IEEE 802.11 Attacks and Defenses

May Aye Chan Aung, Khin Phyo Thant
University of Computer Studies, Mandalay
mayayechanaung@gmail.com, khinphyothantucsy@gmail.com

Abstract

Protection of IEEE 802.11 networks means protection against attacks on confidentiality, integrity and availability. Possible threats come from vulnerabilities of security protocols. The rapid growth in the use of wireless networks attracts the attackers as a target. Wireless traffic consists of management, control and data frames. An attacker can manipulate these frames that affect the data integrity, confidentiality, authentication and availability. A real Wireless Local Area (WLAN) testbed setup is proposed for performing the vulnerabilities of well-known attacks pertaining to IEEE 802.11 network and monitoring the analysis of packets. Based on these categories of vulnerabilities and threats, Confidentiality Attack: Evil Twin Availability Attacks: Deauthentication Disassociation and Café Latte and Authentication Attack: Dictionary attack are conducted through demonstrations in a real environment by using proposed setup.

Keywords: IEEE 802.11; Media Access Control (MAC); DoS; Disassociation; Deauthentation

1. Introduction

Since air is used as medium for wireless network access, wireless security is the major issue for every communication network. Today, wireless technology plays an important role in every aspect of our lives, both personal and public. However, the growth in the use of wireless technology has brought new challenges and limitations to user's privacy. Wireless and mobile networks provide new challenges because of their nature on relying on network signals without exact or known boundaries. Therefore, the security area of wireless network and has become essential and needs to be protected from attacks.

In wireless security, three protection of any packet transmitted over the air: Confidentiality, Integrity, and Availability are mainly managed by various protocols such as Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), and Wi-Fi Protected Access 2 (WPA2). But, IEEE 802.11 network is still vulnerable from availability attacks such as Denial of Service (DoS) attacks. Attackers can launch malicious DoS attacks by flooding authentication, deauthentication, association, and disassociation and so on. There are tools available to prevent these attacks. Many of these tools can be found in the BackTrack and Kali Auditor Security Collection.

The IEEE 802.11 standard defines the two lower layers of the OSI model for wireless communications. The 802.11 standards defines two communication modes: ad hoc mode, in which wireless stations communication directly with each other and Infrastructure mode, in which all communication take place through a fixed access point (AP).

Three types of frame (packet) in 802.11 networks are management, control and data. Each frame type has its own subtypes. Management frames are mainly used for network management and admission control. Control frames are mainly used for access control, and data frames carry data. Certain management frames are exploited by adversaries to launch DoS attacks against IEEE 802.11 networks.

Therefore, this paper focus on management frames among on these three frame types. This paper only considers in 802.11 infrastructure operation mode. This paper is structured as follows: In the next section, defense in depth for IEEE 802.11 standard is described. Section 3 describes about detection techniques. Proposed testbed setup is shown in section 4. Attack demonstration is described in section 5. Attack analysis is described in section 6. The final conclusion is drawn in section 7.

2. Defense in Depth for IEEE 802.11 Network

Defense in Depth comes from the military strategy of utilizing multiple levels of defense to make the enemies' job harder and more complex. These same countermeasures need to be used to

protect assets in an enterprise [15]. The National Security Agency (NSA) recommends a balance between the protection capability and cost, performance, and operational considerations.

Defense in Depth is one of the first steps to securing wireless. Each layer of security slows the attacker; examples include using Wi-Fi Protected Access 2 (WPA2) protection, enabling Wireless Intrusion Detection Systems (WIDS), actively scanning and monitoring for rogue devices [8]. For selecting the proper layers of defense, understanding the types of adversaries' aids determines how to prioritize their deployment. Knowing what types of adversaries and their motivations is one of the first steps to a successful Defense in Depth strategy. Adversaries could include Insiders, Hackers, Nation States, Criminals, Competitors or Terrorists. Motivations could be as simple as pride or bragging rights to theft or denial of service. Without a basic understanding of the types of attackers and their motives, businesses have no idea what to attempt to protect.

2.1. IEEE 802.11 Attacks

802.11 devices use management frames for the discovery, authentication and association of WLAN clients to an access point. Many of these management frame types are not authenticated and thus vulnerable to DoS attacks [17]. Because management and control frames are not protected, adversaries could exploit this fact to launch DoS attacks on 802.11 networks. The most efficient exploit is to flood the surroundings with huge amounts of deauthentication or disassociation frames.

Attacks on wireless networks can be categorized into passive attacks and active attacks. Passive attacks do not involve in altering resources. These attacks are mainly a threat to the confidentiality. A passive attack occurs when someone listens to or eavesdrops on network traffic. Active attacks involve in altering of resources. In active attacks, the aggressor node has to spend some of its energy in order to carry out the attack.

Wireless network attacks include probing and network discovery, DoS attacks, impersonation, main-in-the middle attack etc. Most of the attacks were based on the physical layer and the link layer. The physical layer deals with the radio signals. The link layer deals with exchange of frames. This paper concentrates on link layer attacks.

2.1.1 Deauthentication Attack

Deauthentication attack is a kind of masquerading denial-of service (DoS) attacks that targets communication between a client and a wireless access point (AP) [19]. In this attack, the attacker stop successfully the client to complete the four-way handshake and to establish the connection to wireless access point. This attack is carried out in two ways:

1) To attack the target clients or stations
2) To attack the target access point

2.1.2 Disassociation Attack

After authentication, an association message is exchanged between a client and AP to associate client to AP. An attacker sends a spoofed message to an AP, on receiving the message; AP dis-associates the client whose MAC address is mentioned in the message [19].

2.1.3 Evil twin Attack

An evil twin is a rouge or fake wireless access point (WAP) that appears as a genuine hotspot offered by a legitimate provider **[**3**].** Evil twin is a type of Wi-Fi attack. In this attack, an eavesdropper or hacker creates this rouge hotspot to collect the personal data of unsuspecting users. Sensitive data can be stolen by spying on a connection or using a phishing technique.

2.1.4 Caffe Latte Attack

The Cafe Latte attack allows you to get a WEP key from a client system. This attack is done by capturing an ARP packet from the client, manipulating it and then send it back to the client. The client in turn generates packets which can be captured by airodump-ng. Subsequently, aircrack-ng can be used to determine the WEP key [2]. The attack name come from the concept that a WEP key could be obtained from an innocent client at a coffee bar in the time it takes to drink cafe latte.

2.1.5 Dictionary Attack

A dictionary attack is a form of brute force attack. For defeating a cipher or authentication mechanism by trying to determine its decryption key or passphrase by trying hundreds or sometimes millions of likely possibilities, such as words in a

dictionary [4]. Attackers utilizes a wordlist predefined list of words.

3. Defenses Techniques

Many researchers have already discovered numerous attacking strategies. The classical defense against layerwise attacks are intrusion detection systems (for detection) and filtering (for prevention) and. In this section, Access point monitoring, Wireless client monitoring and Wireless traffic monitoring are studied. Wireless attacks detection techniques to sufficiently detect all of the above mentioned types of attacks in the next sub-sections.

3.1 Access Point Monitoring

Typically Access Point (AP) monitoring entails the owner of the wireless network having a list of authorized AP equipment with their corresponding SSID, MAC address, and channel information recorded as a baseline. Then, the monitoring component will listen to wireless frames (beacons, probe response and authentication / association frames etc.,) sent out by all its AP and compare these information to the pre-recorded information. The monitoring devices listen to all possible channels and record all packets for this technique to be effective [10].

3.2 Wireless Client Monitoring

Unlike APs, it would not be possible to have a list of "allowed" client information baseline without incurring a whole lot of administrative overheads. Nevertheless, the several aspects of the wireless clients can be monitored [10].

Firstly, the owner could keep a "blacklist" of wireless clients that would be checked against all connecting clients, any client within this list trying to access the network would be automatically denied and an alert send off. Secondly, all wireless clients with an "illegal" MAC address will be automatically denied access and an alert send off.

Thirdly, wireless clients that sends out probe requests or wireless clients that send out special distinguishable data packets after the initial probe request. Lastly, for wireless clients that have been authenticated and associated, the sequence number field within the IEEE 802.11 header can be tracked for sudden changes. Usually, when an impersonation attacks occur, the attacker obtain the victim's MAC / IP address, but it will not be able to continue with the sequence number used previously by the victim. Thus, potential impersonators could be identified by monitoring the sequence number in these client generated packets.

3.3 Wireless Traffic Monitoring

Wireless traffic can be monitored for flooding the network using deauthentication, de-association, authentication, association, erroneous authentication frames. Frequency and Signal-To-Noise Ratio (SNR) monitoring could help signal an oncoming Radio Frequency (RF) based DOS attack on wireless network. Failures in authentication and association can also be monitored and reported [10].

4. Proposed Testbed Setup

Based on WLAN vulnerabilities and attacks' categories, Aircrack-ng suite by default in kali linux is used to carry out the attack. A real Wireless Local Area Network (WLAN) had been setup for performing the various attacks and monitoring packet analysis. A laptop machine running on Kali OS acted as an attacker machine. Another Laptop with Wireshark running on Kali OS was acting as a monitoring machine for detecting intrusions. More importantly, all the machines were communicating via the wireless N router in IEEE 802.11 b/g/n WLAN technology with 2.4-54 Mbps data rates and 2.4-2.4835 GHz frequency bands. A graphical representation of the proposed system is shown in figure 1.

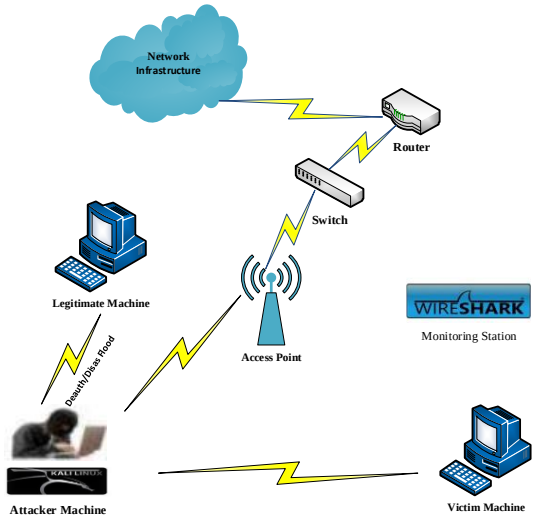

Figure 1. Proposed Testbed Setup

The following subsections provides a brief description of the necessary hardware and software for this research work to perform attacks.

4.1. Hardware Requirements

The hardware requirements include one Wireless Access point/Router, one client station, an attacker laptop, a victim (targeted) machine, a monitoring machine one Wireless USB adapters for Desktop and one portable Wi-Fi hotspot.

Table 1. Hardware Specifications

No.	Device	Mfg. Company	Model No.
1	300 Mbps Wireless N Router	TPLINK	TL-WR940N/TL-WR941ND
2	150 Mbps High Power Wireless USB Adapter	TPLINK	TL-WN7200ND
3	Portable HSPA+WiFi Hotsopt	PROLINK	PRT7001H

Table 2. Hardware/Software configuration in experiments

Function	Model	CPU	RAM	O.S.
Attacker (Laptop Machine)	HP (Model: T7570)	Intel (R) Core (TM) i7-6500U CPU @ 2.50GHz	8 GB	Kali (4.8.0-kali2-amd64)
Client Station	Che-UL00	Octa-core 1.2 GHz	1 GB	Android 4.4.2
Monitoring	Acer Laptop Machine (Aspire E5)	Intel (R) Core (TM) i3 -5005U CPU @ 2.00GHz	4 GB	Kali (4.18.0-kali2-amd64)
Victim (targeted)	HP nippon	Intel (R) Core (TM) i7-2600 CPU @ 3.40GHz	4 GB	Window 7 Ultimate

4.2 Tools and Utilities

In proposed testbed, Aricrack-ng suite and mdk3 are used to launch the attacks and Wireshark is used for monitoring and analyzing packets.

- Aircrack-ng utility on Linux is used for scanning and cracking wireless networks encryption [1]. It can be used for any NIC, which supports raw monitoring mode.
- MDK3 is a proof of concept tool. It is used for stress testing 802.11 networks (wi-fi). It consists of various methods by which we can perform tests.
- Wireshark is a free and open-source packet analyzer. It is used for profiling network traffics and analyzing packets.

5. Attacks Demonstration

For this demonstration, a dummy SSID named Surge MAC" which is broadcasted by my lab. It is simply protected by WPA2. The victim is connected on this SSID and can navigate to Internet without problem. Using kali linux distro, wireless networks will be sniffed to find all needed information to run this attack.

The experiment proceeds with the following categories of 802.11 attacks shown in table 3.

Table 3. Categories of 802.11 Attacks

Attack Name	Purpose	Target	Methodology	Tool
Deauthentication	Availability (DoS)	Client	Flooding	Aireplay
Disassociation	Availability (DoS)	Client	Flooding	Mdk3
Evil Twin	Man-in-the-Middle	Client	Impersonation	Airbase-ng
Caffe Latte	Keystream Retrieving	Network	Impersonation	Aireplay
Dictionary	Key Cracking	Network	Passive	Aircrack

Before attacks are being conducted, information gathering is firstly done.
Using iwconfig, see available wireless interfaces.
Using airmon-ng", generate the monitor interface.
Using airodump-ng", gather information of the surrounding AP.
A details for each attack is as follows.

(1) Deauthentication Attack

Using "aireplay-ng", launch with deauthentication attack.
Usage: aireplay-ng -0 0 -a F8:1A: 67:59: 36:36 -c E0:19:1D: 34:54:A2 wlan0mon
Where:
-0 means deauthentication (1 is the number of deauths to send 0 means send them continuously).
-a F8:1A: 67:59: 36:36 is the MAC address of the access point.
-c E0:19:1D: 34:54:A2 is the MAC address of the client to deauthenticate.
wlan0mon is the interface name.

(2) Disassociaiton Attack

Using "mdk3", launch with disassociation attack.
Usage: mdk3 wlan0mon d Where:

d means disassociation mode.
wlan0mon is the wireless interface name.

(3) Cafe Attack

Using "aireplay-ng", launch with cafe attack.
Usage: aireplay-ng -6 -h E0:19:1D: 34:54:A2 -b F8:1A: 67:59: 36:36 -D wlan0mon
Where:
-6 means Cafe-Latte attack
-h E0:19:1D: 34:54:A2 is the card of MAC address.
-b F8:1A: 67:59: 36:36 is the Access Point MAC
-D disables AP detection.
wlan0mon is the wireless interface name.

(4) Evil Twin Attack

Using "airbase-ng", Generate AP
Usage: airbase-ng –e "Surge MAC" –c 4 –P wlan0mon
Where:
-e is network name of the access point.
-c is the channel to listen on.
-P responds to all probes, even when specifying ESSIDs.
wlan0mon is the interface name.

(5) Dictionary Attack

Using "airodump-ng", collect information from target AP.
Using "aireplay-ng", launch with dictionary attack.
Using airodump-ng, collect WPA handshake.
Using aircrack-ng, launch with dictionary attack
Usage: aircrack-ng –w/usr/share/wordlists/rockyou.txt demo.cap
Where:
-w is the name of the default password file
.democap is the name of group of files containing the captured packets.

6. Attack Analysis

Above mentioned demonstrated attacks, the characteristics of these attacks are summarized. The resulting information from these attack:

- Deauthentication has a fixed subtype value represented by four bits (1100).
- The management deauthentication frame type that was forged and sent by the attacker is represented by two bits (00).
- The values of deauthentication and disassociation values are both fixed and sent in plain form (unencrypted form).

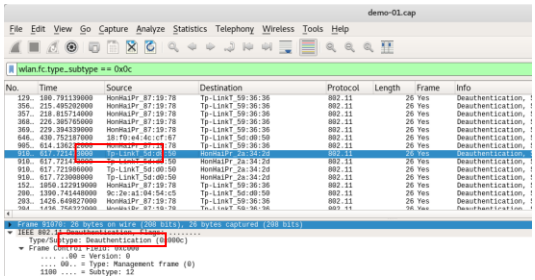

Figure 2. Analyzing Deauthentication Attack in Wireshark

Deauthenticaion attack is shown in figure 2, which is a screen analyzing the used packets with Wireshark network monitoring tool to analyze the real time aired packets.

The following figure 3 depicts the analysis of disassociation Dos attack scenario.

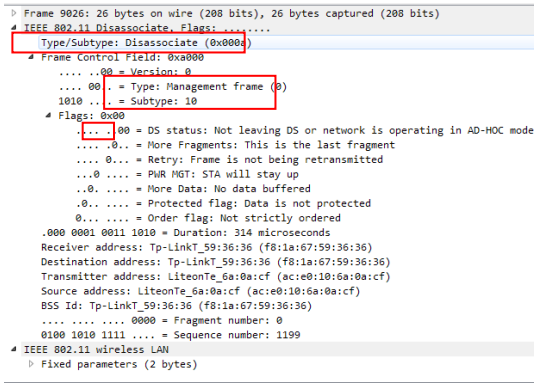

Figure 3. Wireshark Monitoring Disassociation Attack

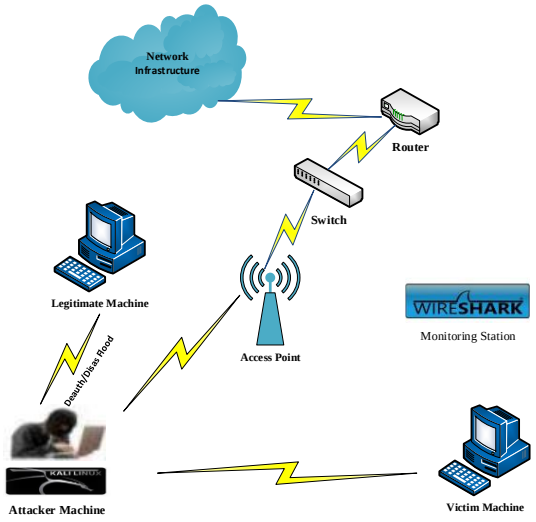

Figure 4. Cracking WPA Key

The above figure 4 indicates that the key was successfully found by the dictionary attack method. In the WEP active cracking, the ARP request is captured and replayed into the network for thousands of times. Each replayed packet gets a response from AP encrypted with WEP. And during WPA/WPA2 cracking, a mounts of deauthentication packets are not normal.

An attacker implement an evil twin attack by configuring a rouge AP which is similar to legal AP, such as SSID and MAC address. To force clients to connect to rouge AP, DOS attack will be performed, and rouge AP usually providing a stronger signal than legal one. Association or authentication flooding indicates a DOS attack.

7. Conclusion

IEEE802.11 wireless networks have become one of the most widely used networks. Hackers and intruders can make utilization of the loopholes of the wireless network due to undefined physical boundaries and shared nature of wireless medium. Attackers can access the signal to listen or cause more damage on the wireless networks. As a result, there are many security threats associated with IEEE 802.11 networks. In this paper, a real Wireless Local Area (WLAN) testbed has been setup for performing the vulnerabilities of well-known attacks pertaining to IEEE 802.11 network and monitoring the analysis of packets. After these attacks have been conducted, the characteristics of attacks have analyzed.

References

[1] http://www.aircrack-ng.org.

[2] https://www.aircrack-ng.org/doku.php?id=cafe-latte.

[3] https://en.techopedia.com/definition/5057/evil-twin.

[4] https://en.wikipedia.org/wiki/Dictionary_attack _note-1.

[5] Aneja, A. and Sodhi, G., "A Study of Security Issues Related With Wireless Fidelity (WI-FI)", *IJCST*, Volume 4, No. 2, pp. 346-349, 2016.

[6] Buchanan, C., Ramachandran, V., "Kali Linux Wireless Penetration Testing Beginner's Guide (2nd ed.)", *Birmingham B3 2PB, UK: Packt Publishing Ltd. Center for Internet Security*, October 15, 2015.

[7] Budhrani, R. and Sridaran, R., "Wireless Local Area Networks: Threats and Their Discovery Using WLANs Scanning Tools", *International Journal Of Advanced Networking & Applications*, pp.137-150, 2015.

[8] Cole, E., "SEC401: Security Essentials Bootcamp Style [Slides]", 2015.

[9] Compton, S. and Hornat, C., "802.11 denial of service attacks and mitigation", *SANS Institute InfoSec Reading Room*, pp.14-18, 2007.

[10] Christopher Low, "Understanding Wireless Attacks & Detection", *SANS Institute Info Sec Reading Room*, April 13, 2015.

[11] Feng, P., "Wireless LAN security issues and solutions", In *Robotics and Applications (ISRA), 2012 IEEE Symposium*, pp. 921-924, June, 2012.

[12] Gan, D., Waliullah, M., "Wireless LAN Security Threats & Vulnerabilities: A Literature Review", International *Journal of Advanced Computer Science and Applications (IJACSA)*, Volume 5, No. 1, pp. 176-183, 2014.

[13] Glass, S.M., "Wireless Networks: Attack and Defence Security in Emergency Communication Networks", Griffith University, 2011.

[14] Hanzo, L., Wang, X., Zou, Y., "A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends", *Proceedings of the IEEE*, 2015.

[15] Joseph F. Matthews., "A Secure Approach to Deploying Wireless Networks", *GIAC (GSEC) Gold Certification, SANS Institute InfoSec Reading Room*, 2016.

[16] Kumar, U. and Gambhir, S., "A literature review of security threats to wireless networks", *International Journal of Future Generation Communication and Networking*, Volume 7, No. 4, pp.25-34, 2014.

[17] O'Connor, T.J., "Detecting and Responding to Data Link Layer Attacks", *SANS Institute Info Sec Reading Room*, October 13, 2010.

[18] Shao-Long Wang, Jian Wang, Chao Feng and Zhi-Peng Pan, "Wireless Network Penetration Testing and Security Auditing", 3rd Annual *International Conference on Information Technology and Applications (ITA)*, Volume 7, 03001, 2016.

[19] T.Moore, "Validating 802.11 Diassociation and Deauthentication Message", IEEE TGI, 2002.

[20] Waliullah M, Moniruzzaman A B M, and Rahman M S., "An Experimental Study Analysis of Security Attacks at IEEE 802.11 Wireless Local Area Network", *International Journal of Future Generation Communication and Networking*, Volume 8, Issue 1, pp. 9 18, 2015.