Global Scientific JOURNALS

GSJ: Volume 6, Issue 9, September 2018, Online: ISSN 2320-9186
www.globalscientificjournal.com

A SURVEY OF WIRELESS NETWORK SECURITY AMONG TERTIARY INSTITUTION IN NIGERIA: A CASE OF STUDY WAZIRI UMARU FEDERAL POLYTECHNIC BIRNIN KEBBI.

***M. K. Ibrahim[1], M. A. T. Abubakar[2], Z. Umar[3].**

1. Department of Computer Science, College of Science and Technology, Waziri Umaru Federal Polytechnic, BirninKebbi. Kebbi State-Nigeria, musaikamba@gamail.com.
2. Department of Computer Science, College of Science and Technology, Waziri Umaru Federal Polytechnic, BirninKebbi. Kebbi State-Nigeria, musaibnabubakar@gamail.com.
3. Department of Computer Science, College of Science and Technology, Waziri Umaru Federal Polytechnic, BirninKebbi. Kebbi State-Nigeria, zayyanuumar1@yahoo.com.

***Corresponding Author: musaikamba@gamail.com, +2348035030270**

ABSTRACT

The use of wireless communications has resulted in a wide expanse of wireless networks. However, the vulnerabilities and threats that wireless networks are subjected to resulted in higher risk for unauthorized users to access the computer networks. This paperinvestigates wireless network security in Waziri Umaru Federal Polytechnic Birnin Kebbi as well as the devices used to monitor and secure the wireless network. The data for thestudy were produced through theoral interview. From the study, the researcher finds out that Waziri Umaru Federal Polytechnic Birnin Kebbi uses *Cacti* and *Nagios* as wireless auditing tools which were originally developed to be used for helping the network administrators to monitor their systems securely. The study also highlighted the security goalthat can assure the secrecy of any network which includes: Authentication, Confidentiality, Integrity, Non-Repudiation,and Reliability.The study further investigates some security threatsfacing wireless network security in Waziri Umaru Federal Polytechnic Birnin Kebbi and proposes some measures that can be taken to minimize the security threats.

Keywords: Computer Networks, Network Security, Security goal, Threats, Unauthorized users, Vulnerabilities, Wireless communications.

INTRODUCTION

Wireless networking is one of the growing technologies being deployed today, from home networksto corporate level wireless networks. Businesses, as well as general users, are trying to take advantage of the benefits which wireless networking provides such as cost-effectiveness, flexibility and easy to use.The wireless networkis considered the most popular networks technologies today. Both individuals and large companies are using them due to their advantages, such as flexibility, mobility, scalability, and easy to use. The wireless networkis widely used in many sectors ranging from corporate, education, finance, healthcare, retail,and manufacturing. According to a study by the Gartner Group, approximately 50 percent of company laptops around the world will be equipped for Wireless network by 2006, (Swisscom.com, 2003).

The wireless networkis a flexible data communications system or distribution method for two or more devices that use high-frequency of radio waves and often include an access point to the Internet.The wireless network allows users to move around the coverage area, often a home or small office, while maintaining a network connection.

Wireless security is the prevention of unauthorized access/damage to computers using wireless networks or protection of information and resources from loss, corruption,and improper use according to Cisco Systems (2013).

However, there has been an increasing demand for greater security in Businesses. Most network threats come from the ignorance of users, the inactive attitudes of organizations and the improper implementation of security features by wireless devices manufacturers according to Loo, A.W (2010). Some researchers suggest that with the increased demand for wireless connections, it becomes a growing concern about the security and protection in the wireless networks (Bulbul, H. I et.al. 2008).with the growth of wireless networking, security is the main weakness of the whole wireless system, which resulted in improper uses of network resources. As wireless access increases, security becomes an, even more,an important issue.

To enhance the security of wireless networks the security threats has to be minimized because those are the problems affecting the security of the wireless network. Some of the threats include Denial of Service, Spoofing, and Eavesdropping. Despite the productivity, convenience and cost advantage that wireless network offers, network security solution has six standard security requirements, namely confidentiality, integrity, availability, authentication, access control, and non-repudiation (Padmavathi, G. 2009).This paper studies the wireless network security issues that may be facingWaziri Umaru Federal Polytechnic BirninKebbi. To identify security devices used to secure their wireless network,the security threats that are facing the network and suggest security measures needed to minimize the threats.

Problem statements

Wireless Network security is an important and complex issue. Although wireless network offers numerous opportunities, thewireless network has many security vulnerabilities which if not fixed will impact negatively on the data transmission and security of thewireless network. Therefore, security must be put in place to ensure that, data sent across the wireless network are secured.

The vulnerabilities and threats that wireless networks are subjected to resulted in higher risk for unauthorized users to access the computer networks.

Research questions

1. What are the softwaresecuritydevices used to secure their Wireless Networks inWaziri Umaru Federal Polytechnic BirninKebbi?
2. What is the level of threats facing the wireless networks in Waziri Umaru Federal Polytechnic BirninKebbi
3. What are the current approaches/ measures used for protecting wireless network from unauthorized users?

Aim of the study

To propose security strategy that can minimize the threats in Waziri Umaru Federal Polytechnic BirninKebbi wireless networks.

Objectives of the study

1. To identify security devices used to secure wireless network in Waziri Umaru Federal Polytechnic BirninKebbi and their limitations.
2. To identify the wireless network security threats that may be facing in Waziri Umaru Federal Polytechnic BirninKebbi.
3. To suggest suitable security measures needed to minimize the threats.

.**Related works**

Various works in theliteratureexist in the area of wireless network security for the successful protection of information and resources from loss, corruption, and improper use. According to Neil, M. &Skea, M. (2011), the author's uses wireless audit tool to investigate, and assess the level of application of wireless network security reaches home and office environments where they determine the extent to which adequate security methods have been applied by end-users. By allowing many end users have purchased wireless routers mainly for their broadband functionality.Also, they provide an encryption scheme to ensure the confidentiality and integrity of a transmission, as well as to prevent network resources from being accessed by unauthorized users. The research instrument used in this investigation was a wireless security auditing tool a software program installed on computer hardware to passively capture, log and analyses signals from wireless networks surrounding the user. A wireless security-auditing tool is used while wardriving to capture security-related data for wireless networks.

Authors, Ahmad, S. et.al. (2013)evaluate the Wireless Network in Jordan as well as the use of the security setting of the systems and tools used.Also, they suggesteda new way for securing wireless network through Wardriving that involves the use of freeware tools such as *NetStumbler*, or *Kismet,* which was originally developed to be used for helping network administrators to make their systems more secure. Also, they propose some measures that can be taken to improve thesecurity of the wireless network which includesmethods of authentication,network ID, encryption method and frequent changes of SSID.

Earliest, Onimode, B.M. &Dajuma, K.J (2014), the author's gave a general view on important security measures related to different network scenarios within the African environment, they discuss different Network Security Measures while using the networks in the Africa environment, which includes the use of firewall, authentication and encryption scheme system.Also, they highlight much of the use of network security tools that protect their networks from unauthorized access, which includes: Net Cat,N-map Security Scanner, Ethereal,and Nessus. They conclude by stating that,Network security policies should not be set, rather, it should be flexible enough to accomplish the need of businesses as well as it should be capable enough to tackle future security threats while at the same time easily convenient and adaptable.

According to Radomir, P. &Dejan, S. (2007),the author's discuss security threats that affect WEP (Wired Equivalent Privacy) protocol for the protection of wireless networks, its security deficiencies, as well as the various kinds of attacks that can jeopardize security goals of wireless network, which includes, Man in the middle attack, Denial of Service Attacks, passive attack etc.

MATERIALS AND METHODS

Security Goals

Every security system must provide a bundle of security functions that can assure the secrecy of the system. These functions are usually referred to as the goals of the security system. These goals can be listed under the following five main categories as mentioned earliest by Abdel-Karim, R. & Al Tamimi (2006).

Authentication: This means that before sending and receiving data using the system, the receiver and sender identity should be verified.

Confidentiality: It means that only the authenticated people are able to interpret the message content and no one else. Or keep information private such that only authorized users can understand it.

Integrity: Integrity means that the content of the communicated data is assured to be freefrom any type of modification between the endpoints (sender and receiver).

Non-Repudiation: This function implies that neither the sender nor the receiver can falsely deny that they have sent a certain message.

Reliability and Availability: Since secure systems usually get attacked by intruders, which may affect their availability and type of service to their users. Such systems should provide a way to grant their users the availability and quality of service they expect.

Wireless Network Security Attacks (Threats)

Security attacks can be classified under the following:

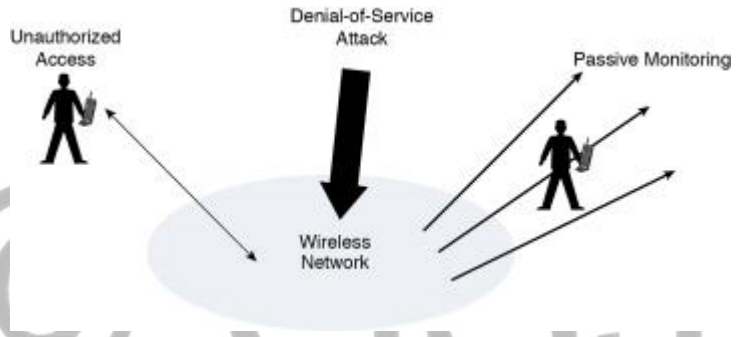

Figure.1Network security protection

I. **Passive attack**:Is the type of attacks that involve attempts to disrupt the system by using experimental statistics. One of the examples of this type of attackis plain text attacks, where both the plain text and the code text are already known to the attacker(Onimode, B.M and Danjuma K.J).

II. **Man in the middle attack**

In this attack, an attacker captures data from the middle of atransmission and changes it, then sends it again to the destination. Receiving source thinks that this message came from theoriginal source. For example, in a share trading company, Jack is sending a message to Rick telling him to hold the shares. An adversary intercepts this message in away that it looks like Jack is telling for sell. When Rick

receives this message, he will think that Jack is telling for the sell and he will sell the shares. This is known as Man in the middle attack (Onimode, B.M and Danjuma K.J).

III. Packet capturing attack

This attack is part of thepassive attack. In this attack, an attacker uses a packet capturing software which captures all packets from thewire. Later, he extracts information from these packets. This information can be used to deploy several kinds of other attacks.

IV. Password attack

In this attack, an adversary tries to login with aguessed password. Two popular methods for this attack are dictionary attack and brute force attack. In brute force method, an adversary tries with all possible combinations (permutations). In dictionary method, an adversary tries with a word list of possible passwords.

V. Active Attack

In this attack, an adversary does not wait for any sensitive or authentication information. He actively tries to break the systems by inserting some viruses, worms, stealing login information, inserting malicious code and penetrating network backbone. Active attacks are the most dangerous in natures. It results in losing sensitive information, modification of data or complete data loss.

VI. Denial of Service Attacks

In this kind of attack, the intruder floods the network with either valid or invalid messages affecting the availability of the network resources by using frequency devices to send continuous noise on a specific channel to destruct the network connectivity. Due to the nature of the radio transmission, the wireless network is very vulnerable against denial of service attacks.

RESULTS AND DISCUSSION

1. Wireless Network Security Measures

Network security measures are measures taken to prevent unauthorized access/damage to thecomputer or is the protection of information and resources from loss, corruption and improper use of the wireless network. Security measures will help in theunderstanding bettermanagement of the network-security control in an organization(Onimode, B.M and Danjuma K.J).

Generally, these are some of the following measures to be taken to secure the network (Onimode, B.M and Danjuma K.J):

i. Security barriers to check the organization's border.
ii. Staffs should be alert to physical confidence.
iii. When using a wireless link, the use of a dynamic password is recommended.
iv. A strong Antivirus and Internet Security Software package should be installed.
v. A very strong proxy and thefirewallare to be used to keep unwanted people out of the network.
vi. For authentication, the use of strong passwords is endorsed and it change is recommended on a weekly/bi-weekly basis.
vii. The use of network monitoring devices is needed.
viii. The application of physical security measures like a CCTV for entry areas and controlled areas.
ix. Fire suffocations can be used for fire-sensitive areas like server rooms and security rooms.

Earliest,Waziri Umaru Federal Polytechnic BirninKebbitheyuse**firewall** and **authentication system** as their major ways for protecting their wireless network from unauthorized access.

I. Firewall

Computer security borrowed the term firewall from firefighting and fire prevention, where a firewall is used to limit a fire within a particular location or building so that it will not spread to another place or area(M. Cobb and M. Rouse, 2014).

A **firewall** is a network security system, either hardware or software-based, that controls incoming and outgoing network traffic based on a set of rules (M. Cobb and M. Rouse, 2014).

A **firewall** is a network security system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software or combination of all according to M. Chapple (2006).

Firewalls protect the network and perform other functions to a network, which includes acting as DHCP or VPN server for the network.

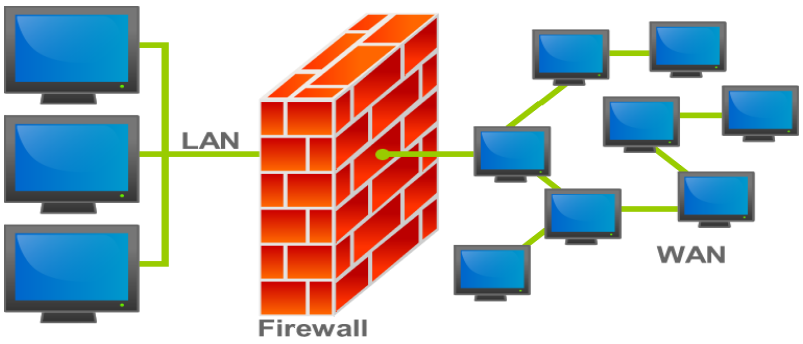

Figure 2: Typical example of a Firewall protecting a LAN from illegal intrusion through a WAN.

1.1 Characteristics of Firewall

1. It is observed to be a block point of control and monitoring in a network
2. Uses trust conditions to interconnect networks
3. Imposes a measure of restrictions on network services
4. permits that only authorized traffic is allowed, based on its configured rules
5. It audits/checks and controls access
6. It can also generate alarm for an abnormal network behavior
7. It provides boundary defense

When categorized based on the position of the firewall in a private network, firewalls can be broadly categorized into three:

1.1.1 Network Level Gateway Firewall: This is also known as proxy gateways. It is the first firewall in a network. These are made up of defender hosts so they do act as a proxy server. This application runs at the Application Layer of the OSI Reference Model. This has proven to be the most secure, because it does not permit anything to pass through it by default, but it also needs to have the programs written and turned on in order to start the traffic passing as shown below:

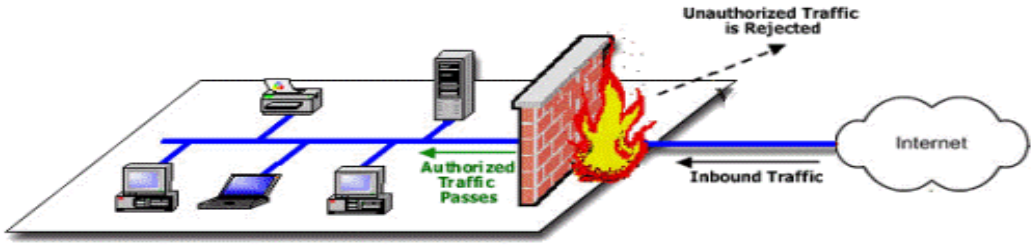

Figure 3: Network Level GatewayFirewall (Srikanth Ramesh, 2010)

1.1.2 Host-Based Firewall:

Here a software layer is provided on the host device that controls network traffic in and out of that single machine. The host-based firewall may be a service as a part of the operating system or an agent application such as endpoint security protection. Host-based firewalls are positioned on the network node itselfas shown below:

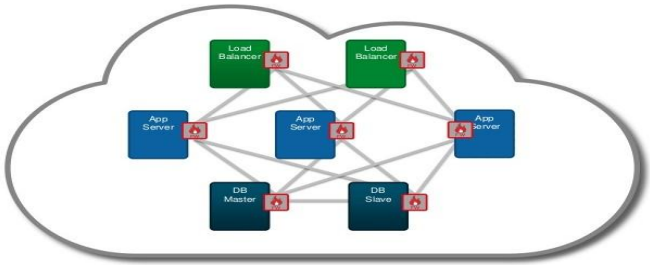

Figure.4 Typical example of a Host-Based Firewall (Sweet, C. et.al. 2010)

1.1.3 Packet Filtering:

Packet filtering is a technique whereby routers that are used in a network have Access Control Lists (ACLs) turned on. By default, a router will pass all the traffic sent through it, without any restrictions. ACL's is a method that is used to define what sorts of access is permissible for the outsiders to have access to theinternal network and vice versa. This is less complex than a proxy gateway because the feature of access control is done at the OSI lower layer. Because it is done with switches and router a packet filtering gateway is often much faster than its application layer.

2. Wireless Auditing Tools

Wireless audit tools can be used to control and regulate the output signal strength, monitor bandwidth consumption and plot the coverage patterns and availability of wireless networks. Wireless-auditing tools can be used by organizations to manage wireless vulnerabilities and also monitor the presence of rogue access points to ensure a high level of network security(Potter, B. 2005).

The wireless auditing tools used in University of Nigeria Nsukka (UNN), to monitor their wireless network are stated below:

1. *Cacti* and
2. *Nagios*

2.1 *CACTI*

Cacti is a free open source tool that offers an easy-to-use Web interface, is used to monitor the performance of devices in a network. *Cacti* is a complete network graphing solution that surveys network devices, gathers the data, then provides graphs based on what is configured. Also,*Cacti*can be used to complement other open source tools such as *Nagios* (for instance, using Cacti to monitor theperformance of devices that are being monitored by *Nagios*).

2.1.1 Cacti's main functions are:

1. Monitoring the network traffic and configuring data sources.

2. Creating and viewing graphs, based on how you configure the graph.
3. Managing users, so that different user can do different things.

2.2 *NAGIOS*

Nagios is a powerful network monitoring tool that helps you to ensure your critical systems, applications and services are always up and running. It provides features such as alerting, event handling and reporting. The *Nagios* Core is the heart of the application that contains the core monitoring engine and a basic web UI. On top of the *Nagios*Core, you are able to implement plugins that will allow you to monitor services, applications, and metrics, a chosen frontend as well as add-ons for data visualization, graphs, load distribution, and MySQL database support, amongst others. But the free version of *Nagios* XI is ideal for smaller environments and will monitor up to seven nodes.

2.2.1 *Nagios* main functions are:

1.Ability to monitor applications, services, operating systems, network protocols, system metrics and infrastructure components with a single tool.

2. Alert acknowledgments provide communication on known issues and problem response

3. User-specific views ensure clients see only their infrastructure components

CONCLUSION

Wireless network security is an important and compound issue. Although wireless network provides flexibility and low cost, it is exposed to the danger of hacking if the security does not be achieved. In this research we examined the wireless network security in Waziri Umaru Federal Polytechnic BirninKebbiand found out that, they do not have wireless security devices that can help to secure their network rather, they only have some software wireless auditing tools that can be used by administrators to manage wireless vulnerabilities, monitor bandwidth consumption and ensure a high level of network security. We have also discussed some wireless network threats affecting the wireless network security in Waziri Umaru Federal Polytechnic BirninKebbiwith some security measures that can help to minimize

the threats. The goals of the security system that can assure the secrecy of the system were also highlighted.

Limitation

The school Wireless Network service is configured in such a way that, the Auditing and Accounting department is completely partitioned from the Lionet Network, therefore, it does not have much security threat because the services are restricted or limited within their domain.

While, Lionet Network is the network that gives internet services to the entire Campus communityand is faced with so many threats e.g. Daniel of Service Attack (Dos), Man in the Middle attack,Passive attack, Password attack etc.

Also,network monitoring toolsare limited for the purpose of observing and analyzing the status and behaviors of the network and providing notifications to a network administrator through a messaging system, usually, emails, when a device fails.

Recommendation

With the growth of wireless networks security, some of the following measures are to be taken to minimize the security threats: a strong Antivirus and Internet Security Software package should be installed. For authentication, the use of strong passwords is recognized also change is recommended on time basis, a very strong proxy and thefirewall is to be used to keep unwanted people out of the network. There will be a need to have a periodic audit of the wireless networks, and to try and assessthe wireless networks, evaluate the systems' vulnerabilities, and analyses the security risks associated with it.

Therefore, the researcher recommendsthat the network administrators of WaziriUmaru Federal Polytechnic BirninKebbishould applythe use of wireless security devices in order to ensure safety and securely of their wireless network. Finally, the very best way to secure wireless network is to have the security knowledge, proper implementation,andmaintenance.

ACKNOWLEDGMENT

We sincerely acknowledge the support of Director Centre for Information Technology (CIT) Waziri Umaru Federal Polytechnic, BirninKebbi in theperson of Dr. YahayaBande. Also, our profound gratitude goes to the Management of Waziri Umaru Federal Polytechnic, BirninKebbi that gave us permission to access their Wireless network services while interviewing some staff and students.

REFERENCES

Abdel-Karim R. Al Tamimi (2006). “A Survey Paper,Security in Wireless Data Networks”, http://www.cse.wustl.edu/~jain/cse574-06.

Ahmad S. Mashhourand ZakariaSaleh(2013). “Wireless Networks Security” in Jordan, International Journal of Network Security & Its Applications (IJNSA), Vol.5, No.4.

B.M. Onimode and K.J Danjuma (2014). “Issues And Challenges of Network Security In the Africa Environment”, African Journal of Computing & ICT. Vol 7. No. 5.

Bulbul, H. I., Batmaz, I., and Ozel, M. (2008). "Wireless network security: comparison of WEP (Wired Equivalent Privacy) mechanism, WPA (Wi-Fi Protected Access) and RSN (Robust Security Network) security protocols".

Cisco Systems, Security Policy for Cisco Wireless LAN Controllers. The USA, (2013).

C. Sweet, R. Holland and P. Stehlik (2013). "Meeting PCI DSS Requirements with AWS and CloudPassage”, Available: http://www.slideshare.net/CloudPassage/aws slides-pci-20130124. Accessed: Oct. 25, 2016.

Dr. G. Padmavathi “Wireless security survey (2009).” International Journal of Computer Science Information Security”, vol. 4, no (1 & 2).

Loo, A. W. (2010). "Illusion of Wireless Security", *Advances in Computers*, Volume 79, 2010, Pages 119-167.

M. Cobb and M. Rouse (2014). "What is a firewall? - definition from WhatIs.com" SearchSecurity, Available: http://searchsecurity.techtarget.com/definition/firewall. Accessed: Oct. 19, 2016.

M. Chapple (2006). "How do circuit-level gateways and application-level gateways differ?” SearchSecurity, Available http://searchsecurity.techtarget.com/answer/How-do-circuit-level-gateways-and-application-level-gateways-differ. Accessed: Oct. 25, 2016.

Neil M. Skea, ManojMaharaj Wireless Network Security (2011). Vol: 07. Available at:https://www.researchgate.net/publication/228533354

Potter, B (2005). “Wireless Vulnerability Assessment”, Accessed 3 October 2008 at http://www.sciencedirect.com/science?

RadomirProdanovi and Dejan Simi (2007). “A Survey of Wireless Security”, Journal of Computing and Information Technology - CIT Vol. 15, No. 3, 237–255 doi:10.2498/cit.1000877.

Srikanth Ramesh (2010). "How Firewalls Works”, Available: http://www.gohacking.com/how-firewalls-work/. Accessed: Oct. 25, 2016.

Swisscom.com. “Swisscom Mobile to launch Public Wireless LAN on 2 December 2002 Jan. 2003.URL:http://www.swisscom.com/mr/content/media/20020924_EN.html(9 Dec. 2002).

Vibhuti, S (2005). IEEE 802.11 WEP Wired Equivalent Privacy Concepts and Vulnerability.

http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Mobility/secwlandg20/sw2dg/

http://searchnetworking.techtarget.com/tip/Open-source-network-monitoring-Monitor-your- routers-with-Cacti