ANALYSIS OF THE WIRELESS CLIENTS SECURITY FROM DOS ATTACKS

Korolkov R. Y., senior lecturer; Kutsak S. V., senior lecturer
National University "Zaporizhzhia Polytechnic", Zaporizhzhia, Ukraine

Security is one of the most important issues to consider in wireless local area networks (WLAN). WLANs are vulnerable to DoS attacks through manipulation of management frames. An attacker can fake a legitimate client's MAC address and perform a deauthentication attack to disable WLAN users from the access point. The consequences of a DoS deauthentication attack are frequent disconnection from the Internet, traffic redirection, "man in the middle" attack and network congestion. Despite tremendous efforts to counteract DoS attacks with deauthentication in the last decade, this attack is still a major security threat in 802.11 wireless networks.

To understand how harmful the threats associated with using WLAN are, the authors conducted a series of tests to identify WLAN vulnerabilities, namely, to discover the mechanism of deauthentication attack and its practical implementation.

The IEEE 802.11 Wi-Fi standard requires two mandatory sequential steps before the user can begin transmitting data: authentication and association. A client device sends a deauth frame of Wi-Fi to another device when it wants to end a secure connection. Deauthentication frame is a notification, not a request [1]. When receiving a deauthentication message (whether it is fake or real), no receiving party can refuse to execute it [2], unless the frame protection mode is on (802.11w: MFP or Management Frame Protection) and failed to successfully complete control against counterfeiting frame MIC (Message Integrity Check). Therefore, an attacker can launch a DoS attack by faking the legitimate client's MAC address and by running periodic frames of deauthentication [3]. Because authentication requests cannot be ignored, the access point responds promptly to those requests. AP responds by sending a reply about canceling client authentication. Should the attack continue, the client will definitely not be able to connect to the wireless network until the attacker cancels the attack. Therefore, a DoS attack is a critical attack that disrupts the client's current download and transaction.

The deauthentication attack was implemented using the Aircrack-ng wireless audit suite of the Kali Linux operating system. For the experiment, a dual band Wi-Fi adapter Alfa AWUS036ACH standard 802.11ac on the Realtek RTL8812AU chipset was used.

The experiment consisted of the following steps: 1) network card testing in monitoring mode; 2) capture and analysis of packages; 3) injection of frames.

In monitoring mode, the hardware interface is not connected to any network and is usually used for passive sniffing and packet injection. Another purpose of the monitoring mode is packet injection. Enter random IEEE 802.11 MAC frames using the radiotap header and the WLAN network interface possible to make only in monitoring mode. In Linux, injection is possible by combining the package with the radiotap header and sending it to the driver using the kernel socket features, fig. 1.

To determine if the network injection card supports, you must enable monitoring mode and run the command < aireplay-ng -9 wlan0>. The program sends broadcast probe requests, who interview all APs who have heard them, providing information about themselves. If any AP responds, a message appears on the screen indicating that the card can successfully make injection. In the next step, the airodump-ng command was used to capture wireless packets. It captures 802.11 frames for later use in aircrack-ng. After packet capture and analysis, important information such as MAC address, channel number, and advanced access point set (ESSID) access is available. Basic Service Set Identification (BSSID) is the MAC address of the AP, and STATION shows the MAC addresses of the wireless devices connected to the AP. Then a victim is selected and a deauthentication attack is implemented.

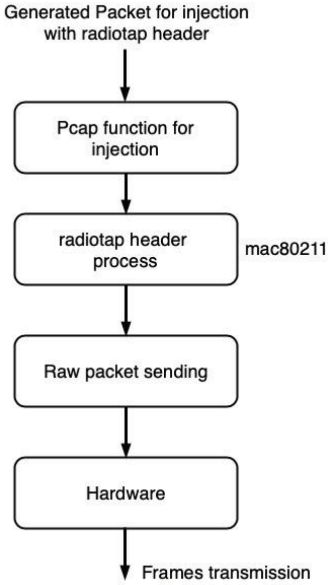
Generated Packet for injection with radiotap header
Pcap function for injection
radiotap header process
mac80211
Raw packet sending
Hardware
Frames transmission

Figure 1. Functional diagram of package injection

For a successful attack, the network card is configured to the desired channel and the aireplay-ng command specifying the MAC address of AP and the MAC address of the client was used to send the deauth packets.

Deauth frames were received at AP for 30 sec. At the time of the attack, the legitimate client was completely disconnected from the AP, which prevented any data transmission, fig. 2.

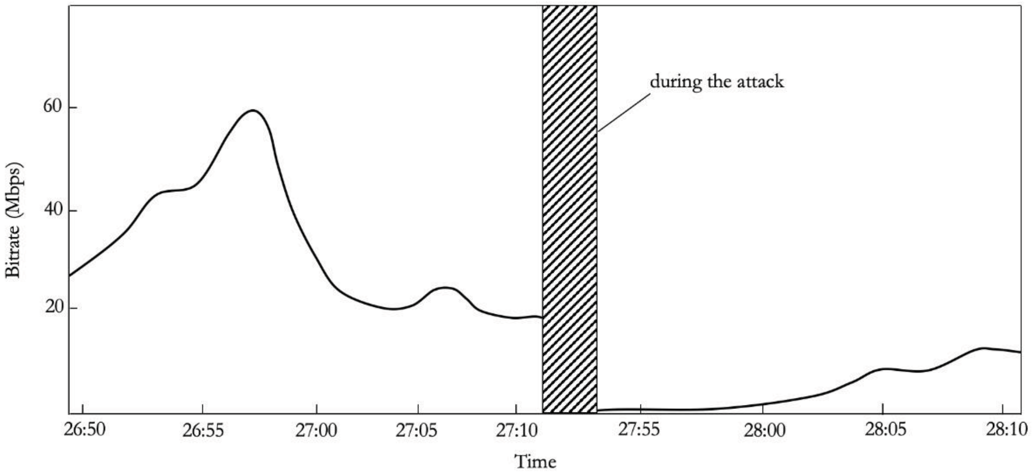

Figure 2. Data transfer during a deauthentication attack

This study allowed us to demonstrate the possible scheme of action of the attacker and the situation of the attack on client. According to the results of the study, based on practical experiments, we can conclude that for wireless clients there is a vulnerability according to which an attacker can implement DoS attack "denial of service", that is, endlessly send packages of deauthentication, which allows to disconnect clients for a long time from the access points to which they are connected.

We believe that current wireless standards require fixes, as the new standards take a long time to deploy.

References

1. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications / IEEE Std 802.11-2007 (Revision of IEEE Std 802.11-1999), 2007. – 1184 p.

2. Mofreh S. A DOS Attack Intrusion Detection and Inhibition Technique for Wireless Computer Networks / S. Mofreh, S. Amany, M. Abu-Bakr // ICGST-CNIR, V. 7, I. 1, 07.2007. – pp. 17-24.

3. Deep J. De-Authentication attack on wireless network 802.11i using Kali Linux / J. Deep, V. V. Dwivedi, K. M. Pattani // IRJET, V. 4, I. 1, 01.2017. – pp. 1666-1669.

Анотація

Досліджено механізм атаки деавтентифікації в мережах на основі стандарту 802.11 та її практична реалізація. Показано, що для бездротових клієнтів існує вразливість, згідно з якою зловмисник може реалізувати DoS-атаку «відмова в обслуговуванні», нескінченно відправляючи пакети деавтентифікації.

Ключові слова: атака, автентифікація, загроза, ін'єкція пакетів, підключення, точка доступу, фрейм, DoS, Linux, Wi-Fi.

Аннотация

Исследован механизм атаки деаутентификации в сетях на основе стандарта 802.11 и ее практическая реализация. Показано, что для беспроводных клиентов существует уязвимость, согласно которой злоумышленник может реализовать DoS-атаку «отказ в обслуживании», бесконечно отправляя пакеты деаутентификации.

Ключевые слова: атака, аутентификация, угроза, инъекция пакетов, подключение, точка доступа, фрейм, DoS, Linux, Wi-Fi.

Abstract

The mechanism of deauthentication attack in networks based on the 802.11 standard and its practical implementation are investigated. It’s shown that there is a vulnerability for wireless clients according to which an attacker could implement a denial of service DoS attack, sending deauthentication packets endlessly.

Keywords: attack, authentication, threat, packet injection, connection, access point, frame, DoS, Linux, Wi-Fi.