# Wireless Network Penetration Testing and Security Auditing

Shao-Long WANG, Jian WANG, Chao FENG and Zhi-Peng PAN

*College of Electronic Science and Engineering, National University of Defense Technology Changsha, China*
*wangshaolong002@126.com,climbspider@hotmail.com*

***Abstract*—**IEEE802.11 wireless wireless networks have security issues that are vulnerable to a variety of attacks. Due to using radio to transport data, attackers can bypass firewalls, sniff sensitive information, intercept packets and send malicious packets. Security auditing and penetration testing is expected to ensure wireless networks security. The contributions of this work are analyzed the vulnerability and types of attacks pertaining to IEEE 802.11 WLAN, performed well known attacks in a laboratory environment to conduct penetration tests to confirm whether our wireless network is hackable or not. WAIDPS is configured as auditing tool to view wireless attacks, such as WEP/WPA/WPA2 cracking, rouge access points, denial of service attack. WAIDPS is designed to detect wireless intrusion with additional features. Penetration testing and auditing will mitigate the risk and threatening to protect WALN.

## 1 Introduction

WLAN uses radio frequencies as the medium to transport data. This exposes layer 1 and layer 2 in the range of the wireless network. WLANs typically operate within two frequency ranges—2.4 GHz and 5.0 GHz at the standard 802.11a/b/g/n. In each of band, there are multiple channels. Everyone can sniff the entire airspace by putting the card into monitor mode in the same channel. WALN communication happens over frames. There are three different types of 802.11 MAC frames, data, control, and management [1]. The majority of wireless attacks target management frames, because they are responsible for authentication, association, disassociation, beacons, and probe request/response [2]. Wireless attacks like denial of service attacks, man-in-the-middle attacks are implemented within the 802.11 frames and can't be detected at layer three past the access point [3]. Unlike traditional intrusion detection systems in a wired network, detecting attacks in a wireless network is at layer two. Penetration testing will help find and plug insecurities which could be exploited by attackers. Measures must be taken on a wireless network in order to have proper vision to view wireless attacks. We expect for a way to be used as a reference for practitioners to protect their WLAN from wireless attacks.

## 2 Security measures and Attacks Based on the Flaws of IEEE 802.11 WLAN

### 2.1 SSID Hiding and Packet Sniffing

Packet sniffer can give plentiful information about ESSID, BSSID, channels, encryption protocol, power etc. This allows attacker to gather information about a Wi-Fi access point. In general, access point will send out its SSID in the Beacon frames. Default SSID comes with its username and password. This brings potential security vulnerability. There are some common default username-passwords: "admin-admin"/TP-LINK, "adsl-adsl1234"/ASUS, "cisco-cisco"/CISCO etc.

Though SSID can be hidden, whenever a legitimate client tries to connect to the access point, they exchange Probe Request and Probe Response packets. These management contains SSID. So hidden SSIDs is a security feature which is relatively simple to beat.

### 2.2 MAC filter and spoofing

Once MAC filtering is enabled, only the authorized MAC address can be able to successfully authenticate to the access point. However there are various available tools we can utilize to change the wireless card's MAC address of the client like: "mac-changer" under LINUX and "MAC address changer" under Windows. It is possible to find authorized

MAC address from unencrypted packets through packets sniffing. Consequently MAC address filters do not provide any security.

### 2.3 Denial of Service

For a high level security environment, there are a variety of ways attacker can still exploit. WPA2-AES is still regarded as a robust encryption standard, it only applies to data frames and not currently to the management frames. Attacker tries to inject forged management frame into the network to conduct a DOS attack [4]. Currently main wireless DOS attacks are the following: Access Point Overloaded attack, Authentication Flood Attack, De-authentication Attack, Association Flood Attack, Disassociation Attack [5]. These attacks will lead to a wireless access point overloaded, service interruption, packets loss rate increasing, even need to restart the suspended AP.

### 2.4 Cracking Encryption

In order to prevent unauthorized users from eavesdropping or invasive wireless network, Wired Equivalent Privacy (WEP), an IEEE standard security algorithm was proposed in 1999, But cryptanalyst has identified several weaknesses in WEP, so IEEE 802.11 standard was developed in 2003 called Wi-Fi Protected Access (WPA), and was replaced by the IEEE 802.11i standard (WPA2) in 2004 [6]. The WEP protocol has been known to be flawed since 2000, but surprisingly it is still continuing to be used and most access points are still equipped with WEP capabilities.

WPA/WPA2 is stronger than WPE, but still vulnerable to dictionary and brute force attacks [7]. An attacker who eavesdrops the entire conversation will get five key parameters: SSID of Network, Authenticator Nonce (ANONCE), Supplicant Nonce (SNONCE), Authenticator MAC address (Access Point MAC), and Suppliant MAC address (Wi-Fi Client MAC) [8], which are essential for a force attack. The only thing needed is the Pre-Shared Key.

A dictionary attack used in WPA/WPA2 PSK, would use a large dictionary of possible passphrases. Firstly it derives each of 256-bit Pre-Shared Key from the dictionary and use it with the other parameters to create the PTK showed in Fig.1. Then the PTK will be used to verify the Message Integrity Check (MIC) in the second handshake packets [9]. If it matches, the passphrase guessed from the dictionary is correct

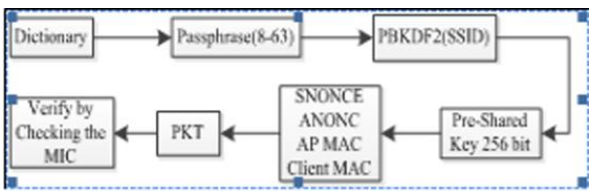


Figure 1. Steps of Dictionary Attack.

### 2.5 Man-in-the-Middle (MITM) Attack

MITM attacks are probably one of most potent attacks on a WLAN system by setting a rouge access point. Attacker prepare two interfaces, one creates the rouge access point and the other interface is connected to the authorized access point. Both these interfaces are bridged. These points broadcast an SSID similar to a local hotspot in vicinity. Users may accidently get connected to this rouge access point or can be forced to using the higher signal strength.

In MITM, victim's traffic is routed through the attacker's computer. Thus the attacker can eavesdrop on all the traffic sent to and from the victim's machine. It is often used with phishing sites. If the user's access to the bank's home page is redirected to the attacker's phishing sites, bank password will be defrauded. A rouge access point may even compromises the security of a WPA-Enterprise network running PEAP or EAP-TTLS [10].

## 3 Wireless Network Penetration Testing

Based on the vulnerabilities listed above, relevant attacks are executed in a wireless lab to conduct penetration testing. To setup the wireless local area network for performing the various attacks and monitoring or detecting them, the following hardware were used to set up the wireless lab: a wireless router, a Desktop machine, 2 laptops and 2 USB wireless adapters.

### 3.1 Wireless Sniffing and Bypass MAC Filters

In order to gain particular information about the local wireless network, an attacker would start running a packet sniffer. After discovering the brand of Wi-Fi router being used and authenticated clients, the attacker can try conducting more attacks. Airodump-ng is an excellent wireless network sniffer that can get plentiful information about local wireless network, including SSID, MAC address, channel, encryption protocol e.t, by setting the USB adapter into monitor mode. TABLE Ⅰ is the information gathered about Testing Lab, including its MAC address (BSSID), SSID (ESSID), encryption protocol (ENC), channel (CH), power (PWR), and packets transformed through the whole network.

**Table 1** Information Gathered about Target Ap

| BSSID | PWR | Beacons | #Data | #/ s | CH |
|---|---|---|---|---|---|
| 80:89:17:A3:F8:96 | -31 | 10 | WEP | WEP | 10 |
| MB | ENC | CIPHER | AUTH | ESSID | |
| 54e | WEP | WEP | Y | Testing Lab | |

At the same time, connected to target AP can be seen in TABLE Ⅱ. It is easy to bypass MAC filters using authorized MAC address with command:

macchanger –m wlan0. 28:C2:DD:9F:B8:95

**Table 2** Authorized Clients Connected to Target Ap

| BSSID | STATION | PWR | Rate |
|---|---|---|---|
| 80:89:17:A3:F8:96 | BE:53:E5:A4:6F:20 | -27 | 54e-54e |
| 80:89:17:A3:F8:96 | 28:C2:DD:9F:B8:95 | -27 | 54e-54e |
| Lost | Frames | Probe | |
| 8 | 846 | Testing Lab | |
| 0 | 582 | Testing Lab | |

### 3.2 WEP Cracking

WEP is a really old encryption technique and can be easily cracked. Many attack examples show that using known initialization vector IV and the first byte of the key stream, and combined with the characteristics of RC4 stream key algorithm, can calculate the WEP key. Firstly using airodump-ng to capture all packets sending in Testing Lab, with the command:

airodump-ng --bssid 80:89:17:A3:F8:96 -c 10 --write WEPcracking wlan0

In WEP cracking, we exploit weaknesses in the protocol which is data packets encrypted with the same IV. The only requirement is a great number of data packets. We need to force the network to produce more data packets through replay attack by capturing ARP packets and injecting them back to the network using tool aireplay-ng. Once enough data packets have been captured, Aircrack-ng will be used to crack WEP key. If data packets captured in the file are not sufficient, aircrack-ng will pause. Fig.2 indicates that enough IVs is collected and key was successfully found.

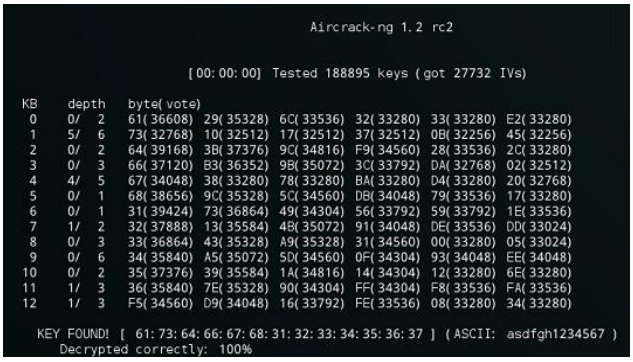


Figure 2. Successfully Cracking WEP.

### 3.3 WPA/WPA2-PSK Cracking

WPA/WPA2 PSK is vulnerable to a dictionary attack. The inputs required for this attack is the four-way WPA handshake between client and access point, and a wordlist containing common passphrases. In the same way, airodump-ng is used to capture the packets. The different is that we send broadcast de-authentication packets to force clients to reconnect, to speed up capturing the four-way WPA handshake packets using aireplay-ng.

The next is starting the dictionary key cracking. The prerequisite of a dictionary attack is that the passphrase must be present in the dictionary file. If the passphrase is not present, the attack will fail. Choosing dictionary is important, when going out for a penetration test. Passwords that people used depend on which country the users belong to, common names and phrases in that region, interests, range of birthday and security awareness of the users. We can execute the dictionary attack by aircrack-ng. WPACrackingDic.lst is the name of the default password file.

Aircrack-ng -w WPACrackingDic.lst WPAcracking-01.cap

In order to speed up cracking, another software uses dictionary to crack WPA and WPA2 password is Elcomsoft. Elcomsoft Wireless Security Auditor Professional (EWSA) is published by the Russian security firm Elcomsoft. The ability of this software is using the powerful graphics card parallel processing capability to crack wireless Wi-Fi network password. By offloading most runtime computation to NVIDIA/AMD GPU, overall hash cracking performance can be improved further. The cracking speed can be increased up to a hundred times compared to CPU. Fig.3 indicates that the key was successfully found.


Figure 3. Speed up Cracking WPA.

### 3.4 Man-in-the-Middle Attack with Rouge AP

MITM attack is one of the most damaged attacks in WLAN. There are many configurations could conducted a MITM attack. In WLAN the common method is setting up a rouge AP. Firstly, airbase-ng is used to create a soft access point. Then we create a bridge to consist the wired (eth0) and wireless (waln0) interface, and turn on IP Forwarding in the kernel. Traffic of clients will be forwarded through the attacker's host. Following command will set up a soft AP With the same name of Testing Lab. Then we send broadcast de-authentication packets. If clients miss-connect to rouge AP, we can eavesdrop on all the traffic sent to and from the clients using sniffer like Wireshark.

airbase-ng -a 3C:76:FB:5F:E3:81 --essid Testing Lab -c 1 wlan0

brctl addbr mitm-bridge

brctl addif mitm-bridge eth0

brctl addif mitm-bridge at0

ifconfig eth0 0.0.0.0 up

ifconfig at0 0.0.0.0 up

echo 1 >/proc/sys/net/ipv4/ip_forwar

The characteristics of wireless attacks are summarized. 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 de-authentication packets are not normal. An attacker implement a MITM attacker 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. We conduct security auditing based those characteristics.

4.Wireless Security Auditing Based on WAIDPS

WAIDPS is an open source wireless Swiss-knife written in Python and work on Linux environment. This is a multipurpose tools designed for audit (penetration testing) networks, detect wireless intrusion (WEP/WPA/WPS attacks).

Additional features are added to current script where previous WIDS does not have.

automatically save the attack packets into a file.

interactive mode where users are allow to perform many functions.

allow user to analyse captured packets.

load previously saved pcap file or any other pcap file to be examine.

customizing filters.

customize detection threshold (sensitivity of IDS in detection).

Fig.4 is the structure of the network in the lab. WAIDPS is installed on Host C, and Host C is the attacker, Host A is the target.

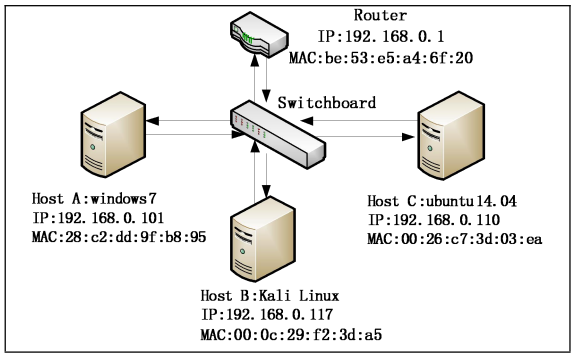


Figure 4. The Structure of the Network in the Lab.

Once wireless detect is found, WAIDPS will capture and analyze wireless packets, and detect and display suspicious data/activities, and display on screen and also log to file on the attack. Below is the alert log file during conducting the penetration testing. When we try to cracking WEP, we get an alert. In WEP cracking, the requirement is a great number of data packets, ARP Replay Requests will force the network to produce more data packets. This alert successfully detected WEP cracking attack, and actually the MAC of 00:0c:29:f2:3d:a5 is attacker's.

Possible Attack : [WEP . ARP . Replay Request] Detected !!!

:[00:0c:29:f2:3d:a5] is attacking Access Point [28:c2:dd:9f:b8:95]

When we send broadcast de-authentication packets in WPA/WPA2 cracking, DOS attack and MITM attack, the packets with frame type of de-authentication are high light show in TABLE Ⅲ. And the command of deauth filter can be used to check those packets to locate attacker. De-authentication packets is used to force clients to reconnect and speed up capturing the four-way WPA handshake packets. If a mass of packets of frame type of Deauthentication is detected, it indicates that WPA/WPA2 cracking, DOS attack or MITM attack occurred. The source MAC 00:0c:29:f2:3d:a5 is attacker's.

**Table3.** Deauthentication Packets Captured

| Rate | Source MAC | Destination MAC | LEN | Procotol | Frame Type |
|---|---|---|---|---|---|
| 1 Mb/s | 00:0c:29:f2:3d:a5 | FF:FF:FF:FF:FF:FF | 48 | 802.11 | Deauthentication |
| 1 Mb/s | 00:0c:29:f2:3d:a5 | FF:FF:FF:FF:FF:FF | 48 | 802.11 | Deauthentication |

When we set up a soft AP to conduct a MITM attack, we get two alerts. Client with MAC address 00:0c:29:f2:3d:a5 is found to be both an access point and wireless client. That indicates it could be a MITM attacker. The alerts accurately allocate the MITM attacker's MAC is 00:0c:29:f2:3d:a5.

Sililar SSID Names Detected !!!

SSID Name [Testing Lab]

Sililar SSID Names Detected !!!

Dual Device Type Detected !!!

Device MAC [00:0c:29:f2:3d:a5] is found to be both an Access Point & Wireless Client.

Commercial IDS is available for 802.11 like AirDefense, Cisco, that needs not a few cost. Open source project Snort Wireless appeared to be defunct. Another WIDS Kismet involves using something like a WRT54G Linux based wireless access point. WAIDPS is an effective tool for auditing wireless networks, detecting wireless intrusion (WEP/WPA/WPS attacks). The most important is that the only hardware needed is one USB wireless adapter. It is could be a convenient and effective reference for auditing.

## Conclusion

Wireless LAN is pervasive but still vulnerable. We try to minimize wireless threats through penetration testing and

intrusion detection. According to the penetration testing of WLAN, it is better to avoid setting the security mode to WEP. WPA/WPA2 is reliable, but the premise is an enough complex passphrase compounding of a number of numbers, letters and symbols. In the WLAN security auditing, WAIDPS could successfully detect and alert attack behaviors and display on screen and also log to file on the attack. It is a valuable reference for practitioners to protect their WLAN. It is always a challenge to protect WLAN and ensure the security of our networks. Penetration testing and security auditing make it possible to mitigate threatening and risks for a better security situation.

## References

[1] Abdallah C T, Jordan R. Wireless Communications Networking: and An Overview[J]. 2002.

[2] Sheldon F T, Weber J M, Yoo S M, et al. The insecurity of wireless networks[J]. Security & Privacy, IEEE, 2012, 10(4): 54-61.

[3] Wang L, Srinivasan B, Bhattacharjee N. Security analysis and improvements on WLANs[J]. Journal of Networks, 2011, 6(3): 470-481.

[4] Dacosta I, Chakradeo S, Ahamad M, et al. One-time cookies: Preventing session hijacking attacks with stateless authentication tokens[J]. ACM Transactions on Internet Technology (TOIT), 2012, 12(1): 1.

[5] Waliullah M, Moniruzzaman A B M, Rahman M S. An Experimental Study Analysis of Security Attacks at IEEE 802.11 Wireless Local Area Network[J]. International Journal of Future Generation Communication and Networking, 2015, 8(1): 9-18.

[6] Bernaschi M, Ferreri F, Valcamonici L. Access points vulnerabilities to DoS attacks in 802.11 networks[J]. Wireless Networks, 2008, 14(2): 159-169.

[7] Hwang H, Jung G, Sohn K, et al. A study on MITM (Man in the Middle) vulnerability in wireless network using 802.1 X and EAP[C]//Information Science and Security, 2008. ICISS. International Conference on. IEEE, 2008: 164-170.

[8] Mathews M, Hunt R. Evolution of wireless LAN security architecture to IEEE 802.11 i (WPA2)[C]//Proceedings of the fourth IASTED Asian Conference on Communication Systems and Networks. 2007.

[9] Parhi S. Attacks Due to Flaw of Protocols Used In Network Access Control (NAC), Their Solutions and Issues: A Survey[J]. International Journal of Computer Network and Information Security, 2012, 4(3): 31.

[10] Li J, Garuba M. Encryption as an Effective Tool in Reducing Wireless LAN Vulnerabilities[C]//Information Technology: New Generations, 2008. ITNG 2008. Fifth International Conference on. IEEE, 2008: 557-562.