ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 3, Issue 4, July 2014

Security Measures taken in Securing Data Transmission on Wireless LAN

[1]AGWU C. O., [2]ACHI I. I., AND [3]OKECHUKWU O.
[1]Department of Computer Science
Ebonyi State University – Abakaliki
[2]Department of Computer Science
Our Saviour Institute of Science and Technology
[3]Department of Computer Science
Madonna University - Okija

Abstract- The need for quality availability and secured data transmission and access at any location without limitation to time is transforming the society and our workplace by increasing the throughput, flexibility, efficiency and convenience at our various locations. This is made possible by the increase proliferation of wireless local area networking (WLAN) at different location in the human society. It is defining the dynamic ways through which data could be seamlessly transmitted and accessed by flexible mobile users at different locations. However, security of data still remains elusive. In this new, highly important and fast emerging field, security is being touted as the main obstacle militating against the extensive usage of this technology. However, in the midst of this security challenge, there is a massive patronage of the wireless local area network by every sector of the Nigeria society for their day to day activities. In this paper, the authors critically x-rayed security measures for data transmission on wireless LAN.

***Keywords*: Access Point, Authentication, Encryption Algorithm, Wireless LAN, Data Transmission**

I. INTRODUCTION

With the ever increasing adoption of wireless local area network (WLAN) in the society today, it is defining the accessibility of timely and quality of a flexible mobile device user. Therefore, with the increase adoption WLAN and the proliferation of mobile devices in the society, there is overwhelming increase in productivity as users gain access to limitless volume of data anytime, anywhere. To this end, in recent years, most mobile devices come with wireless LAN which enables them to see and get connected to an existing wireless network [1]. In this regard, the demands on Wireless LANS for functionality, scalability and increase application services are growing. Recently, in developing countries especially Nigeria, many universities, corporate organizations including individuals are embracing the wireless LAN thereby integrating mobile devices users seamlessly into the network while providing access to limitless volume of data for their various day-to-day activities. However, the convenience offered by the ability to connect to networks using mobile computing devices has also introduced many security issues that do not exist in the wired world[3]. With the arrival of mobile wireless internet, the security issue has become all the more important [2]. There are many security issues that deal with securing wireless/handheld devices, centralized sever and gateway system and more importantly securing information being communicated via wireless channels in addition to persistent applications and data security[2]. Infact, a wireless network can broadcast far outside your building[4]. With a powerful network antenna and some widely available hacking software installed on a mobile computing devices, any mobile user sitting near your wireless network installation or even driving by can passively scan all the data flowing into your network unnoticed. With all features of this emerging technology, it's flexibility and ability to connect from anywhere, wireless networks are often more vulnerable to attack. As many cooperate organizations and individuals are rapidly adopting the wireless technology, it will be necessary to review various security measures and techniques that could be deployed in securing data transmission and accessibility by a mobile flexible user. Therefore, in this paper, we exhaustively discussed various security measures taken in security data transmission and accessibility on wireless local Area Networking (WLAN).

II. ACCESSING WIRELESS LAN

A wireless LAN is set up for shared internet access so that data could be accessed and conveyed to it's desired destination. The host acquires a wireless access point, connect the devices to the internet and then brocasts its signal within it's environ. All that's needed to locate and connect to a wireless LAN is a wireless network interface card (NIC) running in promiscuous mode and some wireless LAN (WLAN) scanning software [3].

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 3, Issue 4, July 2014

Although the wireless received must be compatible to the access point transmitting radio making sure that the standards are maintained. The wireless access points sends out broadcasts and beacons at regular interval which are the signals that enable the wireless client to find the access point and configure the appropriate communication settings [3]. The beacon announces the specific Services Set Identifier (SSID) and the channel they access point is using. The WLAN scanning software then scans to find WLAN where the scanner cycle through all possible channels, sending out a continuous stream of broadcast packets. A nearby access point will respond to the broadcasts packets on the channel it is configured to use, making itself known to the scanner, even if beacons are disable [3]

III. SECURING WIRELESS NETWORK

They are several security measures that could be adopted in securing data transmission on a wireless LAN. An unsecured wireless network coupled with unsecured file sharing can be disastrous during data transmission. The following are some of the possible security steps taken to protect wireless LAN:

a) Encrypt network traffic

The wireless equivalent privacy (WEP) security portal provides various types of encrypted communication between the client and the access point [2]. It employs different types of security algorithm in securing wireless LAN transmission. It protects wireless communication from eavesdropping, modification and unauthorized access. This is achieved through a secret key that is shared between a wireless station and an access point [3]. The secret key is used to encrypt packets before they are transmitted and integrity ahead is used to ensure the packets are not modified in transits. In practice, must installations use a key that is shared between all stations and access points [6].

b)Control Broadcast Area

Wireless Access point has provisions that let you adjust the signal strength and to adjust the signal direction. Hence, placing access points as far away from exterior walls and windows as possible and controlling the direction of the signal can greatly secure wireless LAN transmission.

c) Ban Rogue Access Point

Rogue access point are created with an illusion to a node of the network that rogue point is a part of the network and association with such point which could be vulnerable for a short period of time [7]. Therefore, it is necessary to use some wireless security software to scan, locate and ban all rogue access point before it becomes vulnerable.

d) Usage of SSID or Access Point

Make changes to the default Services Set Identifiers (SSIDS) for your access points as the access point name are not encrypted in header of 802.11 packets [3, 4]. Wireless LAN scanners will detect these values and when you provide these descriptions you may make it easier for an attacker to identify the source of the signal

e) Disable Beacon Packets

Most access point has the ability to disable beacon packets and will then require the wireless NICS to use the same SSID as the access point before it will respond to traffics [3]. Disabling this feature will prevent attackers from discovering access points using wireless LAN scanning tools that passively collect data instead of actively sending out broadcast packages thereby endangering the security of data.

f) Virtual Private Networks(VPNS)

It provides security by creating an encrypted tunnel though the public internet which shields data from unauthorized access. Basics wireless VPNs mechanism can be used for wireless Networks, clients and servers [8]. VPNS encrypt connections at the sending and receiving ends, and keep out traffic that is not properly encrypted. It enables a high level of trust through the use of proven industry- standard security mechanism.

g) Wireless Application Protocol Gateway

When building a wireless network, make sure a single point of entry or access point at a central location as this will help secure and monitor the broadcast signal.

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 3, Issue 4, July 2014

h) Lock each Access Point

Protect your wireless router's administrator password by changing the default password and re-assigning a new password to it. This wireless router password can be changed in the future by resetting your wireless router. This improves the security of your data transmission of WLAN.

i) Do Not use Dynamic Host Configuration Protocol (DHCP) On WLAN

An attacker needs to obtain a valid Internet Protocol (IP) address and sub net mask in other to access a network through a WLAN connection. If an access is configured to use DHSP it will supply a valid address and sub net mask to any wireless devices that successfully authenticates and associates with the access point. [3] Therefore, if you don't have too many users, consider limiting the maximum number of DHCP address or not to use DHCP completely on wireless transmission. [3, 4].

j) Turn Off File Sharing

Use file sharing capabilities with caution. If the user does not share directories and files over his network, he should disable file sharing on his operating system network settings menu. This measure if taken will help in safeguarding your data on WLANs.

k) Keep Access Point Software Patched

Knowing and acknowledging the fact that the risk in wireless technology has increased exponentially as services become popular, there is need to keep access point software patched and up to date. This will greatly prevent intrusion into the WLANs.

l) Turn off wireless card

It is advisable to turn off the network wireless card during extended period of non usage as it could dynamically connect to any available wireless LAN where integrity of your data could be compromised. This security feature can be enhanced by disabling the auto-connect option to open WI-FI (wireless fidelity) networks.

m) Use 128-bit WEP

Passively cracking the WEP (wired Equivalent Privacy security protocol is merely a nuisance to a skilled hacker using Linux Freeware [4]. Hence, it is advisable to protect your wireless LAN with the 128-bit WEP technology while enabling MAC address filtering and SSID with the broadcast feature disable [2, 4].

n) Using Radius Server

Remote authentication Dial-in user service (RADIUS) server is another method of safeguarding data on WLAN by providing another authentication method [4, 2]. For authentication to work, the user's transmission must go through a wireless LAN access point to reach the back-end server performing the authentication. The wireless client contacts the access point, which in turn communicates the RADIUS server on the enterprise LAN [2]. The RADIUS server with the configure authentication webpage then verifies the client's credentials to determine whether the device is authorized to connect to the WLAN. Therefore, if the RADIUS server accepts the client device, the server sends data, including security keys to the access point to enable a secure connection with the client.

o) Firewalls

Since WLAN are inherently unsecured, we should allow WLAN traffic to co-exist with the wired LAN traffic in a trusted environment. Firewalls or screenings routers should be placed between the networks and authentication will be performed to restrict network traffic through the gateway according to a set of rule [3, 2]. Typically located as a gateway or access point, it controls the flow of traffic, preventing inside and outside users from accessing data and services as defined by the system administration.

p) WLAN Protected setup

Do not use the WLANs protected setup when deploying your wireless LAN. If your router allows it, disable it as it has been shown to be vulnerable to attacks.

q) MAC Address and Access Point

Determine if the access point has the ability to maintain a list of the MAC address of the network cards allowed to connect to the access [3]. Using this feature provides additional security to WLANs Attackers who can still

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 3, Issue 4, July 2014

identify the access point and sniff the traffic but they will not be able to connect to the network unless they spoof a more address on the list.

r) Access control

It is a process of ensuring that only trusted users can have access to network resources and they can see only what they are authorized to see. [2] This is done by granting a level of privileges and access to a client user by the wireless administrator. It consists of a two in one process known as authentication and authorization. Authentication is the process the user confirms his/her identity to the system and authorization involves control over what the user can do on the system once she or he has been authenticated. Authentication systems range from simple name-password pairs, to more elaborate challenge system, such as smart cards and biometrics [2]. There are the two ways which access control is provided.

s) Services Set Identifier (SSID)

Network access control can be implemented with the usage of an association SSID with a corresponding access point group of access points. [2] The SSID provides a mechanism to sequence a wireless network into multiple networks services by one or more access point such that client computers must be configured with the correct SSID to access the AP, the SSID acts as a simple password and thus provides a measure of security.

IV. ADVANCED WIRELESS LAN SECURITY TECHNIQUES

There are other advanced security measures that could be deployed in enhancing the security of data transmission over a Wireless LAN. These security features are as follows:

I. MAC Address Filtering – This method deploys the usage of the unique medium Access control (MAC) identifier that is part of every Ethernet devices [2]. Here the access points can limit which clients can access the network by using a list of authorized MAC addresses.[2][3]. If the client‘s MAC address is not listed the client is denied access. This procedure is very effective for smaller operations where the MAC address list can be efficiently managed.

II. WEP-based security- As earlier discussed the WEP security protocol provides encrypted communication between client and an AP. WEP technology deploys new technologies and various types of algorithm in safeguarding data transmission on wireless LAN. It has several architectural framework for implementing various authenticating schemes.

V. 802.11X WIRELESS LAN SECURITY ENHANCEMENTS

A. Extensible Authorization Protocol (EAP)

It is a framework for providing centralized authentication and dynamic key distribution. EAP lets wireless clients communicate through an access point with a RADIUS authentication server [2, 3]. Communication between the access point and the RADIUS server is through a secured channel. This Eliminates “main –in-the-middle attacks” by rogue access points and RADIUS server.[2] EAP when used with 802.1x, it provides an end-to-end authentication and wireless client that associates with AP cannot gain access to the network until the user performs a network login. When the user enters his credentials, the client and the RADIUS server performs a mutual authentication instead of one-way authentication, with the client authenticates by the supplied user name and password. EAP performs mutual authentication, where each side is required to prove its identity to the other using its certificate and private key.

B. Internet Protocol Security (IPsec)

It is a frame work collection of open standards for ensuring private communication over internet protocol (IP) networks. IPsec and VPNs use the protocol defined in IPsec to ensure confidentiality, integrity and authenticity of data transmission over public networks. [3] It deploys filters which prevent any wireless traffic from reaching any destination other than the VPN gateway. Confidentiality of the IP traffic is ensured via an encryption algorithm which encrypts the data three times with up to three different keys.

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 3, Issue 4, July 2014

C. LEAP

It is an extension of extensible authorization protocol (EAP) and it provides both mutual user-based authentication and centralized key management and distribution. [3]Addition key features of LEAP include:

- Secure key derivation

The initial original shared secured key derivation is used to construct responses to the mutual challenges which undergoes an irreversible one-way hashes that make password-replay attacks impossible.

- Dynamic WEP keys

In LEAP technology session keys are unique to the users and are not shared among them. In LEAP authentication, the broadcast, WEP key is encrypted using the session keys before being delivered to the destination client [3]. By having a session key unique to the user and by typing it to the network logon required by EAP, the solution also eliminates vulnerabilities due to stolen or lost client cards or devices.

- Re-authentication Policies

LEAP also allows administrators to set security policies for re-authentication at the backend RADIUS server. This forces users to re-authenticate more often and to get new session keys. This can minimize attacks where traffic is injected during the session.

VI. CONCLUSION

Wireless LAN is a communication network technology that provides connectivity to wireless devices within a geographic area. Corporate organizations, businesses and individuals are massively adopting the wireless local Area Network (Wireless LANs) because of flexibility and mobility to a flexible mobile user and its ability to provide the mobile user access to limitless volume of data anywhere anytime. It is gradually changing the way networked computing devices communicate. The major goal of the wireless LAN technology is to provide information and services on demand in a secure platform to a mobile user anytime, anywhere and in the desired quantity. However, the security of data transmission on WLAN still remains elusive and cannot be guaranteed. The convenience it offered by the ability to connect to networks using mobile computing devices has also introduced many security issues that do not exits in the wired world [3]. Because of the flexibility and ability to be accessed from anywhere, it is often more vulnerable to attack [5]. Therefore, in this paper, we x-rayed various security measures that could be deployed in ensuring the security of data in wireless local area Networks (WLAN).

REFERENCES

[1] L. Huang, K. Matsura, H. Yamane, and K. Sezaki, “Enhancing Wireless Location Privacy Using Silent Period”, In the proceedings of the IEEE Wireless Communications and Networking Conference (NCNC), 2005.

[2] R. Acharya, V. Vityanathan and R. Pether, “Wireless LAN Security – Challenges and Solutions”, International Journal of Computer and Electrical Engineering, Vol 1, No 3., 2009.

[3] K. Tyrrell, “An Overview of Wireless Security issues”, SANS Institute, 2003.

[4] K. Konstantinos, “Ten Steps to a Secure Wireless Network”, 2006.

[5] R. Scotland, “Unsecure or Secure: The Network Security Challenge for Small and Mid-Size Businesses”, 2013.

[6] N. Borisov, I. Goldberg and D. Wagner, “Security of The WEP Algorithm”, 2002.

[7] D. Frank, “Important Security Issues in Wireless Networks”, Cloud Computing Strategy, 2012.

[8] Y. Hu and H. Wang, “Location Privacy in Wireless Networks”, In the Proceedings of the ACM SIGCOMM Asia Workshop, 2005.