Computing, Information Systems, Development Informatics & Allied Research Journal
Vol. 8 No. 1, March, 2017 - www.cisdijournal.net

An Enhanced Wireless Network Security Framework for Federal Road Safety Corps in Nigeria

Oladeji, F.A.
Department of Computer Science
University of Lagos
Akoka, Lagos State, Nigeria
faoladeji"unilag.edu.ng

Akeredolu, E.I.
Driver Licence Center
Federal Road Safety Commission, Nigeria
Email address: paidowu@oauife.edu.ng

Komolafe, O.
Engineering Materials Development Institute
Federal Ministry of Science & Technology,
KM 4, Ondo Road Akure, Nigeria

Oyetunji, M.O.
Department of Computer Science and Mathematics
Mountain Top University
Ibafo, Nigeria
Email address: mooyetunji@mtu.edu.ng

ABSTRACT

Wireless Network Security: Consideration Design for an Enterprise Network taking Federal Road Safety Corps (FRSC) as a case study is a research embarked on to identify the existing network framework of wireless network in FRSC, to select the best network framework, modify the best network and propose the modified wireless network framework that will enhance better security for FRSC wireless network. This paper studied the security settings of Wireless Local Area Network (WLAN), their vulnerability, and alternative solution (s), in FRSC wireless LAN. It presents results from a comprehensive assessment of wireless network security in a large wireless LAN which is the FRSC wireless LAN. The method employed in this paper was achieved through physical observation of five (5) access points in the five categories of FRSC network spread over the formation of the Corps with the use of Network Performance Metrics (NPM) parameters. The personnel at the Information Technology Centers (ITC) of each office were directly interviewed on the standard and the performance of their WLAN. From the physical observation conducted on the five formations, it was discovered that almost all the formations visited are running on WPA and MAC Address security type and IEEE 802.11a, 802.11b and 802.11g as radio type for the network channels. These security types have been deduced that they are not capable enough to shield the network from outside attackers. In conclusion, this paper identified and discussed the potential problem(s) and appropriate solution(s) which is the use in WPA2 for the improvement of the wireless network in terms of security settings for effective and secure communication putting access control in to cognizance.

Keywords: FRSC, WLAN, LAN, WPA2, Network Security,

CISDI Journal Reference Format
Oladeji, F.A., Akeredolu, F.I., Komolafe, O. & Oyetunji, M.O. (2017): An Enhanced Wireless Network Security Framework for Federal Road Safety Corps in Nigeria. Computing, Information Systems & Development Informatics Journal. Vol 8 No 1. Pp 161-172

1. INTRODUCTION

Security is the degree of resistance to, or protection from harm (Caravan, 2001). It applies to any vulnerable and valuable asset, such as a person, dwelling, community, nation, or organization. This could be termed 'security in its common sense'. Security provides a form of protection where a separation is created between the assets and the threat. The physical realm of security include Airport security, Aviation security, Communications security, Corporate security, Food security, Home security, Infrastructure security, Physical security, Port security/Supply chain security, Private security, School security, Shopping center security and Transportation security (Muhammad-Tukur, 2011).

In the Information Technology (IT) perspective, security can involve the following: Computer Security, Internet Security, Application Security, Data Security, Information and Network Security which is the focus of this paper. Network Security is a measure put in place to protect data during transmission within an organization (Curtin, 1997). An effective network security demands an integrated defense-in-depth approach. The first layer of a defense-in-depth approach is the enforcement of the fundamental elements of network security. These fundamental security elements form a security baseline, creating a strong foundation on which more advanced methods and techniques can subsequently be built (Cisco, 2008). Network security has become more important to personal computer users, organizations, and the military alike. With the advent of the internet, security has become a major concern and the history of security allows a better understanding of the emergence of new security technology (Bhavya, 2010). The internet structure itself has allowed for many security threats to occur on organizational networks. The architecture of the internet when modified can reduce the possible attacks that can be sent across the network. Knowing the attack methods, allows for the appropriate use of security measures to be applied. Many business organizations protect themselves from the internet by means of firewalls and encryption mechanisms over their network. The business organization creates an Intranet for internal network purposes can also be connected to the internet but must be secured from possible threats (Daya, 2002).

Security itself could be categorized into four major categories viz: IT realm, Physical realm, political and monetary (Serpanos, 2002). The IT realm of security deals on aspect of technological life security mentioned above. There could be Airport Security, Communication Security, Aviation security, corporate Security, Home Security and the likes as the physical realm of security. State Security, Internal Security, National Security, International Security, Homeland Security and Human Security are in the political realm of Security while Social Security, Financial Security and Economic Security are in the monetary family of security. Wireless security is the prevention of unauthorized access or damage to IT infrastructure (computer hardware and software, data communication path and database) using wireless networks. The most common types of wireless security are Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA) (Adeyinka, 2008). WEP is a notoriously weak security standard, the password it uses can often be cracked in a few minutes with a basic laptop computer and widely available software tools (Sotillo, 2006). WEP is an old IEEE 802.11 standard created in 1999, which was outdated in 2003 by WPA. WPA was a quick alternative to improve security over WEP.

The current standard is WPA2; which some hardware cannot support without firmware upgrade or replacement. WPA2 uses an encryption device that encrypts the network with a 256-bit key; the longer key length improves security over WEP. Many laptop computers have wireless cards pre-installed. The ability to enter a network while mobile has great benefits. However, wireless networking is prone to some security issues (Kartalopoulos, 2008). Hackers have found wireless networks relatively easy to break into, and even use wireless technology to hack into wired networks. As a result, it is very important that enterprises define effective wireless security policies that guard against unauthorized access to important resources (Cisco, 2008). Wireless Intrusion Prevention Systems (WIPS) or Wireless Intrusion Detection Systems (WIDS) are commonly used to enforce wireless security policies.

The risks to users of wireless technology have increased as the service has become more popular, although, there were relatively few dangers when wireless technology was first introduced (Dowd, 1998). Hackers had no time to latch on to the new technology, and wireless networks were not commonly found in the work place. However, there are many security risks associated with the current wireless protocols and encryption methods, and in the carelessness and ignorance that exists at the user and corporate IT level. Hacking methods have become much more sophisticated and innovative with wireless access. Hacking has also become much easier and more accessible with easy-to-use Windows- or Linux-based tools being made available on the web at no charge. The Institute of Electrical and Electronics Engineers (IEEE) 802.11 Wireless Local Area Network (WLAN) has become the effective standard for wireless networking since it was introduced in 1999, providing mobility and connectivity at relatively low cost (Wee, 2004). However, the key concern with the 802.11 WLANs has been security. Wireless signals can travel long distances and are not bounded by physical boundaries such as walls and perimeters. Since the Radio Frequency (RF) spectrum is a shared medium, wireless signals can also be picked up by unintended recipients such as potential attackers using the right equipment available to them. When wireless signals are sent across radio waves, interception and masquerading becomes trivial to anyone with a radio (Borisov, 2002). This can compromise the confidentiality, availability and integrity of information in a network.

This paper addresses the problem of designing secure 802.11-based wireless network architecture for an enterprise by providing insight on developing trends and technologies adequate to provide secured wireless networks for Federal Road Safety Corps (FRSC). FRSC is a government paramilitary organization that is saddled with the responsibility of creating safe motoring environment on Nigerian roads. The organization is to make sure that there are no obstructions on Nigeria roads. FRSC has, in pursuit of these and other important vision, put in place strategies that will actualize the enforcement of the above. Part of the strategies is creating a robust database for all vehicles and vehicle owners. FRSC has information about all vehicles and vehicle owners, detailed record of traffic offenders and their offences including the time the offence was committed. It also has records of the fines to be paid and fines paid. This makes an organization like FRSC to be prone to hackers finding a way into its network.

There is therefore a need to design a framework for the deployment of safe and reliable wireless network architecture for the FRSC using the IEEE 802.11i – WPA2 protocol required for the protection of information confidential to FRSC.

2. RELATED WORKS

In order to design the framework for deployment of secured, reliable and efficient wireless network architecture for FRSC some related works were reviewed as follows:

In 2008, a study was undertaken to find out if wireless networks are inherently insecure thereby limiting enterprise deployment. What are the known holes, and to see if they can be fixed. The author tried to answer these questions through comprehensive and broad literature study. The study shows that wireless LANs are prone to many different kinds of attacks –ranging from passive to active, and that wireless security initiative has come a long way, from weak WEP to a more robust WPA2. It also show that optimal security solution for Wireless LANs involves a combination of security technologies, and that vulnerability assessment and risk analysis are essential for development of effective security policy and determination of appropriate security measures for risk mitigation (Nwabude, 2008).

The study really dealt in WLAN standards and focused on IEEE 802.11 family, showing a systematic comparison its components: IEEE 802.11b, IEEE 802.11a, IEEE 802.11g, IEEE 802.11n, 802.11h, 802.11j and 802.11i. It also evaluated the current known IEEE 802.11 wireless LAN vulnerabilities and threats. It ends with sections which explain how to discover wireless network threats, and what to do to reduce or eliminate the threats. The aim is to encourage network and security administrators to carry out risk assessment so as to identify the risks and threats relating to their information system, and then deploy adequate control measures to reduce or eliminate possible risk (Nwabude, 2008). In 2011, Shehu studied the security settings of Wireless Local Area Network (WLAN), their vulnerability, and alternative solution(s), on ABU wireless LAN. The research work present results from a comprehensive trace of wireless network security in a large wireless LAN which is the ABU wireless LAN using two software tools as CommView for Wi-Fi for packet capture on the network, and Aircrack-ng for decrypting the encryption found in some Access Points (AP) within the network coverage range. This has been carried out using the campus-wide network of more than 100 access points (APs) spread over the buildings of the University.

Potential problem(s) and appropriate solution(s) which is the use of WPA2 has also been discussed for the improvement of the wireless network in terms of security settings for effective and secure communication putting access control in to cognizance. This was done to carry out an empirical study on wireless network security behaviour, taking ABU wireless network as the case study for appropriate data; to analyze the data gotten from the study with respect to the security of the network; to suggest a better security mechanism and management techniques for a secured, effective and efficient communication, from the wireless network within the main campus, and the entire University (ABU, Zaria) at large putting access control in to cognizance, by connecting and reading data from access points within the wireless coverage range across the entire campus, to the laptop using the CommView for Wi-Fi software tool; using Aircrack-ng software tools to study the security setting for its strength or otherwise; an Enhance encryption mechanism has been given with its simulated instance (Muhammad-Tukur, 2011).

Implementation of Wireless Security on Wi-Fi according to Arashpour, 2011 was aimed at making Virtual Wi-Fi driver more secure. The main challenge is how to implement WPA and WEP in this driver, to scrutinize Virtual Wi-Fi driver and find out how it works. It also propose a method or service which can be utilized in Windows XP to make Virtual Wi-Fi driver more secure than simple WEP which is implemented in its last version. This was done with adequate knowledge on Wi-Fi, wireless security and Network Driver Interface Specification (NDIS) and adding required C++ code to implement wireless security in the Wi-Fi driver. The work focused on designing and implementing a proposed improved virtual Wi-Fi driver. This research proposed new Virtual Wi-Fi that can communicate with wireless networks which support WEP and/or WPA as their wireless security. Implementing dynamic WEP by configuring periodic time of key changing and implementing WPA by configuring TKIP algorithms have done in Virtual Wi-Fi source codes (Arashpour, 2011).

1.METHODS
2.

3.1 Data Identification and Collection Methods

The data used for this paper were identified majorly by direct system observation at the strategically selected locations in FRSC formation. The collection method adopted was direct interview of the personnel in charge of FRSC Information Technology Center in each formation visited. The FRSC is basically for the purpose of this study seen in five categories viz: The National Headquarter, The Zonal Commands, The Sector Commands, The Unit Commands and the Driver's License Centers. Particular location was picked from each of these categories based on proximity, and were physically visited to see what and how the WLAN in these centers are configured and distributed. The personnel in charge of the IT package in each of the selected commands were interviewed and mode of operation of each was studied.

3.2 Identification of Existing Frameworks for Wireless Network Architecture in the FRSC

The existing framework for wireless network architecture in FRSC was identified through direct interview of the personnel in charge of the IT systems (Information Technology Center Staff) in five categories of Command in FRSC. The categories are as follows:

i. FRSC Headquarters in Abuja (RSHQ)
ii. FRSC Zone 8 Headquarters in Ilorin (RS8HQ)
iii. FRSC Ekiti Sector Comand in Ado Ekiti (RS8.2)
iv. FRSC Ido Unit Command in Ido Ekiti (RS8.21) and
v. FRSC Drivers License Center Ido-Osi.

The existing framework for wireless network architecture in these commands was viewed under the Network Performance Metric (NPM) parameters. The NPM parameters that are used for the purpose of this thesis are availability, loss, delay, utilization and the Security radio which is the major point of consideration in the research work.

Network Performance Metric (NPM) is the basic metric of performance measurement in the network management layer. The NPM is categorized into four types, namely: Availability, Loss, Delay and Utilization (Figure 3.1).

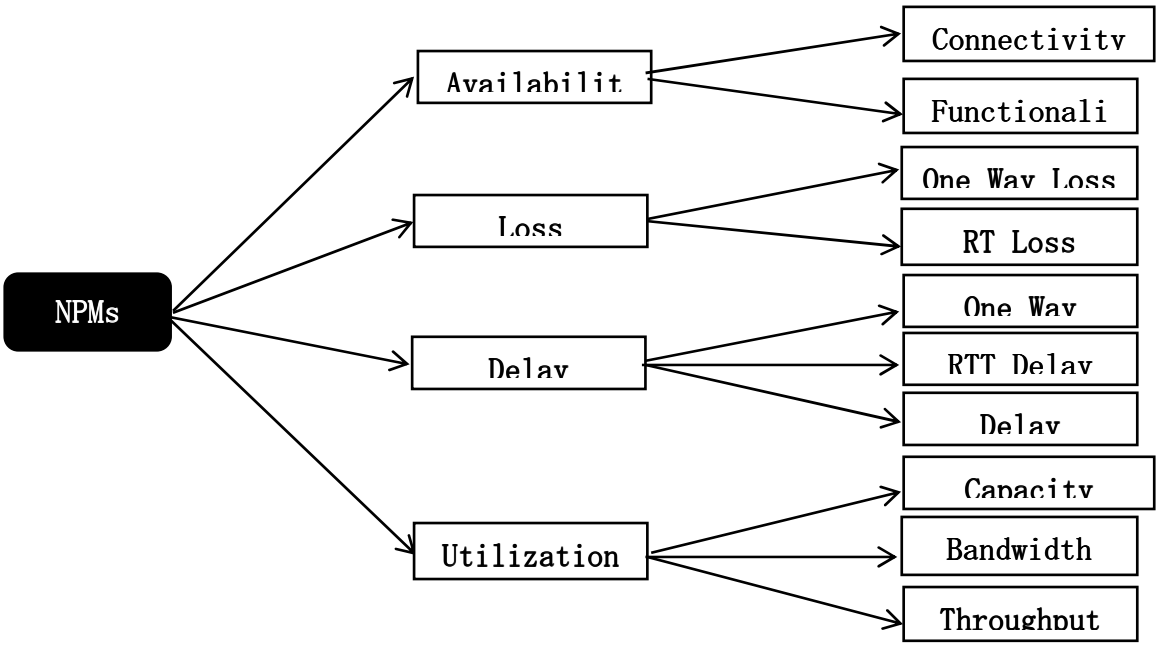

Figure 3.1: Network performance metrics model

3.2 Selecting the Best Network Framework for Wireless Network in FRSC

The best network framework for wireless network in FRSC was selected by looking at the characteristics of each of the IEEE 802.11 wireless LAN standards; more importantly, frequencies at which each standard is operating was compared and at the same time comparing their bandwidths. Network performance metrics was majorly used to make the selection of the network framework that is best suitable and used for wireless network in FRSC. The standards with higher frequencies, wider bandwidth, less loss and delay are preferred to otherwise.

3.3 Proposing an Effective Wireless Network Framework for FRSC

It is imperative to note that the focus of this paper is to take a critical look in considering wireless network security as an important tool in designing an enterprise network. Therefore, considering the existing wireless network in FRSC and having a security based wireless network at heart to achieve a secure wireless network, there arises need to modify the best wireless network standards within the existing wireless network in FRSC. The proposal of an effective wireless network framework for FRSC was achieved by modifying the best known IEEE 802.11 standards operating in FRSC at large. The modification is done by placing priority on the Security of the wireless networks. Hence IEEE 802.11i that caters for wireless network Security was introduced into the framework to bring in new wireless network.

In summary, in order to design the framework for FRSC, existing frameworks for wireless network deployment within the FRSC were reviewed. Also, a comparative analysis of the existing wireless network framework were performed using network performance metrics with the best selected; and modified effective wireless network framework by introducing security mechanism IEEE 802.11i standard (WPA2).

4. RESULTS AND DISCUSSION

4.1 Existing Wireless Network Architecture in FRSC

Figure 4.1 shows a description of the FRSC existing wireless network framework. The wireless network architecture in FRSC was observed in five different commands which are picked with the five categories of the corps formation. The following are the commands observed:

- The FRSC headquarters
- The zonal quarter (RS8HQ, Ilorin)
- The Sector Commands (RS8.2)
- The Unit Commands (RS8.21) and
- The Drivers' License Center (DLC, Ido Ekiti).

Table 4.1 shows the analysis of the wireless network features of the five categories of the Corps. From the table below, wireless network architecture that is secured with WPA and MAC Address filtering are seen to be the best network architecture. In Mac Address filtering, every wireless card has a special ID, named as MAC address. This MAC address is unique and will not be the same to any other wireless card, just as your personal ID belongs to you only.

If there is a way to instruct the wireless router (or wireless AP) to allow that MAC address of a wireless card only, while prohibiting all others, then a wireless network will know the wireless PC only, denying all other unwelcomed visitors (other unknown wireless PC). The MAC address does much in protecting the network from intruders to a reasonable extent. It should be noted that MAC Address filtering does not totally address the issue of security breach in wireless network; hence a better approach is hereby proposed. So from the table, the best network architecture is described in Figure 4.1.

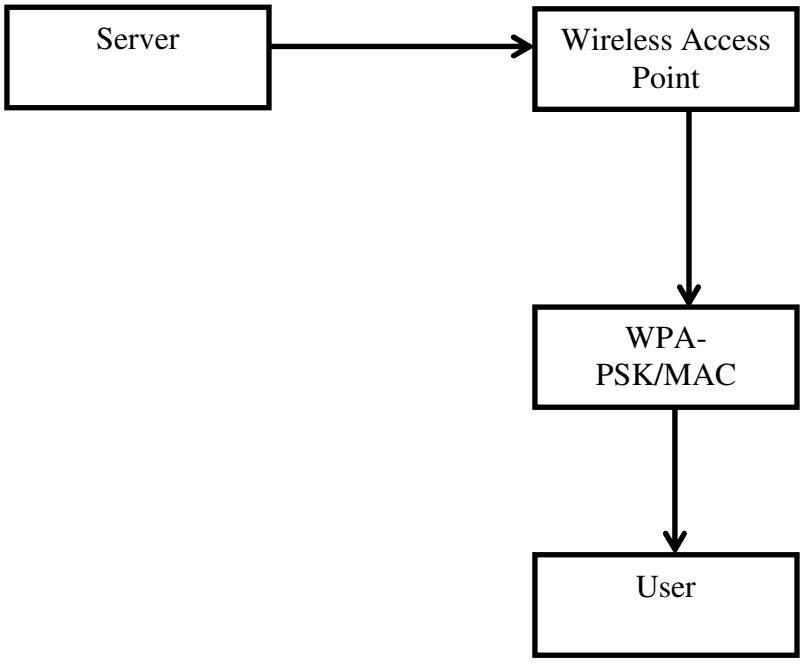

Figure 4.1: Existing wireless architecture

Table 4.1: Features of FRSC wireless LAN network architecture

Command	SSID	Signal Strength	Link Speed	Security Type	Radio Type	Service Provider
RSHQ	FRSC-HQ	Excellent	100Mbps	WPA and MAC Address Filtering	802.11a, 802.11b 802.11g	Blue Sky And Galaxy Sat
RS8HQ	FRSC-RS8HQ	Good	80Mbps	WPA-PSK and MAC Address Filtering	802.11b 802.11g	Blue Sky
RS8.2	FRSC-ADO	Excellent	54Mbps	WPA-PSK	802.11g	Galaxy Sat
RS8.21	FRSC-IDO	Excellent/Good	54Mbps	WPA-PSK	802.11g	Galaxy Sat
Ido DLC	DLC-IDO	Excellent	100Mbps	WPA-PSK	802.11g	Galaxy Sat.

4.2 Existing Architecture in FRSC Network

From the wireless network architecture analysis shown in Table 4.1, it was deduced that the architecture is well channeled with the quality of the signal and the security type. But it was observed that the original native security mechanism for wireless local area networks (WLANs) in the Institute of Electrical and Electronics Engineers (IEEE) 802.11 specification was not utilized in any of the centers. This could have been because the security mechanism for WLANs is a later innovation of IEEE 802.11 that basically deals on securing Wi-Fi. The major modification that is done to this existing framework is to introduce this later innovation of IEEE standards that is basically based on security mechanism for securing Wi-Fi. This security mechanism for WLANs is termed Wi-Fi Protected Access 2 (WPA2) using the IEEE 802.11i standards.

FRSC wireless network which is a design that is tailored towards an enterprise network; more importantly when it is being used for offenders' dashboard, drivers' license processing and vehicle number plate registration, it is important that network security be given high priority. Therefore, for a network that will be safe for an organization like this, it is imperative that important security features are involved in their wireless network. In a world where everyone is dynamically becoming more technologically oriented every day and hackers are intruding into network every moment with up to date hacking software, it becomes highly imperative that enterprise networks like that of FRSC are well protected from hackers due to the sensitivity of information they keep and the importance of same to the masses and the government. Therefore, the best network architecture that corresponds with the level of security needed in network is the WPA2 network architecture, IEEE 802.11i. The proposed architecture is simply shown in Figure 4.2.

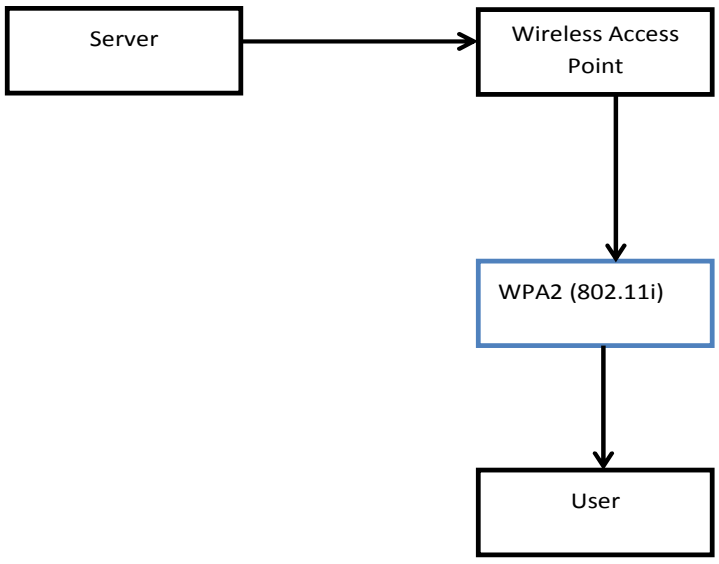

Figure 4.2: Proposed (Modified) wireless network architecture

4.3 Discussion

With the importance and necessity of network security at heart, the WPA 2 was proposed to be deployed in FRSC wireless network system to achieve a protected wireless network. IEEE 802.11i (WPA 2) offers a quite complete security suite to satisfactorily accomplish advance security objectives in wireless network provided that all featured mechanisms collaborate in a proper way. It has specification for wireless networks security mechanisms. This standard is based on the AES (Advanced Encryption Standard) and can encrypt transmissions that run on 802.11a, 802.11b and 802.11g technologies. The migration path in upgrading to WPA2 will depend upon the security environment and the user authentication policies in place. We are at this point presenting the 7 Steps to Prepare for a WPA2 deployment. These steps focus on the authentication portion of WPA2 (Paul, 2006). Each of the 7 steps listed below is required to determine the components of a WPA2 deployment, which will prepare network, network managers to deploy WPA2 including the implementation of IEEE 802.1X authentication and AES (WPA2) encryption for an FRSC network environment.

After following all 7 steps, network managers will know the components needed for a WPA2 deployment and be prepared to implement IEEE 802.1X authentication policies and begin deployment. These 7 steps address the requirements for any network using IEEE 802.1X authentication. The effort and investment made in following the 7 steps will serve for WPA2 deployments. The seven steps are as follows:

i. Security Mechanism and Credentials

Many existing enterprise networks already have a network security policy in place. Security policies, credentials and user identity management mechanisms will impact WPA2 enterprise deployment. Typically, the database is stored on the server or, externally, in Microsoft Active Directory, Novell LDAP, iPlanet or Secure ID Token. With IEEE 802.1X authentication system in place, a network manager can continue to use it to store security credentials if it supports the EAP type(s) selected for the Wi-Fi network. If there is no security policy in place, network manager will have to select one, provide the necessary user credentials to support it, and confirm that the credentials chosen can be managed by the authentication server.

ii. User Authentication Database

A database is required for user authentication. If users are already being authenticated, network managers should consider the database already in house. In the absence of an existing user authentication database, network managers will have to select one. Selection should be based on the following considerations:

- The security policy and the management of user credentials
- The credential type selected
- How user identity information will be stored
- Budget considerations
- Server environment

The server environment (UNIX, Linux, or NT) will heavily influence what database is implemented. This is due to the technology in place with these different types of Operating System.

iii. Client Operating Systems

Determine which client operating systems (OS) will be supported — Windows 8, Windows 7, Windows XP, 2000, NT, 98, 95; Windows CE; Mac OS; Linux; Palm OS; DOS or a proprietary system.
Network managers should make sure that EAP type, selected database, and supplicants will support the operating system that will be used with WPA or WPA2.

iv. Supplicants

This step and Step 3 (Client Operating Systems), Step 5 (EAP Types), and Step 6
(Authentication Server) should be considered in parallel as the selection of the supplicant should be based on the EAP types, as well as on the client operating systems and authentication database being used. FRSC Network managers should obtain supplicant to support existing client operating systems. Some operating systems include free supplicants. Others require the purchase of an after-market supplicant. In some settings, aftermarket supplicants may offer more flexibility as they are not tied to a particular operating system. Features may vary between built-in supplicants and third party supplicants.

v. EAP Types

In parallel with Step 4, decide which EAP-type to be used. The EAP type selected should support the selected database for user credentials and the network security strategy. It should match the user authentication policies, user management strategy, and client operating system.

Some examples of EAP types that match various databases include:

- **Windows** Microsoft format NT or Active Directory—works with PEAP v0/-MSCHAP v2, EAP-TLS, and EAP-TTLS/ MSCHAP v2
- **Linux** LDAP or Netscape Directory Service (NDS)—works with PEAP v1/ MD5, PEAP v1/ GTC, EAP-TLS, EAP-TTLS/CHAP
- **UNIX** A token or one-time password (OTP) server—The server has a token card with a reference ID that works with PEAP v1/EAP-GTC, EAP-TTLS/GTC

Network managers should ask their vendor how other EAP types compare. Since the Wi-Fi Alliance certifies WPA-Enterprise and WPA2-Enterprise products in tests on an open architecture, a variety of open standard and other EAP types can be used.

vi. Authentication Server

Select an authentication server that will work with the selected user credentials database and matching EAP types. Network managers may change EAP types to match the current server. Or, network managers may wish to purchase a new server to work with the EAP type that best supports their security policies. Typically, a RADIUS server is used. If selecting a new server, network managers must verify that it will work with the selected database and matching EAP-types.

vii. Access Points and Client NIC Cards

Confirm that all APs and client devices to be used in the deployment are WPA-Enterprise or WPA2-Enterprise Wi-Fi CERTIFIED as applicable. WPA-Personal and WPA2-Personal APs and clients are not recommended for enterprise deployments because they do not support IEEE 802.1X and EAP authentication. Typically, WPA and WPA2 are not automatically implemented in the default configuration of new wireless client devices and APs. They must be configured when the products are installed. Legacy devices may require WPA2 upgrades. Many vendors provide WPA firmware updates for legacy APs and client devices. A hardware upgrade may be needed for WPA2 devices. Network managers should contact their vendor for upgrade information regarding the devices already in place. Do this for all of the client computers on your network. Once you get everything working, if you take a look at your wireless connections screen, you should see something like this, where the wireless3 access point is showing that it has WPA2 security enabled. OK, now you should be done. If you aren't getting a connection, chances are there is a mismatch between your router and your client. Check all the steps and make sure that the WPA2 choices are showing up in the right places and that you have chosen the appropriate encryption method (AES or TKIP) for both router and client pairs. You might also have to use the wireless management software from your adapter vendor, rather than Microsoft's, to set up your connection. Once you have a working connection, you don't have to go through all these steps and should be connected securely automatically.

WPA2 protects the FRSC wireless network from a variety of threats, including lost or stolen devices (Resource stealing) and hacker attacks such as ‘man-in-the-middle’, authentication forging, replay, key collision, weak keys, packet forging, and ‘brute-force/dictionary’ attacks. WPA2 addresses the weaknesses of original WEP security resulting from WEP’s imperfect encryption key implementation and its lack of authentication. Using TKIP, it brings an enhanced encryption algorithm and with IEEE 802.1X/EAP authentication it brings standards-based mutual authentication to Wi-Fi networks. Together, TKIP encryption and mutual authentication insulate the Wi-Fi network from a variety of threats when WPA Enterprise mode is used.WPA2 offers advanced protection from wireless network attacks. Using AES, government grade encryption and IEEE 802.1X/EAP authentication. WPA2 provides stronger standards based mutual authentication and advanced encryption to protect the Wi-Fi network from a variety of threats and attacks.

When compared with the IEEE 802.11 security standard using 40-bit WEP with no dynamic keying, TKIP and AES make it far more difficult-if not impossible-for a would-be intruder to break into a Wi-Fi network. By greatly expanding the size of keys and number of keys in use, creating an integrity checking mechanism, using a strong encryption cipher; and imposing replay protection, AES and TKIP greatly increase the strength and complexity of wireless encryption. Together with the IEEE 802.1X/EAP mutual authentication framework, TKIP and AES magnify the complexity and difficulty involved in decoding data on a Wi-Fi network—making the Wi-Fi network secure.

5. CONCLUSION

The paper is out to analyze wireless LAN security, taken FRSC wireless LAN as the case study. Based on the analysis, a solution which when applied to wireless local area networks, an organization such as FRSC, and others, could have secured wireless communication channel for its end users is proposed. In this paper, it has been shown that FRSC wireless LAN lacks the best security setting, and/or the one in place can be broken through by network hackers usually using some set of simple software tools. This problem can be faced not only by FRSC wireless LAN, but even those enterprise wireless network deployment that have been configured with the basic IEEE802.11 wireless security settings such as the use of WEP, SSID, MAC Address and the likes as there are one hundred and one war driving tools freely available for cracking such encryption techniques which are widely in use.

In conclusion, wireless LAN security in FRSC has been successfully studied and it has been shown that a better IEEE 802.11 standard has the almost perfect security package for the wireless network. This package is the IEEE 802.11i standard (WPA2). It takes care of all wireless security issues. FRSC can now be sure of reliable barrier against network intruders if the newly proposed mechanism is applied into the organization's wireless network. Based on these findings, the use of WPA2 which is an enhanced security mechanism with no known decryption tool has been proposed. A simulated instance of this security mechanism has also been provided.

REFERENCES

1. Adeyinka, O. (2008). Internet Attack Methods and Internet Security Technology. *2nd Asia International Conference on Modelling and Simulation 2008* (pp. 77-82). AICMS.
2. Arashpour, M. Y. (2011). *Implementation of Wireless Security on Virtual Wi-Fi.* Malaya University, Faculty of Computer Sciense and Information Technology. Kuala Lamputr: Unpublished.
3. Bhavya, D. (2010). NEtwork Security: History, Importance, and Future. 1-13.
4. Borisov, N. I. (2002). Intercepting Mobile Communications: the Insecurity of 802.11.
5. Caravan, E. J. (2001). *Fundamental of Netwrok Security.* Boston, London: Artech House Inc.
6. Cisco. (2010). Borderless Networks Architecture: Connect Anyone, Anywhere, on Any Device. *Cisco Information Publication*, 1-11.
7. Curtin, M. (1997). *Introduction to Network Security.* Kent Information Services.
8. Dowd, P. M. (1998). Network Security: It's Time to Take it Seriously. *Computer*, 24-28.
9. Kartalopoulos, S. (2008). Differentiating Data Security and Network Security. *IEEE International Conference on Communication 2008* (pp. 1469-1473). New York City: ACM.
10. Muhammad-Tukur, S. (2011). *Wireless Local Area Network Security Analysis: A Case Study of ABU WLAN.* Zaria: Unpublished.
11. Nwabude, A. S. (2008). *Wireless Local Area Network (WLAN): Security Risk Assessment and Countermeasures.* Blekinge Institute of Technology, Department of Telecommunications. Blekinge: Unpublished.
12. Serpanos, D. V. (2002). Secure Network Desing: A Layered Approach. *2nd International Workshop on Autonomous Decentralized System*, (pp. 95-100).
13. Sotillo, S. (2006). *IPv6 Security Issues.* LA: Infosec Writers.
14. Wee, O. K. (2004). *Wireless Network Security: Design Consideration for an Enterprise Network.* Monterey, California: NPS.
15. Wei, N. J. (2006). A Security Architecture for IEEE 802.11 Wireless Networks in Large-scale Multinational Corporations. *ITS Telecommunications Proceedings* (pp. 846-849). NYC: Cisco Press
16. Adeleye, T. R. (2015). Understanding the Role of ICT in FRSC. *Commanders Capacity building* (pp. 6-9). Abuja: Unplblished.
17. Adeyinka, O. (2008). Internet Attack Methods and Internet Security Technology. *2nd Asia International Conference on Modelling and Simulation 2008* (pp. 77-82). AICMS.
18. Adya, A. B. (2004). Architecture and Techniques for Diagonising Faults in IEEE 802.11 Infrastucture Networks. *The 10th Annual International Conference on Mobile Computing and Networking* (pp. 30-44). Philadephia, USA: MobiCom ACM.
19. Anderson, T. M. (2008). Openflow: Enabling Innovation in Campus Networks. *SIGCOMM Comput*, 69-74.
20. Arashpour, M. Y. (2011). *Implementation of Wireless Security on Virtual Wi-Fi.* Malaya University, Faculty of Computer Sciense and Information Technology. Kuala Lamputr: Unpublished.
21. Barken, L. (2004). *How secure is your Wireless Network? Safeguarding your Wi-Fi LAN.* New York City: Prentice Hall.
22. Bhavya, D. (2010). NEtwork Security: History, Importance, and Future. 1-13.
23. Borisov, N. I. (2002). Intercepting Mobile Communications: the Insecurity of 802.11.
24. Brown, B. (2003). 802.11: The Security Difference Between b and i. *IEEE Potentials*, 23-27.
25. Bulbul, H. B. (2008). Wireless Network Security: Comparison of WEP (Wired Equivalent Privacy) Mechanism, WPA (Wi-Fi Protected Access) and RSN (Robust Security Network) Security Protocols. *Ist International Conference on Forensic Applications and Techniques in Telecommunications, and Multimedia and Workshop.* Adelaide.
26. Caravan, E. J. (2001). *Fundamental of Netwrok Security.* Boston, London: Artech House Inc.
27. Chandra, R. (2006). *A virtualization Architecture for wireless Network Cards.* Cornell University, Graduate School. Ithaca, NY: Unpublished.
28. Chereddi, C. (2006). *System Architecturefor Multichannel Multi-Interface Wireless Networks.* University of Illionis, Electrical and Computer Engineering. Urbana, Illionis: Unpublished.
29. Chereddi, C. K. (2007). Net-X: A Multichannel Multi-Interface Wireless Mesh Implementation. *SIGMOBILE Mob* (pp. 84-95). LA: Comput. Commun.
30. Cisco. (2008). *Network Security Baseline.* San Jose, USA: Cisco System Inc.
31. Cisco. (2010). Borderless Networks Architecture: Connect Anyone, Anywhere, on Any Device. *Cisco Information Publication*, 1-11.
32. Curtin, M. (1997). *Introduction to Network Security.* Kent Information Services.
33. Dave, W. (2004). *The Implementation of a Multi-site, Wireless Network at Northumbria University.* Northumbria University, Project Management, IT Services. London: Unpublished.
34. Dowd, P. M. (1998). Network Security: It's Time to Take it Seriously. *Computer*, 24-28.
35. Draves, R. P. (2004). Routing in Multi-hop Wireless Mesh Networks. *10th Annual International conference on Mobile Computing and Networking* (pp. 18-26). Philadelphia PA, USA: Unpublished.

36. Edney, J. a. (2004). *Real 802.11 Security, Wi-Fi Protected Access and 802.11i.* Wesley: Addison Press.
37. Elankayer S.; Muthukkumarasamy, V.; Danny Powell. (2005). *IEEE 802.11i WLAN Security Protocol- A Software Engineer's Model.* Griffith University, School of Information and Communication Technology. Queensland, Australia: Unpublished.
38. Engelsman, W. J. (2009). Architecture-Driven Requirements Engineering. *Proceedings of the 2009 ACM Symposium on Applied Computing (SAC '09)* (pp. 285-286). Honolulu, Hawaii: ACM.
39. Gast, M. S. (2005). *802.11 Wireless Networks: The Definite Guide, Second Edition.* O'Reilly Media, Inc.
40. Hull, B. B. (2006). Cartel: A Distributed Mobile Sensor 73 Computing System. *The 4th International Conference on Embedded Netwroked sensor System* (pp. 125-138). Colorado, USA: SenSys '06. ACM.
41. Hytnen, R. a. (2006). An Analysis of Wireless Security. *J. Comput. Small Coll*, 210-216.
42. Ivan M, G. Z. (2007). Introduction of IEEE 802.11i and Measuring its Security versus Performance Tradeoff. *The 13th European Wireless Conference.* Unpublished.
43. Jarvis, B. (2003). Enterprise Architecture: Understanding the Bigger Picture - A Best Practice Guide for Decision Makers in IT. *The UK National Computing Center*, 9.
44. John, V. D. (2001). Wireless LAN Access Control and Authetication. *Interlink Networks Resource Library*, 27-32.
45. Kandula, S. L. (2008). FatVap: Aggregating AP Backhaul Capacity to Maximize Throughput. *5th USENIX Symposium on Networked Systems Design and Implementation* (pp. 89-104). San Francisco: Eds USENIX Association, Berkeley, CA.
46. Kang, M. K. (2008). An Energy-Efficient Real-Time Scheduling Scheme on Dual-Channel Networks. *Information Sciences, 178*, 2553-2563.
47. Kappelman, L. M. (2008). Enterprise Architecture: Charting the Territory for Academic Research. *AMCIS.* Texas: Information Systems.
48. Kartalopoulos, S. (2008). Differentiating Data Security and Network Security. *IEEE International Conference on Communication 2008* (pp. 1469-1473). New York City: ACM.
49. Karygiannis, T. a. (2002). *Wireless Network Security 802.11, Bluetooth and Handheld Devices.* Gaithersburg: NIST Special Publication.
50. Kim, C. C. (2008). Floodless in SEATTLE: A scalable Ethernet architecture for large Enterprises. *Proceedings of ACM SIGCOMM, 2008* (pp. 39-44). Los Angeles: ACM.
51. Kim, K. a. (2006). On Accurate Measurement of Link Quality in Multihop Wireless Mesh Networks. *12th Annual International Conference on Mobile Computing and Networking* (pp. 38-49). Los Angeles: ACM.
52. Koziol, J. (2003). *Intrusion Detection with Snort.* Indianapolis: Sams Publishing.
53. LAN MAN Standars Committee of the IEEE Computer Society. (2004). *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specification Amendment 6: Medium Access Control (MAC) Security Enhancements.* LA: IEEE.
54. Lapalme, J. (2012). Three Schools of Thought on Enterprise Architecture. *IT Professional, 14*(6), 37-43.
55. Marin, G. (2005, Nov-Dec). Network Security Basics. *Security and privacy*, pp. 68-72.
56. Martinovic, F. a. (2008). Wireless Network Security and Interworking. *IEEE Wireless Communication Magazine*, 13-21.
57. Minho, S. a. (2008). Security & Vulnerability Analysis of Wireless Messaging Protocols & Application Wrieless Client Puzzles in IEEE 802.11 Networks: Security by Wireless. *Proc. ACM Conference on Wireless Network Security* (pp. 36-45). New York City: ACM.
58. Moen, V. R. (2004). Weakness in the Temporal Key Hash of WPA. *SIGMOBILE Mob.*, 76-83.
59. Molva, R. (1999). Internet Security Architecture. *Computer Networks and ISDN Systems*, 787-804.
60. Muhammad-Tukur, S. (2011). *Wireless Local Area Network Security Analysis: A Case Study of ABU WLAN.* Zaria: Unpublished.
61. N. Borisov, G. I. (2008). *Security of the WEP Algorithm.* Berkeley: UC.
62. Naveen, S. U. (2003). Secure Verifcation of Location Claims. *2nd ACM Workshop on Wireless Security* (pp. 1-10). LA: ACM.
63. Nicholson, A. C. (2006). Improved Access Point Selection. *4th International conference on Mobile Systems, Application and Services* (pp. 233-245). Uppsala, Sweden: ACM.
64. Nwabude, A. S. (2008). *Wireless Local Area Network (WLAN): Security Risk Assessment and Countermeasures.* Blekinge Institute of Technology, Department of Telecommunications. Blekinge: Unpublished.
65. Obitz, T. a. (2009). Enterprise Architecture Expands its Role in Strategic Business Transformation: Infosys Enterprise Architecture Survey. *Information Systems*.
66. Olagunju, O. M. (2013). *Road Sense.* Abuja.
67. Pang, R. A. (2005). *A First Look at Modern Enterprise Traffic.* IMC.
68. Paul, A. (2006). Benefits of Wi-Fi Protected Access 2 (WPA2). *INFS 612*.
69. Pejman, R. &. (2006). *802.11 Wireless LAN fundamentals: A Practical Guide to understanding, designing and operating 802.11WLANs.* Indiana: Cisco Press.

70. Peter, H. P. (2010). *ADVANCED DYNAMIC ENCRYPTION - A SECURITY ENHANCEMENT PROTOCOL FOR IEEE 802.11 AND HYBRID WIRELESS NETWORK.* A&A University, Graduate Studies. Teaxas: Unpublished.
71. R. Zhang, &. J. (2007). A Survey on Current Practices in Enterprise Wireless Networking and Security Management. *J. Information Systems*, 279-382.
72. Radack, S. (2008). *Security for Wireless Networks and Devices.* Indiana: Cisco Press.
73. Samuel, C. D. (2013). *Processing of National Drivers Licence.* Ilorin: Unpublished.
74. Sankar, K. (2004). *Wireless LAN Security: Expert Guidance for Securing Your 802.11 Networks.* Indianapolis: Cisco Press.
75. Savage, B. a. (2009). *Wireless 802.11i Network Made Simple.* Cisco Coop.
76. Serpanos, D. V. (2002). Secure Network Desing: A Layered Approach. *2nd International Workshop on Autonomous Decentralized System*, (pp. 95-100).
77. Sotillo, S. (2006). *IPv6 Security Issues.* LA: Infosec Writers.
78. Stallings, W. (2006). *Wireless Communications and Networks.* Indiana: Pearson Education.
79. Wee, O. K. (2004). *Wireless Network Security: Design Consideration for an Enterprise Network.* Monterey, California: NPS.
80. Wei, N. J. (2006). A Security Architecture for IEEE 802.11 Wireless Networks in Large-scale Multinational Corporations. *ITS Telecommunications Proceedings* (pp. 846-849). NYC: Cisco Press.
81. Wong, S. (2003). *The Evolution of Wireless Security in 802.11 Networks: WEP, WPA and 802.11 Standards.* GSEC.
82. Yang, H. R. (2006). Securing a Wireless World. *Proceedings of the IEEE*, (pp. 442-454). Los Angeles, CA.