Environment. Technology. Resources. Rezekne, Latvia
Proceedings of the 15th International Scientific and Practical Conference. Volume IV, 150-154

Wireless security issues

Kaloyan Kolev
National Military University
Veliko Tarnovo, Bulgaria
kolevkaloqn35@gmail.com

Yordan Shterev
National Military University
Veliko Tarnovo, Bulgaria
jshterev@abv.bg

Abstract. **Wireless home networks, for small organizations, as well as multi-user institutions and public networks need to be secured. This is a topical issue, especially since wireless protocols do not always provide good protection. The article aims to discuss the vulnerabilities and privacy security issues associated with wireless networks. The tools airmon-ng for monitoring, WireShark for snooping, aircrack-ng for dictionary pre-generation and also airodump-ng and aireplay-ng present in Kali Lunix were used. The results of attacks and penetration tests performed on an experimental wireless connection protected with WPA2 show the vulnerability of wireless networks protected with this protocol. Therefore, accelerated implementation of WPA3 protocol is imperative.**

Keywords: attacks, Kali Linux, security issues, wireless networks.

I. INTRODUCTION

Introduction Wireless networks use radio waves to connect devices. These include notebook computers, desktop computers, personal digital assistants (PDAs), cellular phones, pagers, and more. Wireless networks work similarly to wired networks to transmit and receive information. They serve many purposes. In some cases, they are used as an alternative to wired networks, while in others they are used to provide access to corporate and personal data from remote locations. Wireless infrastructure is built at significantly lower costs than wired networks. They provide the local or business community with cheaper and easier access to information. Wireless networks allow remote devices to connect at a certain distance from each other. This makes the use of wireless technology very popular and rapidly spreading [1,2,3,4,5].

Wireless networks are rapidly expanding their capabilities. In addition to this, their bandwidth also increases. Due to their flexibility and freedom, they become an alternative communication infrastructure. Wireless communication provides users with the ability to exchange data at any time, with almost anyone, from anywhere in a communication channel. Because wireless communication and the Internet are compatible, users rely on communication to be secure and accessible. Data that is sent and received over the network is expected to be guaranteed to:

• authentication (sender and recipient are who they say they are);

• confidentiality (the message cannot be understood and read except by the recipient);

• integrity (the message has not been altered in integrity and content) [6].

For small organizations or in home networks, WLAN is a widely preferred solution. It can replace wired LAN and offers many advantages. Apart from them, the disadvantages should also be considered. As such, security can be cited compared to wired networks. It is an aspect that needs to be researched, especially in multi-user and public networks [7].

Improperly secured wireless networks can be used to infiltrate companies, banks, and government organizations. The frequency of these attacks increases due to ignorance and lack of analysis to secure wireless networks in a reliable manner [8,9].

Weaknesses and loopholes of Wi-Fi networks protected with protocols of the 802.11 standard – WPA2-PSK [7, 17, 20, 21] are researched with Kali Lunix tools and computers with a wireless connection. The same protocols are widespread and the advanced WPA3 protocol is not yet widely used. Access to office, institutional and public wireless networks put the mobile devices in use at risk. Therefore, a similar study was carried out here, but using a computer with a wireless connection for analysis, and two mobile devices were used for users (clients of the network).

This article aims to discuss the vulnerabilities, weaknesses and privacy security issues associated with wireless networks. Separately, the results of attack and penetration tests performed on experimental wireless networks using the Kali Linux distribution are shown and analyzed.

II. WI-FI NETWORKS SAFETY REVIEW

WLAN networks work according to the concept of the Open Systems Interconnection model (OSI model) [10]. Communication takes place through frames (packets), which are a sequence of bits. Each frame has a certain fixed length, which is determined by the type of transmission medium [11]. Each frame consists of a

Print ISSN 1691-5402
Online ISSN 2256-070X
https://doi.org/10.17770/etr2024vol4.8186

header and body and additional data from higher layers of the OSI model. They contain control information related to the recipient. The frames contain a mechanism for checking the integrity of the content during delivery. The recipient checks the integrity of the packet and then sends an acknowledgment of receipt. The frame header structure is shown in Figure 1.

From the header structure, the fields Type, Subtype and Wep are important for security.

The *Type* field specifies three types of WLAN frames:

Management - enable the maintenance of communication, represent the presence of the AP, as well as connecting and disconnecting to it;

Control - allow and facilitate the exchange of data between stations with as little loss as possible;

Data frames – represent the majority of Wi-Fi communication, as payload. They are limited to 2312 bytes in size, so they can be split into fragments. They carry the actual information sent between clients.

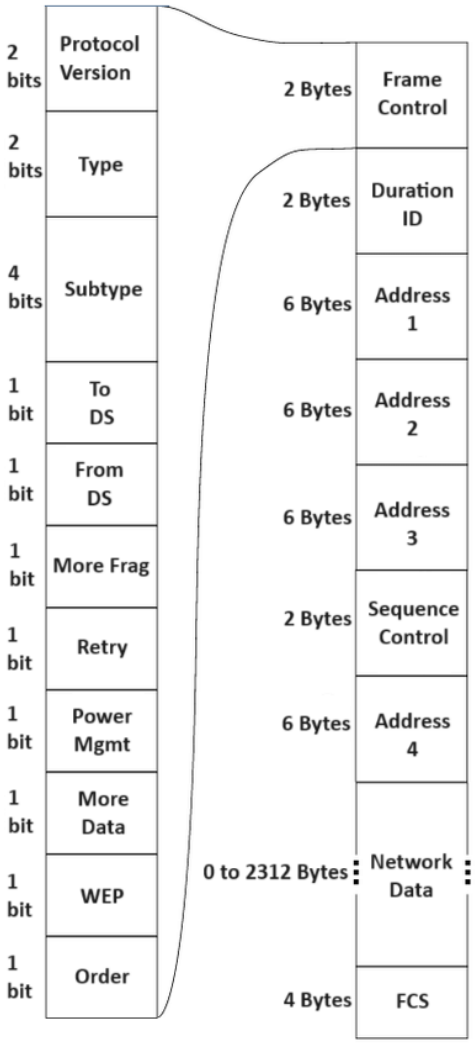

Fig. 1. Frame header structure

Control frames have the following subtypes from the *Subtype* field:

Authentication - sent by the client device as an authentication frame to the AP, contains information about its identity;

Deauthentication – sent by a wireless client that wants to terminate the connection to another client's network;

Association Request - sent by the client, allows the AP to synchronize and allocate resources. It carries information about the wireless connection, data rate and SSID if the AP is accepted, reserves memory and establishes an ID for the device;

Response to the association request – sent by the AP to the client and contains acceptance or rejection information;

Reassociation Request - a device sends a reassociation request when it goes out of range of the currently connected AP and finds another one with a stronger signal. The new AP coordinates the forwarding of any information that may still be contained in the previous AP's buffer;

Reassociation Request Response - sent by the AP, contains the acceptance or rejection of the device's reassociation request.

Disassociation – sent by a device that wants to disconnect. On receipt, the AP relinquishes the memory allocation and removes the device from the association table;

Beacon – sent periodically by the AP to announce its presence and provide the SSID and other pre-configured parameters;

Probe request – sent by a client when information is required from another client;

Probe response – sent by the AP, contains information about capabilities, such as supported data rates, etc. [12].

Control frames have the following subtypes:

Request To Send (RTS);

Clear To Send (CTS);

Acknowledge (ACK) [8].

Encryption is one of the most important tools used to create a secure network.

Most APs offer the option of enabling one of the wireless encryption standards – Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), WPA2 or WPA3 [13].

WEP encrypts traffic using 64- and 128-bit keys. Encryption uses static keys, and every authorized system on the same network receives and exchanges encrypted messages using the same key.

WPA uses the Temporal Key Integrity Protocol (TKIP), which generates a new key for each individual packet. This type of encryption uses a 128-bit key and includes Rivest Cipher 4 (RC4) message integrity checks to determine whether there is interception and changes to data packets.

WPA2 uses the Advanced Encryption Standard (AES). It is more secure than RC4, the encryption standard used in TKIP and WEP. Cipher Block Chaining Message Authentication Code Protocol (CCMP) counter mode is also used to verify the integrity of encrypted packets. WPA2 operates in two modes, personal and enterprise. Private mode or Pre-Shared Key (PSK) relies on a shared key known to both the AP and the client device. Enterprise mode uses the more advanced Extensible Authentication Protocol (EAP) and uses an authentication server and individual credentials for each user or device on the wireless network.

WPA3 adds additional security to Personal and Enterprise modes. It uses individual data encryption. Each data transmission is encrypted with its own unique key. WPA3 uses a 192-bit key for personal mode and a 256-bit key for corporate mode.

In WPA3, AES is implemented using the Simultaneous Authentication of Equals (SAE) protocol, which provides better protection against offline attacks and password spoofing attempts by using stronger cryptographic algorithms and a more secure key exchange method [14].

A service set identifier (SSID) defines or extends a set of services. It is broadcast generally visible to all from an AP or other type of station in beacon packets. It announces and indicates the existence and presence of a network, which is visible to users as a name. The SSID can be customized with a length from zero to 256 bits [15].

Shared Key Authentication (SKA) is possible with the WEP encryption standard. It establishes in advance that the requesting system has knowledge of a shared key required for authentication. The key is delivered over the wireless network via a secure channel that is independent. The user only enters the password for a particular Wi-Fi network [16].

III. MATERIALS and METHODS

A configuration consisting of a HP Pavilion 15.6-inch Laptop PC 15-eh1000 with Kali Linux operating system [17,18,19] equipped with a TP-link Archer T2U Plus AC600 wireless dual-band USB adapter. Samsung S20 mobile phone is used as the AP and Alpha 20 mobile phone is used as the client. The configuration of the AP is as follows: SSID: WirelessLab, Password: 12345679, Band: 2.4GHz, Security: WPA2-Personal, Broadcast channel: 1, MAC address type: Phone MAC and Hidden network: off.

The research was done in two stages with Kali Lunix operating system. The first - checking for the hardware's ability to inject packets and the second - cracking a password on a Wi-Fi experimental network.

The research aims at the first stage to check with the specified hardware the possibility of packet injection.

In the second stage, possible password cracking in the Wi-Fi network is checked. For this purpose, a previously generated dictionary containing possible passwords [8, 17] and the Kali Lunix tools: Wireshark, airodump-ng, aireplay-ng and airmon-ng was used.

IV. RESULTS and DISCUSSION

For scanning and obtaining detailed information from the wireless interface in the form of a list of available APs in our range, the command: iwlist wlan0 s (scanning) is used in the terminal of the Linux distribution (fig. 2).

Wireless network cards have several modes of operation, according to their specific model. Most often, they are used as a managed mode subscriber station. Wireless network eavesdropping and packet injection requires the hardware to operate in monitor mode. In this configuration, it stops transmitting data and, on a pre-set channel, outputs the contents of all observed packets to the operating system.

Fig. 2 Command iwlist in Kali Linux.

To switch to monitor mode, use the airmon-ng tool, which is available in the Kali Linux distribution (fig.3).

Fig. 3 Starting monitor mode of Wi-Fi card with airmon-ng.

Wireshark present in Kali Linux is used to eavesdrop on the wireless packets with the command wireshark [20] in the terminal. Select the used interface - wlan0 and filter packets only from the experimental network (fig. 4).

From the information given by the iwlist command, it is clear that the AP to which packets are injected works at a frequency from Channel 1 (2.412MHz)(fig. 2). For the effect to be possible, the antenna must be configured on the same channel as the AP. This is possible with the command: iwconfig wlan0 channel 1.

Restarting Wireshark and using a filter in the console to capture packets only from the experimental network: wlan.bssid == <MAC>, the name and MAC address of the AP are visible via iwlist.

A filter in the Wireshark console is used to perform an injection test:

```
wlan.fc.type_subtype == 0x08,
```

it outputs only *non-beacon* packets for the experimental network.

The next step is to inject using the *aireplay-ng* tool and the following command in a terminal:

```
aireplay-ng -9 -e WirelessLab -a <MAC> wlan0.
```

Wireshark observes multiple packets that are sent by *aireplay-ng*, and the output in terminal is: Injection is working! (fig. 5).

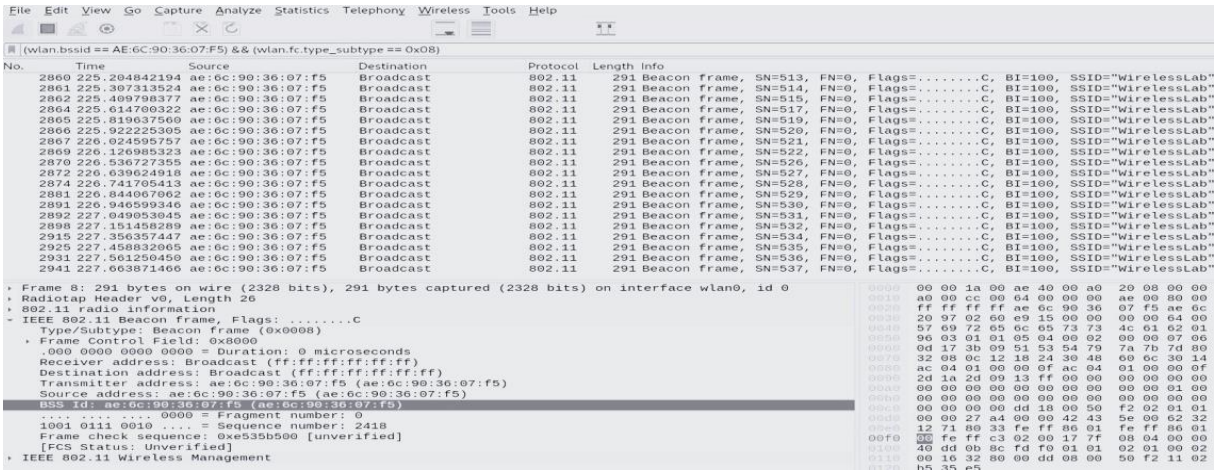

Fig. 4 View in Wireshark Screen in Kali Lunix.

Fig. 5 Injection of packets in experimental Wi-Fi network.

Packet injection is a possibility for many attacks, such as denial of service (DoS), Man-in-the-middle attack (MIMT), as well as sending deauthentication packets, which is necessary when cracking passwords on Wi-Fi networks.

In the second stage, the vulnerability associated with the Pre-Shared Key (PSK) authentication scheme is used to crack the password of the experimental network. It is protected with WPA2 personal.

The password being searched for is PMK- Pairwise Master Key. PSK is a translated 256 bit string from PMK.

WPA2 PSK is created through a four-step data exchange process. In the first step, the AP sends to the client an Authentificator Nonce (ANonce), a random number generated by it. In the second stage, the client returns a Supplicant Nonce (SNonce) along with a Message Integrity Check (MIC). SNonce is a random number generated by the client and MIC is a message integrity code. In the third step, the AP sends the Group Temporal Key (GTK) to the client. It is the same for all network subscribers. In the fourth stage, the client sends data to the AP. They indicate that the key is installed and communication between them continues.

WPA2 PSK works by generating a session key between the AP and the client called a Pairwise Transient Key (PTK). It contains PMK, ANONCE, SNONCE, MAC(AA) and MAC(SA). PSK is used to encrypt all data in the session between the AP and a specific client.

With WireShark in monitor mode, all communication between APs and clients can be viewed [20]. Only the PSK is not known when attempting to crack a password. It is retrieved as a combination provided by the user along with the SSID. It is sent via Password-Based Key Derivation (PBKDF2), which derives the 256-bit shared key.

A pre-generated dictionary of possible passwords is used to crack the password. The attack tool extracts the PSK and uses it in combination with the other parameters in it to create the PTK. It is used to check the MIC in one of the intercepted packets. If the combination of the tested password together with the other data matches, then the assumed password is correct.

The command tool is used to crack the experimental network password:

```
airodump-ng -bssid <MAC> --channel 1
```

write WPACrackDemo1234 wlan0. (fig. 6)

Fig. 6 View of terminal with use of airodump-ng

Airodump-ng displays information about the presence of the four-way *handshake* process and the MAC address of the client that performed it.

Injection sends deauthentication packets to all clients via:

```
aireplay-ng -0 5 0 -a <AP's MAC>.
```

Clients automatically or manually connect to the network. This process generates data.

The data from the four-way handshake process is stored in a file: WPACrackDemo1234.cap. It is used together with a pre-generated dictionary via the aircrack-ng tool with the command [21]:

```
aircrack-ng WPACrackDemo1234.cap -w
/usr/share/wordlists/passwords.lst
```

Various combinations are tried by the method described above. If the password is present in the dictionary, the tool succeeds in cracking it on the experimental network. (fig. 7)

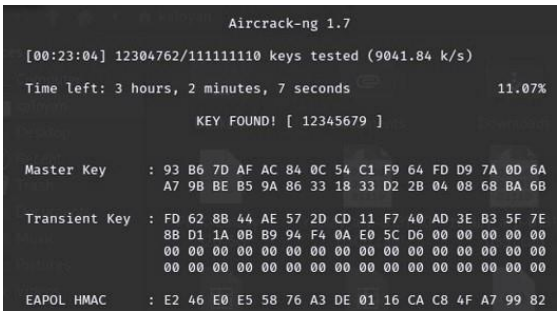

Fig. 7 Result of cracking password with aircrack-ng

CONCLUSIONS

The article reviews key aspects of the information security of Wi-Fi networks - protocols, keys, security fields in the data packet headers. Separately, research has been carried out under Kali Lunix operating system for packet injection and password cracking in a Wi-Fi experimental network. The tools airmon-ng for monitoring, WireShark for snooping, aircrack-ng for dictionary pre-generation and also airodump-ng and aireplay-ng present in Kali Lunix were used.

The research results show that packet injection and password cracking are possible using the Kali Lunix tools used and a pre-generated dictionary. This confirms the weaknesses and gaps in the security of Wi-Fi networks protected with the WPA2-PSK protocols for mobile client devices. It also indicates the need to accelerate the transition to the WPA3 protocol.

Investigations with other tools including the Kali Lunix operating system for Wi-Fi vulnerabilities is a future field of research.

ACKNOWLEDGMENTS:

This report is supported by the National Scientific Program "Security and Defense", approved by Decision No. 171/21.10.2021 of the Council of Ministers of the Republic of Bulgaria.

REFERENCES

[1] Salazar J., Wireless networks., Czech Technical University of Prague.

[2] Mehdi Khosrow, Steve Clarke, Murray E. Jennex, Annie Becker, Ari-Veikko Anttiroiko, Wireless Technologies: Concepts, Methodologies, Tools and Applications, Volume I, Published in the United States of America by Information Science Reference, ISBN 978-1-61350-102-3 (ebook), 2012 by IGI Globa.

[3] Fundamentals of wireless sensor networks Waltenegus Dargie, Christian Poellabauer, ISBN 978-0-470-99765-9, Published by John Wiley & Sons Ltd, 2010.

[4] Ivan Stojmenovic, Handbook of wireless networks and mobile computing, ISBN 0-471-22456-12002, Published by John Wiley & Sons, 2002.

[5] Matthew Gast, 802.11 Wireless Networks The Definitive Guide, Publisher: O'Reilly, ISBN: 0-596-10052-3, April 2005.

[6] Boncella R.J., Wireless Security: An Overview., Washburn University.

[7] Jaiaree T., The security aspects of wireless localarea network (WLAN)., Monterey, California Thesis.

[8] Buchanan C., Ramachandran V., Kali Linux Wireless Penetration Testing Beginner's Guide - Third Edition, Packt Publishing.

[9] Gregory Kipper, Wireless crime and forensic investigation, , Auerbach Publications Taylor & Francis Group, ISBN-10: 0-8493-3188-9, 2007.

[10] [ISO/IEC 7498-1:1994, Information technology Open Systems Interconnection Basic Reference Model: The Basic Model.

[11] Георгиев. В., Вградени и автономни системи. София, Университетско издателство „Св. Климент Охридски“, 2014.

[12] https://www.ii.pwr.edu.pl/~kano/course/module8/8.2.1.4/8.2.1.4.html [Accessed: January, 2024].

[13] https://www.techtarget.com/searchnetworking/feature/Wireless-encryption-basics-Understanding-WEP-WPA-and-WPA2 [Accessed: January, 2024].

[14] https://www.nordvpn.com/blog/wep-vs-wpa-vs-wpa2-vs-wpa3/ [Accessed: January, 2024].

[15] Terry L.; Barber, Simon, eds. (2007), "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications (IEEE Std 802.11-2007).

[16] Rouse M., “Shared Key Authentication”, Technopedia.

[17] https://www.kali.org/ [Accessed: January, 2024].

[18] Ric Messie, Learning Kali Linux, ISBN: 9781492028697, O’Reilly Media, 2018 July.

[19] Sanjib Sinha, Beginning Ethical Hacking with Kali Linux, ISBN-13 (electronic): 978-1-4842-3891-2, 2018.

[20] https://www.wireshark.org/ [Accessed: January, 2024].

[21] https://www.aircrack-ng.org/ [Accessed: January, 2024].