indeed, the last two decades saw an explosion in the advancements of wireless systems. Wireless communications systems migrated from the first-generation (1G) which used narrow-band analogue signaling for voice transmission in 1980s, to the second-generation (2G) narrow-band systems in the 1990s, which used digital communication techniques with TDMA, FDMA or CDMA. 2G was deployed for the transmission of voice signal operating on GSM 900MHz with GPRS 56Kbps to 114Kbps. 2G technology also saw the invention of the Global Systems for Mobility (GSM), personal digital cellular (PDC), IS-136, and IS-95, which make use of digital transmission techniques. Currently, different wireless technologies (e.g. GSM, CDMA, and TDMA), are deployed throughout the world for 2G, 2.5G, and eventually 3G networks. According to [8], 2.5G network offered a higher data rate of 144Kbps which was far much higher than 2G and also was used to deliver basic data services like text messages. However, 2.5G could not be used to download an image or browse a website from a PDA [7]. Members of this family of technology include GPRS, EDGE and CDMA2000. The conception of 3G technologies commenced just as 2G began to roll out. The design and deployment of 3G networks were aimed at overcoming all the limitations of the 2G technologies by offering more advanced and innovative services such as high-bit-rate and broadband multimedia services.

Manuscript Received on May, 2014.

G. K. IJEMARU, is a lecturer in the department of Electrical & Electronics Engineering, Federal University Oye Ekiti, Ekiti State, Nigeria. .

A. I. UDUNWA, is a lecturer in the department of Information Management Technology, Federal University of Technology Owerri Imo State, Nigeria..

E. T. NGHARAMIKE, is a graduate assistant in the department of Computer Science, Federal University Oye Ekiti, Ekiti State, Nigeria..

E. U. OLEKA is a lecturer in Electrical & Computer Engineering, University of Uyo, Nigeria.

According to [10], 3G systems should be able to make information services instantly available and should prove roaming capabilities. The Universal Mobile Telecommunications System (UMTS) is a 3G cell phone technology, which is also being developed into a 4G technology. 3G technologies used digital communication techniques that involved the transmission of voice signals as well as multimedia services. It is expected that the 4G technology (a term used to describe the next step in wireless communications) should be able to provide a comprehensive IP solution where voice, data and streamed multimedia could be given to users on “anytime” “anywhere” basis, and at a higher data rate than the previous generations. According to [8], a 4G is the technology considered to complete the cycle of technological advancements in wireless communications, with features that will permit a much faster velocity in data transfer and wider area coverage than with the current 3G.
Incidentally, wireless communications systems have gone through series of tremendous advancements with a furious pace. For instance, in 2002, mobile phones worldwide began to outnumber fixed-line phones. By November 2007, the number of subscriptions to mobile phones worldwide dangled around 3.3 billion, and just then, more than 798 million people worldwide had access to the internet or equivalent mobile internet services [3]. The early wireless systems composed of a base station with a high-power transmitter and covered a significantly large geographic area. Each of the base stations served only a small number of users and was also costly. There was lack of compatibility in the systems with only a few communicating with the public switched telephone networks (PSTN). Today, however, there has been significant increase in the number of base stations with low-power radio transmitters, which now cover a large geographic area. This has consequently led to the proliferation of mobile systems around the globe. To date, mobile services have witnessed four stages of progression ranging from simple communication, high-speed downloading, high-speed downloading and uploading, to real-time latency-sensitive services, which were all enabled by wireless technology. In addition to the multimedia services such as speech, audio, video, and data, the pervasive use of wireless communications could also be traced to various aspects of our lives, including health care, home, automation, etc, such that lack of wireless service is seen as preposterous to network users who can no longer do without it.

III. BLOCK DIAGRAM OF A COMMUNICATION SYSTEM

A communication system deals with the transmission of information from one point to another. Fig. 3.1 shows a block diagram of a digital communication system. According to [3], the diagram may also be applicable to remote sensing systems such as radar and sonar in which the transmitter and receiver may have the same location. Hence, the source generates either analogue signals (e.g. speech, audio, image, and video) or digital data such as text or multimedia. Information from the source is passed to the source-encoder which generates binary data. The generated binary data is then encoded in a channel and is modulated to generate waveforms for transmission over a channel. The channel is subject to various types of impairments (e.g. noise) due to its open nature. At the receiver, the whole process is reversed so as to finally restore the original source information.

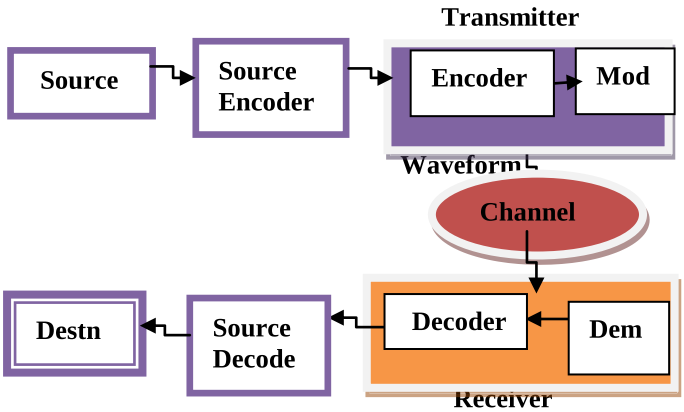

Fig. 3.1 Block Diagram of a general Comm. System

IV. INTRODUCTION TO WLAN

A Wireless Local Area Network (WLAN) is a flexible data communications system that can use either infrared or radio frequency technology to transmit and receive information over the air. The first WLAN standard – 802.11 was implemented in 1997 based on radio technology operating with a frequency of 2.4 GHz and a maximum throughput of 1 to 2 Mbps [5]. The most current standard, IEEE 802.11b, was introduced early 2000 with the same frequency range but has a maximum speed of 11 Mbps. One major advantage of WLAN is the simplicity of its installation which usually eliminates the needs to pull cable through walls and ceilings. The basic units of a WLAN are access points (Aps) and Network Interface Cards (NICs)/client adapters.

V. WIRELESS SECURITY ISSUES

Wireless communications security refers to measures taken to ensure that the confidentiality and integrity of the information transmitted via a wireless means are not compromised. It entails any measures put in place to ensure the prevention of unauthorized access or damage to information transmitted over wireless networks. According to [6], security of wireless communications systems can be grouped into four major components such as physical security, network security, communications security and administrative security. Physical security ensures the protection of all the facilities where communications system components are housed; network security ensures the protection of system’s hardware, software, and associated interfaces; communications security ensures the confidentiality and integrity of information transmitted over the airwaves; while administrative security involves the use of procedural controls to ensure the confidentiality, integrity, and availability of communications systems. Some of the issues relating to wireless networks as noted by [5], [7], [12] and [13] are summarized as follows:

- ***Eavesdropping on Non-secured Channels:*** This involves the act of illegitimate interception and reception of information transmitted over a wireless communications system.

It has to do with an attack against the confidentiality of the data being transmitted over the network [5], and is possible because of the ease with which network signals are received outside the vicinity of the valid users. This enables an attacker to hijack the signal over the air from a certain distance

- ***Electromagnetic Interference:*** This results in signal fading and disruption of wireless signals as a result of too long a distance between the transmitter and the receiver, atmospheric conditions or metallic surfaces which reflect the radio waves and also due to obstacles in the line-of-sight.
- ***Overloading of Bandwidth:*** This is caused by piggybacking, which is an access to someone else's wireless internet connection by another who lives within the neighborhood of the wireless connection, without the due consent and knowledge of the main subscriber. Piggybacking can also cause service violations, direct attack on your computer and illegal activities by malicious users which may be traced to you.
- ***Wireless Sniffing:*** Many public access points are not secured, and the traffic they carry is not encrypted. This can therefore put your sensitive communications or transactions at risk. Here, the attacker uses "sniffing" tools to invade such sensitive information like passwords, bank account numbers, credit card details and so on. Similar to this is ***Shoulder Surfing***, which makes use of direct observation techniques such as looking at someone's shoulder to fetch information.
- ***Denial of Service (DoS):*** Wireless intruders can flood the network with either valid or invalid messages affecting the availability of the network resources by using a powerful transceiver enough to cause interference effects on the WLAN network. This probably makes WLAN unable to communicate using the radio path. Since DoS would ordinarily cause network interruption thereby preventing data transmission, the intent behind it is to observe the recovery of the wireless network by the malicious attacker, during which all the initial codes are re-transmitted by the valid users thereby paving way for the attacker to record these codes with various cracking devices that will aid him to break the security and gain unauthorized access to the system.
- ***Spoofing and Session Hijacking:*** This involves a case whereby an attacker illegitimately gains access to privileged data and resources in the network by impersonating the identity of a valid user. This has been possible because 802.11 networks do not authenticate the source address, which is Medium Access Control (MAC) address of the frames. According to [9], spoofing can be eliminated by ensuring that proper authentication and access control mechanisms are put in place in the WLAN.
- ***Traffic Redirection:*** This involves a change in the traffic route of a particular computer to that of a malicious attacker by manipulating the media access control (MAC) address as well the IP address of a particular wired station.
- ***Rogue Access Point:*** A rogue Access Point is one that is installed by an attacker (usually in public areas such as shared office space, airports etc) to accept traffic from wireless clients to whom it appears as a valid Authenticator. Packets thus captured can be used to extract sensitive information or can be used for further attacks before finally being re-inserted into the proper network.
- ***Caffe Latte Attack:*** This is a process that enables the intruder to break into the WEP key of a remote client by sending a flood of encrypted ARP requests. He takes the advantage of the flaws in 802.11 WEP and uses the ARP responses to obtain the WEP in just few minutes.

VI. IEEE 802.11B SECURITY MEASURES AND THEIR LIMITATIONS

The security features provided by 802.11b standard as noted by Sing (2012) are as follows:

- **SSID – Service Set Identifier:** Here, all devices trying to get access to a particular WLAN must first be configured with the same SSID. It is added to the header of packet sent over the WLAN and verified by Access Point. Hence, a client cannot communicate with a particular access point unless both have the same SSID configuration. It provides very little security as it is more of a network identifier than a security feature. The SSID and the access point name are not encrypted in the header of 802.11 packets. WLAN scanners will detect these values and when you provide these descriptions it becomes easier for an attacker to identify the source of the signal.

- **WEP – Wired Equivalent Privacy:** This is a standard encryption mechanism for wireless networking used to overcome the security threats. "WEP is an algorithm that's used to protect wireless communications from eavesdropping and modification. A secondary function of WEP is to prevent unauthorized access to a wireless network. It relies on a secret key that is shared between a wireless station and an access point. The secret key is used to encrypt packets before they are transmitted and an integrity check is used to ensure the packets are not modified in transit [11]. It provides security by encrypting the information transmitted over the air, so that only the receivers with the same encryption key can decrypt the information [5]. The initial intent was to provide data "confidentiality" that has semblance with that of a typical wired local area network (LAN), which does not employ cryptographic techniques to enhance privacy. Unlike WLANs that require an encryption mechanism, wired LANs do not necessarily need to be encrypted since they have physical security such as walled structures and controlled entrance to building. WEP utilizes an encryption WEP key. The message signal is first encrypted with the WEP key and is sent to the receiving station which decrypts the message using the same WEP key. WEP uses RC4 encryption algorithm and CRC -32 (Cyclic Redundancy Code) checksum algorithms as its stream cipher. However, there has been a lot of growing concerns regarding the integrity of WEP.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

The following therefore are some of the limitations and vulnerabilities associated with WEP as posited by [5] and [12] – (i) WEP does not provide any forgery protection thereby making it possible for an attacker to masquerade as an authentic user and deliver data to unauthorized parties by manipulating the encryption key or even without the key. (ii) There is also no protection against replays. Such an attacker can create forgeries without changing any data in an existing packet by simply recording WEP packets and then retransmitting later. (iii) By reusing initialization vector, WEP enables an attacker to decrypt the encrypted data without having to learn the encryption key. The IEEE 802.11 design community blames 40-bit RC4 keys for this and recommends using 104- or 128-bit RC4 keys instead. Although using larger key size can increase the work of an intruder, it does not necessarily provide completely secure solution.

- **MAC – (Media Access Control) Address Authentication:** Here, the access point is configured to accept association and connection requests from only those nodes whose MAC addresses are registered with it. This scheme makes provision for an additional security layer. The problem with this scheme lies in the fact that an attacker who manages to steal a laptop with a registered MAC address will continue to appear to the network as a legitimate user.

VII. WIRELESS SECURITY CONTROL MECHANISMS

Despite notable risks and vulnerabilities common with wireless communications, a number of mechanisms are in place to checkmate some of these security lapses and limitations. The following are some of the security control mechanisms as posited by [5], which include:

- Change the default SSID as regularly as possible. The Service Set Identifier (SSID) is a unique identifier usually attached to the header of packets sent over wireless networks, which acts a password when a mobile device tries to connect to a particular WLAN. It is recommended that this identified is changed regularly as doing otherwise is a common security mistake often committed by WLAN administrators. It is also advised not to use a descriptive name for the SSID or the Access Point [11].
- Utilize Virtual Private Network (VPN). This is a network technology which creates a secure connection over a public network such as the internet or a private network owned by a service provider. This is common with large corporations, educational institutions, and government agencies. A VPN is capable of connecting multiple sites over a large distance similar to that of a Wide Area Network (WAN). According to [11], a VPN provides high security for the wireless network implementation without adding significant overhead to the users. A VPN technology provides three levels of security which includes Authentication, Encryption and Data Integrity.
- Change the Default Passwords and IP Addresses
- Hard code the MAC Addresses that can connect to the Access point
- Use the Extensible Authentication Protocol (EAP). This provides a centralized authentication and dynamic key distribution.
- Use the Lightweight Extensible Authentication Protocol (LEAP). This was introduced by Cisco in the year 2000 to provide additional security feature to EAP, which includes secure key derivation, Dynamic WEP keys, Re-authentication policies, and Initialization Vector changes [11].
- Access Point placement should be done outside the firewall in order to prevent a hacker from accessing corporate network resources.
- Minimize radio wave propagation in non-user areas by positioning antennas not to give coverage to areas outside the physically controlled boundaries of the facility [1].
- Use of smart cards, USB tokens and Software tokens
- Use the Temporal Key Integrity Protocol (TKIP). This was designed to address the flaws associated with WEP, and it implements a message integrity check.
- The Wi-Fi Protected Access (WPA and WPA2). These security protocols were also developed to address the deficiencies of WEP.
- Secure Socket Layer (SSL). This is a security protocol developed for internet users. Many websites use SSL for secure areas of their sites, such as user account pages and online checkout [12]. Normally, when an internet user logs in on a website, the resulting page is SSL which encrypts the data being transmitted to avoid being intercepted by a third party. It is this security protocol that keeps your name, address, credit card details between you and your client.

VIII. CONCLUSION

WLAN was developed to provide security features similar with those of wired LAN. Since this would normally require an expanded physical boundary which gives access to both authorized and unauthorized users, WLAN is inadvertently subjected to various vulnerabilities and security issues. Some of the security concerns were x-rayed, their limitations and control measures also discussed in this paper. It is instructive that WLAN users can protect their networks by exploiting the suggested actions that are mentioned in this paper ostensibly based on the cost implications and the level of security deficiencies. However, wireless communication networks have inherent vulnerabilities thereby making it almost impossible to have a perfect secured network. Therefore, a notable best practice to secure WLAN is to have adequate security knowledge, proper implementation and continued maintenance.

ACKNOWLEDGMENT

G. K. IJEMARU expresses gratitude to Mrs Peace Gerald for her love and encouragements towards the realization of this work. A. I. UDUNWA wishes to thank Mrs Peace Ikenna for her support and love.

REFERENCES

1. AirDefense™, Inc. 'Wireless LAN Security: Intrusion Detection and Monitoring for the Enterprise.' URL: http://www.airdefense.net/products/index.shtm (30 April 2014).
2. Chuah, M., and Zhang, Q. (2006) Design and Performance of 3G Wireless Network and Wireless Lans. USA: Springer
3. Du, K., and Swamy, M.N.S. (2009) Wireless Communication Systems: From RF Subsystems to 4G Enabling Technologies. London: Cambridge University press
4. Finkle II, L.G. (2000) 'Wireless Communications: A Modern Necessity.' Journal of Information Technology 63, (5)
5. Hamid, R.A. (2003) 'Wireless LAN: Security Issues and Solutions'
6. Homeland Security (2006) 'Wireless Communications Security.' [online] available from http://www.safecomprogram.gov/NR/rdonlyres/7F55866C-13B5-419E-B698-1C4022696A49/0/Wireless_Communications_Security_090607.pdf [6th May 2010]
7. ISO (2005) 'Information Technology-Security Techniques-Code of Practice for Information Security Management.' [online] available from http://www.iso.org/iso/support/faqs_widely_used_standards/widely_used_standards_other/information_security.htm [10th May 2014]
8. Khan, F. (2009) 'LTE for 4G Mobile Broadband: Air Interface Technologies and Performance'
9. Miller, K. S. (2001) 'Facing the Challenges of Wireless Security.' Technology News 17 July: 16-18
10. Moore, L. (2006) 'Wireless Technology and Spectrum Demand: Advanced Wireless Services.' Congressional Research Services (CRS) Report for Congress
11. SANS Institute (2003) 'An Overview of Wireless Security Issues'
12. Sing, G. (2012) 'Security Issues in Wireless Local Area Networks (WLAN)'
13. US-CERT (2008) 'Using Wireless Technology Securely a government organization.' [Online] Available from <http://www.us-cert.gov/reading_room/home-network-security/> [12th March 2014]

AUTHORS PROFILE

Engr. G. K. IJEMARU is a lecturer in the department of electrical and electronics engineering, Federal University Oye Ekiti, Ekiti State. He has taught in various institutions of higher learning. He worked as a transmission/maintenance engineer with the Federal Radio Corporation of Nigeria before proceeding to the United Kingdom for Postgraduate studies. He obtained his MSc from Coventry University United Kingdom, and is currently undergoing his PhD program. He has many publications.

Mr. A. I. UDUNWA is a lecturer in the department of Information Management Technology, Federal University of Technology Owerri. He obtained his MSc from Coventry University United Kingdom, and is currently undergoing a PhD program. He has many publications

.

Mr. E. T. NGHARAMIKE obtained a Bachelors degree in Computer Science at Federal University of Technology, Owerri, Imo State Nigeria**. He** is a graduate assistant in the department of Computer Science, Federal University Oye Ekiti. He is currently undergoing an MSc program.

Engr. E.U OLEKA obtained a B.Eng and M.Eng in Electrical & Electronics Engineering from Enugu state University of Science and Technology, Enugu Nigeria. He is lecturer in the department of Electrical and Computer Engineering, University of Uyo and he is currently pursuing a PhD program in North Carolina Agricultural and Technical State University, Greensboro NC, USA.