International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 09 Issue: 12 | Dec 2022 www.irjet.net p-ISSN: 2395-0072

Layer 2 Security for Wi-Fi, How 802.11w addresses some of the security issues of 802.11 standard and Experimental De-authentication and De-association denial of service attacks.

Bello Usman[1],Umar Usman Bello[2], Aliyu Uthman Bello[3]

[1]*Engineer, Directorate of Information and Communication Technology, ATBU Bauchi, Nigeria*
[2]*Lecturer, Department of Computer Science, FCT-College of Education, Zuba, Abuja, Nigeria.*
[3]*Lecturer, Department of Information Technology, Federal University Dutse, Nigeria.*

Abstract - ***This Paper appreciated the wide acceptability and inevitable need of Wireless Network in This 21stCentury but Cautiously Outlining the Vulnerabilities of Wi-Fi Technology. It showed how 802.11w addressed some but not all of the security issues associated with the 802.11 standard. The Experimental Results demonstrated the pathetic vulnerability of wireless Network clients as a result of De-authentication and Di-association Denial of service attacks****).*

Keywords—component, formatting, style, styling, insert (*key words****)***

1 INTRODUCTION

1.1 BACKGROUND

Wireless Data Network Technology Is the means of accessing the internet using wireless technologies instead of the traditional wired connection-using radio frequency to transmit packet data in a two-way communication. Wireless Local Area Network (WLAN) is a kind of Local Area Network (LAN) that utilises the concept of Frequency Radio than wires to enable network-enabled devices to communicate with one another (***WIRELESS NETWORKING SECURITY***). The wireless devices, normally hand-held and portable, include laptop Computers, Mobile cellular phones and PDAs etc. Transportation sectors, hotel providers, school campuses are now competing to provide wireless internet access to its teaming customers in order to attract potential customers or to provide more satisfaction to its already existing members or customers.

But The use of WLANs have its security consideration because of the associated security concern that is considered as a vulnerability in its operation.(MANAGING WIRELESS NETWORK) because intruders can access uncontrolled WLANs thereby interfering with network by either uploading a viral attack or blocking a transmission which is normally called Denial of service attack (D.o.S) etc. Thereby posing a lot of security concerns and begging for the need to ensure secure mechanism to be applied by the network administrators.

1.2 802.11 PROTOCOL INFORMATION

WEP, WPA, WPA2 are defined by 802.11 as security protocols for most probable countermeasures. The most recent of which is the WPAW, which stresses the concept of Data integrity, confidentiality and authenticity while somehow neglecting the issue of availability. Control and management frames in WAP2 are still sent in visible manner thereby making it an easy target for DoS attacks [1]

Security in Wireless and Mobile Networks is accorded a great deal of concern just like any wired Network, thereby necessitating the need for the implementation of encryption algorithm, that is normally common in 802.11 WLANs which is the Wired Equivalent Privacy (WEP). It uses 104 or 40 bit shared secret key which need manual configuration of the Access Point (AP) and the Radio Network Interface card (NIC) [2]

The paper was structured such that section 1 introduces the concept of Wireless Data Technology and associated Security issues and 802.11 protocol information. Section 2 discussed the 802.11 layer 2 security issues. Section 3 discussed the Experimental Method. Section 4 presented the results of the experiment and Section 5 discussed the achieved result.

2.0 802.11 LAYER 2 SECURITY ISSUES

Layer 2 is the Data-link layer of the Open System Interconnection (OSI) model including that moves data over the physical links in a Network. This involves using a switch to redirect the data messages via destination Media Access Control (MAC) to ascertain the target destination of the redirected message.

The major types of attacks associated with 802.11 are Denial of service, impersonation, Integrity, Physical and disclosure. Some of the Vulnerabilities of 3.0 802.11 include Dissociation attack , passive monitoring , packet spoofing , Rough Access points , Online dictionary Attack, Pre-Computed Dictionary attacked , Impersonation and NIC Theft etc[3].

Management frames in WLANs via a rogue AP can launch doS attacks even when WAP2 is already in place. WAP1 and WAP2 are normally a protection for Data frames but not management Frames(Zhang and Sampalli 2010).

[4]) proposed an alternative Authentication Server(AS) which they called Central Manger (CM) that manages APs in a dynamical nature thereby acting as a Backend Server that pinpoints clients to avert DoS. Attacks in an authentication chain of operation.

Deauthentication/Deassociation Attacks In 802.11 standard is when cryptographic protections is not applied to the management frame which will open an opportunity for tapping/listening of the station together with AP, and the attacked can clone the Deauthentication/Deassociation frames pass it to either of the client or AP. Some of the countermeasures include MAC address spoof detection, management and control Cryptography among others.([5]

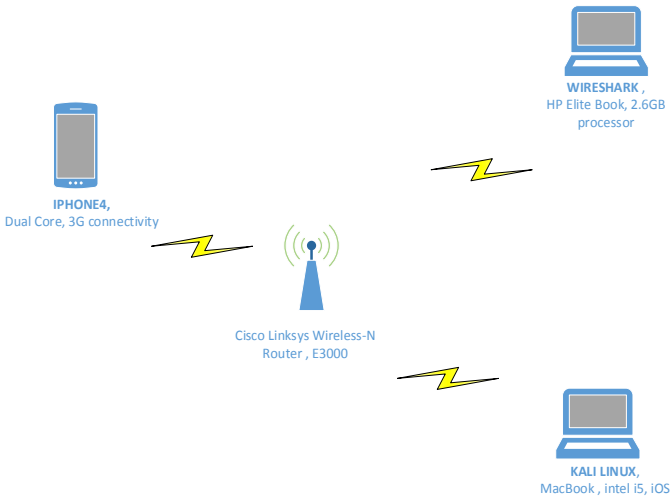
3.0 **802.11w: Layer 2 Security issues and Contribution to Enterprise Network Design.**

Due to the fact that Management frames are nowadays used to transmit sensitive and delicate information over a wireless network, IEEE introduced an amendment to 802.11 standard and proposed it to be named 802.11w. In the years before the advent of 802.11, Data frames are the only frames requiring protection while users don't care about protection on Control frames and management frames. Some of the DoS attacks include Authentication attacks, which is done by taping the MAC address of the victim AP after Careful learning/listening process. Others include Association request and response and Re-Association request and response. Furthermore, there is Dissociation and DE authentication in addition to EAPOL and jamming attacks [6].

Robust management (RM) frames provides partial solution to management frames attacks preventing impersonation and avoids listening capabilities. Cisco have an anti-forgery system that that addresses RM which is Management Frame Protection (MFP). Since WEP is no longer desirable security, BIP (broadcast Identity Protocol is provided to provide message protection and regulating access. Some of the vulnerability includes Radio frequency jamming attacks, Deadlock attacks prior to the commencing of Association and Reassociation and SA Query which leads to MESSAGE deletion. Others include Request-to-send and Clear-to-send attacks as well as Association starvation. Some of the solution in which 802.11 addresses these security issues are; Secure Control Packets (SCP), Temporary Safe Tunnels and Deadlock detection Systems [7].

In their paper, [8] proved that 802.11w can counteract attackers only before group and 4-way handshakes are completed but not before then it is helpless. They finally opined that Temporary Safe Tunnel is a better alternative to 802.11w which is susceptible to forgery, eavesdropping and distortion.

4.0 EXPERIMENTAL METHOD



The above diagram depicted the method employed which presented in two subsections, i.e. the first one outlining the devices, tools and the experimental set-up while the other Sub section describes the manner in which the experiment was carried out.

4.1 **DEVICES USED**

The devices used include **ACCESS POINT (AP)**, **Wireless USB Network Adapter**, **Computer Laptop(s)** and a **smart mobile phone**.

ACCESS POINT: The AP was the exchange facility that allows access to network devices into the network. It was a Cisco LINKSYS Wireless-N Router and the model was E3000

WIRELESS USB NETWORK ADAPTER: This was the device used interfacing the Access point to the Computer. It was Linksys Wireless-N Network Adapter and the Model was WUSB600N.

NOTE: I made sure that this particular USB supports the Kali Linux software.

COMPUTER LAPTOP The Computer laptop with a running Windows Operating System (OS) was used. It was a HP Elite book E50 G2, 2.60GB processor and 64-bit Operating system. We also used another laptop to run the Wireshark Tool. It was a MacBook Pro, Intel i5, 4G RAM, iOS.

MOBILE PHONE: My mobile phone was used as the client with the following details. It was an Apple iphone4 Dual Core. The OS is iOS and the connectivity status is 3G, Bluetooth, GPRS and GPRS.

4.2 TOOLS

Wireshark: This is a tool for Network Analysis and troubleshooting such as Packet and Network Traffic capturing and monitoring etc. It is supported by most OSs including the Windows and Linux used for this experiment.

KaliLinux: This the Software for Digital forensic and penetration testing. It is a Debian derived Linux distribution funded and maintained by Offensive Security Lt

The Experimental Setup

The Laptop Computer was used as the attacker and the Mobile phone was used as the victim client. A Virtual Box Linux was installed on the OS of the Laptop and thereafter Linux was also installed on the virtual Box. The Laptop was also used to setup the Access Point by first inputting the IP Address of the router AP which is 192.168.1.1 and then changing the administrative password and the WPA wireless key was set in place. The SSID was set as the initials of my full name which was my network name. The Linux Virtual box was created on my windows OS and then Kali Linux was installed on the Virtual Box.

The Main Experiment was carried out mostly utilizing the terminal of the kali Linux by launching a ping commands for Detecting the All the available APs on the Wireless USB Network Adapter within range. Using; ***''airodump-ng wlan0*** ''which revealed the various MAC addresses of the nearby APs specifically the one used for this experiment; **C0:C1:C0:4C:A4:F6,** It also showed the beacon frames and Data frames among other authentication details. The ESSID of **''LAB_WIRELESS''** was also displayed. The next step was that another ping command was launched on the kali Linux terminal to search for all available device(s) found on the AP which is ; **''airodump-ng –c 1 –bssid C0:C1:C0:4C:A4:F6 –w dump wlan0**''which eventually revealed the MAC Addresses of both the AP and my mobile phone as well as the frames probe. Furthermore, another ping command was launched on the Kali Linux Terminal to achieve Dissociation of the victim client (my Mobile phone) from the AP connection. ''**aireplay-ng -0 – 300 –a C0:C1:C0:4C:A4:F6 –c E0:C9:7A:35: BB:45 wlan0**'' command was launched to achieved the Dissociation by sending De-Authentication packets including the period for the dissociation which 300seconds in this case. Note that attacker can abort the attack any point before the expiration of the set period by using ''control C'' command.

Another aspect of the Experiment was the use of Wireshark tool for monitoring and evaluation of the Management and the Control Frames using the following commands on the Wireshark to achieve the targeted result. **Wlan.fc.type eq 0** for Management frame. **Wlan.fc.type eq 1** for Control frames. **Wlan.fc.type eq 2** for data frames. **Wlan.fc.type_subtype eq 0** for Association Request. **Wlan.fc.type_subtype eq 1** for Association Response. **Wlan.fc.type_subtype eq 4** for Probe request. **Wlan.fc.type_subtype eq 5** for Probe response. **Wlan.fc.type_subtype eq 11** for Authentication and finally **wlan.fc.type_subtype eq 12** for De-Authentication.

5.0 RESULTS

The Results of Experiment can be shown below from the screen snapshots;

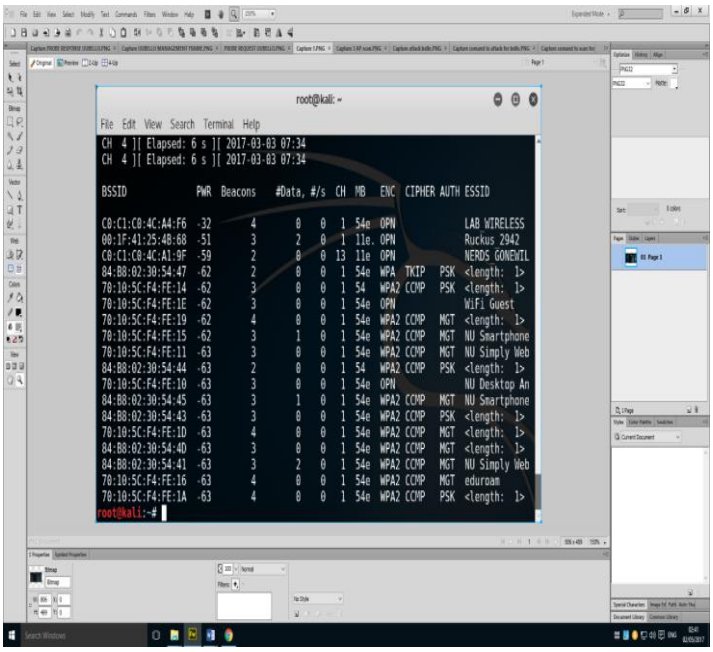


Figure a: Showing all the available APs associated the USB wireless Card including the AP

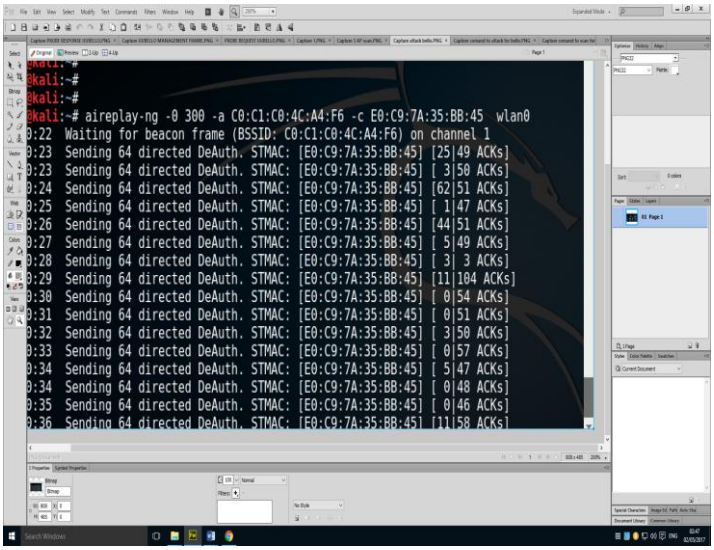


Figure b: Showing the all the devices connected to AP showing MAC addresses of the client(s)

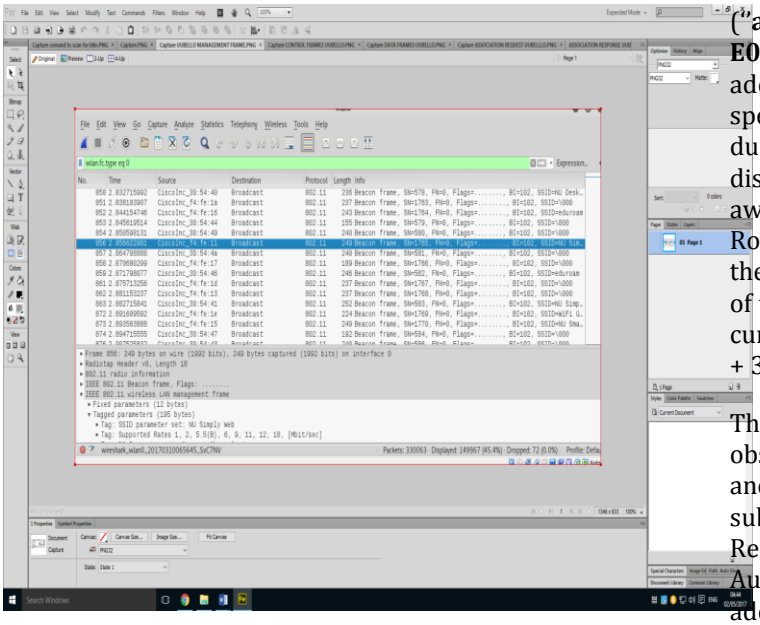


Figure c: Management frames

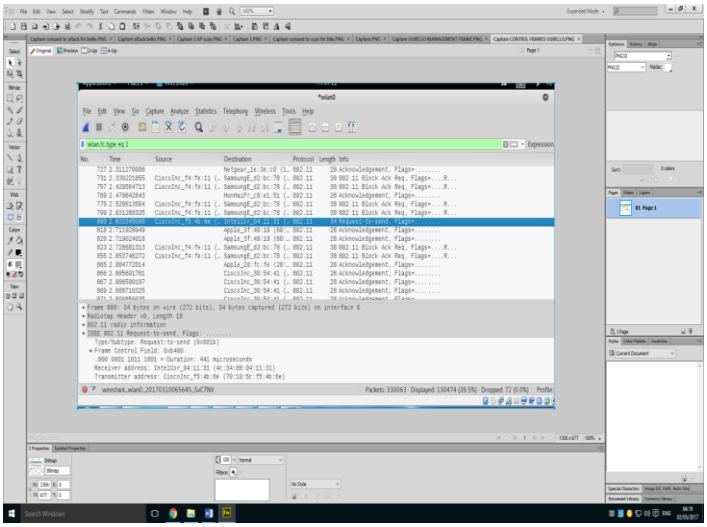


Figure d: Control frames

6.0 **DISCUSSION OF RESULT**

It was a good experimental beginning when the AP was setup and connected to the Computer Laptop via the Wireless USB Network Card. The initial Kali Linux response of the *''airodump-ng wlan0''* command showed all the available APs in the Room but we picked the LINKSYS E3000 Wireless-N Router which was already been named LAB_WIRELESS on channel 1 and that's when we identified the MAC address of the AP. The next command on the kali Linux Terminal (''**airodump-ng –c 1 –bssid C0:C1:C0:4C:A4:F6 –w dump wlan0**'') also proved useful as we were able to also see the MAC Address of my mobile phone been synchronized with the AP. This made it possible to eventually launched a successful attack on the client Victim (my Phone) from the Command (''**aireplay-ng -0 – 300 –a C0:C1:C0:4C:A4:F6 –c E0:C9:7A:35:BB:45 wlan0**'') by including the MAC address of both the AP and the Victim Client. More so, specifying the duration of the dissociation of 300secs during which we realized that our phone was practically disconnected from the Network. When we tried moving away the laptop away from the AP on 2nd floor S3 lab Room to the ground floor, The connection disconnected on the ground floor by the stairs thereby having a rough idea of the distance using a mobile Phone Application to have a cumulative distance of 51.60meters.(7.7m + 15.2m + 4.4m + 3.5m + 12m +8.8m).

The output results displayed by Wireshark have made us observed the various packets of the Management, Control and data frames. We also appreciated the discovery of subsidiary packets of both Association and Probe Requests/Responses as well as the Authentication and De-Authentication packets. Receiver and transmitter MAC addresses were recaptured. Beacon sub-frames of Management's frame were clearly seen, Blocking request acknowledgement and Request-to-send flags of the Control frames were shown among other numerous details that can be seen in the attached screen snapshots.

7.0 CONCLUSION

This paper discussed how 802.11 addresses layer 2 issues that showed the vulnerabilities of our wireless Networks we use on daily basis. It also showed how 802.11w addresses some the vulnerabilities as an amendment to 802.11 standard while cautiously pointing out its limitations. The experiment carried out exposes how MAC addresses can be spoofed and used for attacking a victim client using the relevant digital forensic and detection tools specifically kali Linux using Deauthentication and Deassociation DoS attacks.

REFERENCES

1. K'Ondiwa, N. and E. Ochola (2013). An anti-DoS attack architecture for wireless IT Infrastructure. Information Science, Computing and Telecommunications (PACT), 2013 Pan African International Conference on, IEEE.

2. Weber, R., et al. (1998). A quantitative analysis and performance study for similarity-search methods in high-dimensional spaces. VLDB.

3. Simon, D., et al. (2000). "IEEE 802.11 security and 802.1 X." IEEE document**802**(1): 1-00.

4. Zhang, Y. and S. Sampalli (2010). Client-based intrusion prevention system for 802.11 wireless LANs. Wireless and Mobile Computing, Networking and Communications (WiMob), 2010 IEEE 6th International Conference on, IEEE.

5. Ding, P. Q., et al. (2004). Improving the security of Wireless LANs by managing 802.1 X Disassociation. Consumer Communications and Networking Conference, 2004. CCNC 2004. First IEEE, IEEE.

6. Bicakci, K. and B. Tavli (2009). "Denial-of-Service attacks and countermeasures in IEEE 802.11 wireless networks." Computer Standards & Interfaces**31**(5): 931-941.

7. Ahmad, M. S. and S. Tadakamadla (2011). Short paper: security evaluation of IEEE 802.11 w specification. Proceedings of the fourth ACM conference on Wireless network security, ACM.

8. Wang, W. and H. Wang (2011). Weakness in 802.11w and an improved mechanism on protection of management frame. 2011 International Conference on Wireless Communications and Signal Processing (WCSP).