Annals of Spiru Haret University.
Economic Series
Since 2000
ISSN:2393-1795 ISSN-L:2068-6900

Issue 1/2022

# PENETRATION TESTING OF WPA AND WPA2 SECURITY PROTOCOLS AND THE ANALYSIS OF SECURITY SOLUTIONS

**Luka RAJN[1], Nikola PAVLOVIC[2], Šemsudin PLOJOVIĆ[3]**
***[1] Information Technology School, Link Group Belgrade, Serbia,***
***Email: luka55219@its.edu.rs***
***[2] Information Technology School, Link Group Belgrade, Serbia,***
***Email: nikola.pavlovic@its.edu.rs***
***[3] Information Technology School, Link Group Belgrade, Serbia,***
***Email: semsudinplojovic@gmail.com***

**How to cite:** RAJN, L., PAVLOVIC, N., & PLOJOVIĆ, Š. (2022). "Penetration Testing of WPA and WPA2 Security Protocols and the Analysis of Security Solutions." *Annals of Spiru Haret University. Economic Series, 22*(1), 93-110, doi: https://doi.org/10.26458/2214

**Abstract**

*This paper will discuss the security protocols of wireless computer networks. WEP, WPA / WPA2 encryption and the reasons for the existence of such protocols and how they are applied will be explained. The security of WEP and WPA / WPA2 protocols will be tested with practical examples and penetration testing in a secure environment, using Airgeddon and Pixiewps tools. The operating system to be used is ParrotOS.*

**Keywords:** *network security; WPA; WPA2; security protocols; security solutions.*

**JEL Classification:** O30

## Introduction

The growth and development of information technologies have contributed to the fact that technologies have become easy to use at people's fingertips.

Nowadays, many devices facilitate human needs daily. Amongst these numerous devices, the most common are mobile phones; rarely anyone can function without them. As well laptops and personal computers are used every day in developed countries. Furthermore, Internet is being used in everyday business, and in addition to wired networks, quick adoption has been seen with wireless networks to the Internet. With the rapid development of these technologies, there has been a need to implement security protocols and adequate protection to ensure data integrity and protect against malicious attacks.

Given that the Internet is being used in every form of e-business and increasingly wirelessly, the data must be securely transmitted and preserved its integrity. Unfortunately, attackers became interested in wireless networks precisely because of the possibility of abuse and exploitation, and they began to develop techniques to exploit these security protocols. As a result, the security of all wireless technology users has become endangered. Various types of attacks on wireless computer networks are happening every day all over the world. Security protocols evolve, but not all users can keep up with the latest trends, and most users do not think much about security until their data is compromised. This paper discusses the testing of WPA and WPA2 security protocols and the analysis of security solutions.

## 1. WPA и WPA2 (wifi Protected Access)

WPA and WPA2 are new protocols, successors of WEP [6]. These new problems brought solutions to many problems that WEP brought, although WPA had some deficiencies initially. From the very creation of the WPA protocol, the WPA2 was being developed, which was much more complex and secure. A new security infrastructure was being tested, which was the latest standard in the field of security of wireless computer networks and brought many changes in function and authentication of users with access points and changes in data encryption. WPA2 is to this day the most widespread standard proven to be reliable in practice. However, new threats have emerged that have led to further improvements. Although they seemed perfect at first glance, both WPA and WPA2 have some weaknesses that put users at risk.

### 1.1 History and functionality of WPA

WPA standard became available in 2003, and it was supposed to replace the WPA security protocol [6]. This protocol was implemented within the existing infrastructure and could be downloaded as an access point update. Unfortunately, most devices older than 2003 could not get this type of update, and users who had older devices were advised to switch to newer devices with the latest security updates.

WPA implements most IEEE 802.11i standards [6]. In addition, the Temporal Key Integrity Protocol, better known as TKIP, has been adopted [6]. This standard introduced packet-by-packet, a method that dynamically generates a 128-bit key for each packet released to the network and thus protects the access point from all known attacks on the WEP protocol [6].

TKIP is a security protocol used in the 802.11 standards [6]. It was designed by a group working on the 802.11i standard, a group of people put together by the wifi alliance. As the wifi Alliance is committed to spreading, promoting and certifying wifi products, they have organized a team of people who will be in charge of the security of these wireless computer networks.

TKIP and the latest WPA standard introduce three new security measures to protect wireless computer networks [6]. The first security measure is implementing a key mixing function that combines a secret root key with an initialization vector before sending it in RC4 [6]. Another security measure is the implementation of a sequence counter, which protects the network from repetitive attacks. This access point rejects all packets that are not sent in an adequate order. The third security measure is the implementation of a 64-bit data integrity check (better known as MIC - Message Integrity Check) [6]. TKIP uses similar mechanisms as WEP and is therefore vulnerable to similar attacks to which WEP is vulnerable. Message integrity checking, packet hashing, broadcast key rotation, and sequence counter are mechanisms that deter attackers' most known attacks. The key shuffle function also disables an attack in which a WEP key is obtained. Even with this implementation of the latest security measures, new attack vectors to breach networks have opened up, targeting even more specific weaknesses than the previous ones [6].

### 1.2 WPA2

Shortly after the usage of WPA, just a year later, WPA2 was also released. It was brought firstly certification by the wifi alliance and then a major innovation in encryption. Elements from the IEEE 802.11i standard have dominated this protocol [6]. Specifically, this standard introduced CCMP (Counter Mode Cipher Block Chaining Message Authentication Code Protocol), a version of the AES encryption mode [6]. Certification of this protocol began in September 2004. As of March 13, 2006, WPA2 becomes necessary for devices to carry the original wifi tag. Until 2018, this system was the only set of security measures of wireless computer networks that have proven to be a good and reliable mechanism of security [6].

The CCMP was essentially designed to finally solve all those WEP encryption problems that were not solvable. It is an improved cryptographic data encapsulation mechanism designed for confidentiality and is based on the CCM mode of AES [6].

AES (Advanced Encryption Standard), also known as Rijnadael, is a type of electronic data encryption provided by NIST (National Institute of Standards and Technology) [6]. This encryption standard is a subset of Rijnadael block cyphers developed by Vincent Rimien and Joan Daemen [6]. They sent this standard to the NIST while selecting a new successor to the DES symmetric algorithm. Rijnadael is essentially a family of cyphers with different keys and blocks dimensions [6]. For the AES algorithm, NIST selected three members of the cypher family, where each block size is 128 bits but with three different key lengths. Thus, the key lengths were 128, 192, and 256 bits.

What is very important for AES is that this is a very secure algorithm for data encryption and is also very popular and widespread in the world. AES also became the official standard for the U.S. federal government on May 26, 2002, which shows how secure this system is. It is also a part of the ISO / IEC 18033-3 standard [6].

### 1.3 System weaknesses

There are two very significant weaknesses in WPA / WPA2 systems that could compromise the security of wireless networks [6]. Moreover, new methods are emerging every day by which hackers try to compromise their security. The two main attack vectorswe will discuss are the WPS pin recovery and the dictionary attack methods.

WPS (wifi Protected Setup) is a part of the WPA / WPA2 system where it is easier to connect various devices, most often a printer with one click on the device [6]. When this option is turned on on the router, a button on the printer is pressed while the printer connects to the router. The problem with this system is that this pin contains only eight numbers. This is not safe because eight numbers are a small set, and therefore, the device is being exposed to brute force attacks [6]. Most devices have this option enabled in advance, and if the default pin is not changed during the router configuration, the attacker can find out very quickly which pin it is and thus authenticate to the access point.

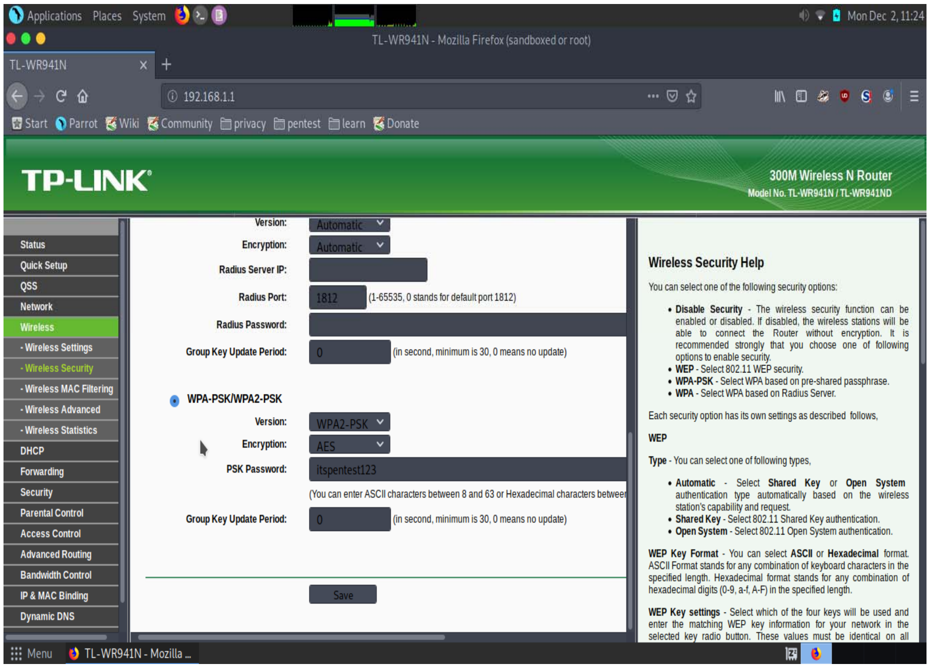
The problem with the dictionary-attack method is that the user provides sensitive data during the first authentication when handling the access point. Therefore, for an attacker to attack with a brute force attack, it is necessary to capture the information that contains this handling and authentication process. Therefore, the attacker usually performs the first attack by which he "removes" (*deauthorizes*) the user from the network and automatically waits for his new authentication. When this is done, he (*attacker)* saves the captured informationon a file on the computer. Since this file is encrypted, the only way to find the password is to compare the captured information (*hash*) with the existing information *(hash)*. Therefore we use a dictionary [6]. Even sites on the Internet have supercomputers that have huge lists of dictionaries that can compare a file that a user uploads to with their dictionaries. Once a match is found, the user has a password and can access the network.

### 1.4 A practical example of an attack on WPA / WPA2

The attack will be performed on the same router model with different settings. This time we will use WPA2-PSK for the security protocol, and the encryption will be AES. The WPA2 security protocol is the most widely used globally, and the highly used TP-Link router provides a very realistic overview of attacks on this security protocol. Figure 1 shows the router configuration settings. Enter the password "itspentest123" in the PSK Password field, which should be "broken" by a dictionary attack (Figure 1).

Before an attack is carried out, it is necessary to make an adequate dictionary for brute force. For the purposes of this paper, a dictionary was made, which is very short and contains only a few words, for the purposes of testing. Dictionaries can be generated independently, but also through tools like Crunch and some other online tools. As mentioned earlier, dictionaries are the size of a few terabytes of text on the Internet, which contain all the most common passwords and are collected and stored in a single file. These dictionaries are very dangerous and most likely contain most of the codes of wireless computer networks because users do not pay enough attention when setting up their routers. A slightly more difficult circumstance for breaking the password with this attack in the Republic of Serbia is that Serbian is different from English. Most citizens of the Republic of Serbia will not use foreign vocabulary to form their passwords. This can be useful, but there is still a risk of someone using this attack. The dictionary used in this attack contained the words: 12345678; 34567890; port1234; and123TS; itsjenajbolji;

pentest123; admin123; password; username; document; code1234; car12345; luka1234; luka9700; itspentest123. All passwords were at least eight characters long because WPA has a requirement of a minimum of 8 characters.



Version: Automatic
Encryption: Automatic
Radius Server IP:
Radius Port: 1812 (1-65535, 0 stands for default port 1812)
Radius Password:
Group Key Update Period: 0 (in second, minimum is 30, 0 means no update)

● WPA-PSK/WPA2-PSK
Version: WPA2-PSK
Encryption: AES
PSK Password: itspentest123
(You can enter ASCII characters between 8 and 63 or Hexadecimal characters betwee
Group Key Update Period: 0 (in second, minimum is 30, 0 means no update)

Wireless Security Help

You can select one of the following security options:

- **Disable Security** - The wireless security function can be enabled or disabled. If disabled, the wireless stations will be able to connect the Router without encryption. It is recommended strongly that you choose one of following options to enable security.
- **WEP** - Select 802.11 WEP security.
- **WPA-PSK** - Select WPA based on pre-shared passphrase.
- **WPA** - Select WPA based on Radius Server.

Each security option has its own settings as described follows,

**WEP**

**Type** - You can select one of following types,

- **Automatic** - Select **Shared Key** or **Open System** authentication type automatically based on the wireless station's capability and request.
- **Shared Key** - Select 802.11 Shared Key authentication.
- **Open System** - Select 802.11 Open System authentication.

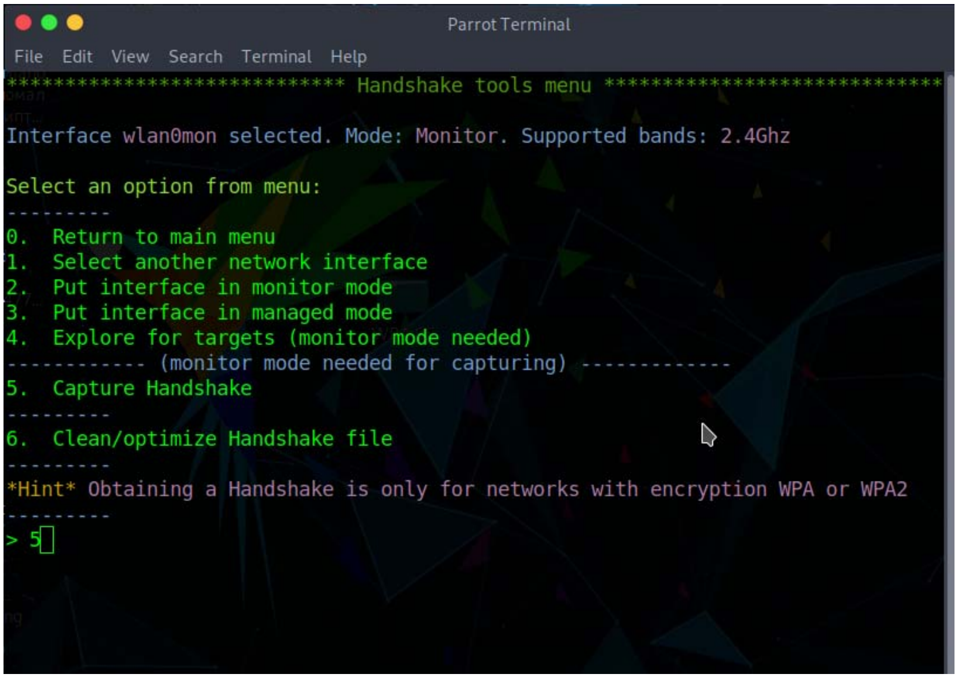
**WEP Key Format** - You can select **ASCII** or **Hexadecimal** format. ASCII Format stands for any combination of keyboard characters in the specified length. Hexadecimal format stands for any combination of hexadecimal digits (0-9, a-f, A-F) in the specified length.

**WEP Key settings** - Select which of the four keys will be used and enter the matching WEP key information for your network in the selected key radio button. These values must be identical on all

**Figure 1. Setting up WPA2 in the Wireless Network Configuration Interface**

After the dictionary is created, following the same procedure as in the previous practical example, we use the airgeddon tool, and the wifi card is switched to monitoring mode. After that, we select option number 5, i.e. the **Handshake tools menu**, where we find options for capturing the handshake packet. Using this option, it is possible to perform reconnaissance; we wait for any user to connect to the access point. If the user connects at eavesdropping, it is possible to successfully capture and save the encrypted handshake packet. What is an aggravating circumstance is just waiting for a user to connect to the network. What can speed this up by a deauthentication attack that will temporarily block the user from the network, and then the attacker will wait for the user to reconnect to the access point.

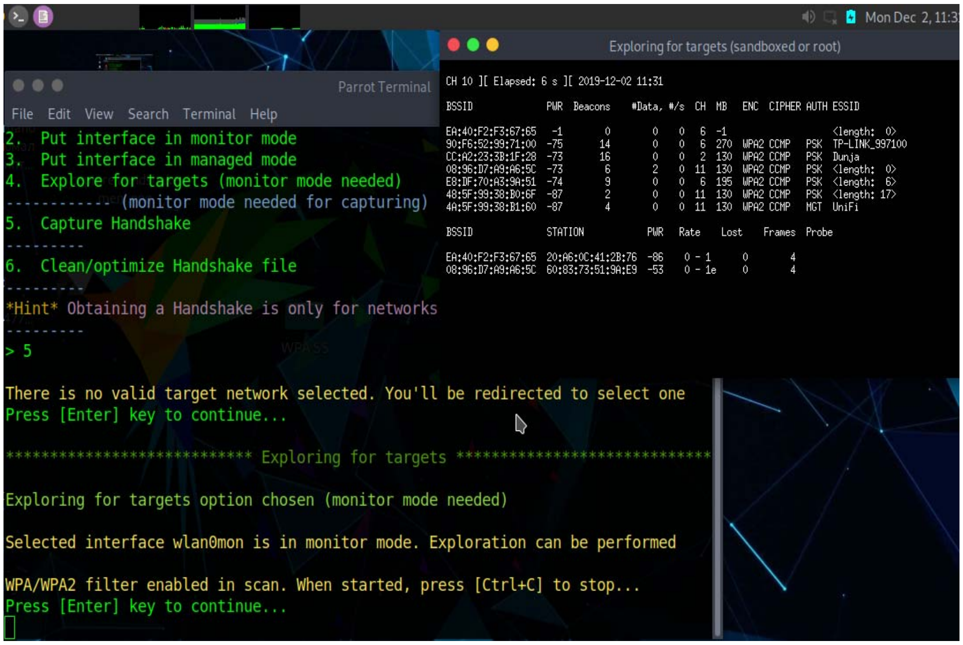
The “**capture handshake**" menu opens, and we select option number 5. Figure 2 shows that options 5 and 6 are the only options in the submenu. This option is logical since it is necessary to "catch the handshake" to carry out an attack. Option 6 is used to clean or optimize the captured file. This option will not be required to show a practical attack using this method.



```
**************************** Handshake tools 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 capturing) -------------
5.  Capture Handshake
---------
6.  Clean/optimize Handshake file
---------
*Hint* Obtaining a Handshake is only for networks with encryption WPA or WPA2
---------
> 5
```

**Figure 2. Display option 5 for "handshake capture."**

After that, we start in monitoring mode and capture packets of all networks in the vicinity. There are many networks in the scope, and we need to single out the network on which we will make the testing/attack. It is noticeable that some hidden networks can be seen, proving that it is possible to see the networks that should be hidden using monitoring mode. What is not known about these networks is their name, but the unique MAC address of the router can be seen. The menu also shows that only WPA2 networks are shown, which practically proves that this is the most widespread security protocol used today. Since we are working with a pre-configured router for practical testing of this network, long-term scanning of the surrounding networks is unnecessary. The router, which needs to be singled out here, is visible and does not have a hidden name; there is only one router named TP-LINK_997100 in the network range. The tool will automatically recognize networks and devices connected to the network, as seen in Figure 3.


Mon Dec 2, 11:3
Parrot Terminal
File Edit View Search Terminal Help
Exploring for targets (sandboxed or root)

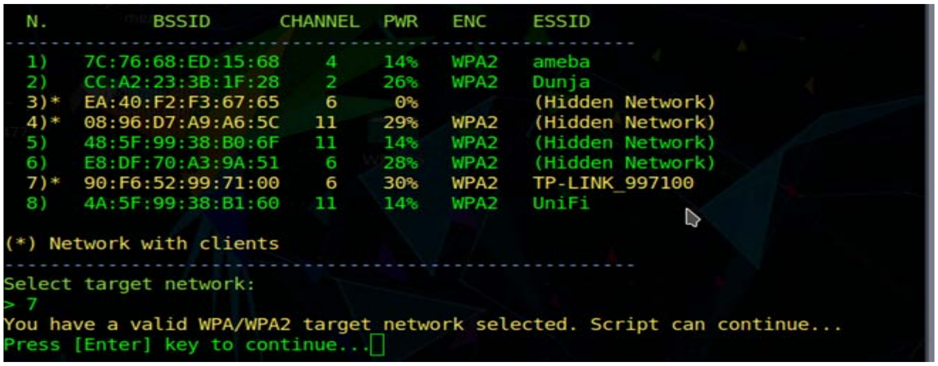
```
2.  Put interface in monitor mode
3.  Put interface in managed mode
4.  Explore for targets (monitor mode needed)
------------ (monitor mode needed for capturing)
5.  Capture Handshake
---------
6.  Clean/optimize Handshake file
---------
*Hint* Obtaining a Handshake is only for networks
---------
> 5

There is no valid target network selected. You'll be redirected to select one
Press [Enter] key to continue...

*************************** Exploring for targets ****************************

Exploring for targets option chosen (monitor mode needed)

Selected interface wlan0mon is in monitor mode. Exploration can be performed

WPA/WPA2 filter enabled in scan. When started, press [Ctrl+C] to stop...
Press [Enter] key to continue...
```

```
CH 10 ][ Elapsed: 6 s ][ 2019-12-02 11:31

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

EA:40:F2:F3:67:65   -1        0        0    0   6  -1                    <length:  0>
90:F6:52:99:71:00  -75       14        0    0   6  270  WPA2 CCMP   PSK  TP-LINK_997100
CC:A2:23:3B:1F:28  -73       16        0    0   2  130  WPA2 CCMP   PSK  Dunja
08:96:D7:A9:A6:5C  -73        6        2    0  11  130  WPA2 CCMP   PSK  <length:  0>
E8:DF:70:A3:9A:51  -74        9        0    0   6  195  WPA2 CCMP   PSK  <length:  6>
48:5F:99:38:B0:6F  -87        2        0    0  11  130  WPA2 CCMP   PSK  <length: 17>
4A:5F:99:38:B1:60  -87        4        0    0  11  130  WPA2 CCMP   MGT  UniFi

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

EA:40:F2:F3:67:65  20:A6:0C:41:2B:76  -86    0 - 1     0        4
08:96:D7:A9:A6:5C  60:83:73:51:9A:E9  -53    0 - 1e    0        4
```

**Figure 3. Finding access points and users on them**

Before launching an attack, it is necessary to choose a target. The data shows that the network required for testing is at number 7. We then select this option. The window also displays the MAC addresses of all other networks in the area. In Figure 4, we can also see four hidden networks with no name (*SSID*[1]).

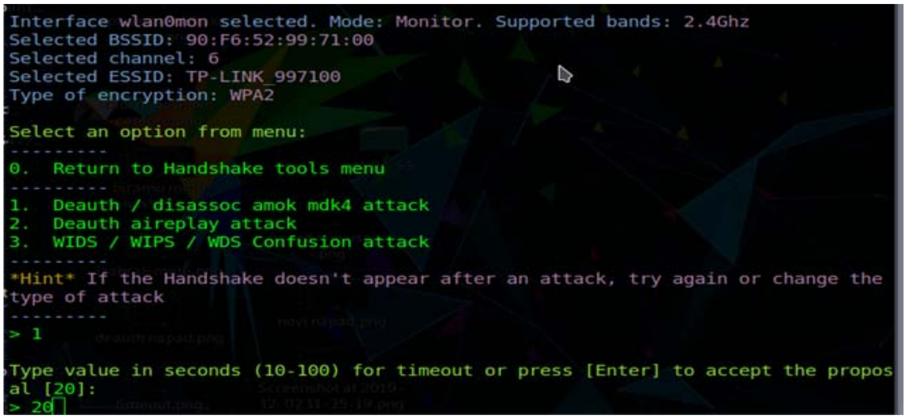
[1] SSID - *service set identifier* - https://en.wikipedia.org/wiki/Service_set_(802.11_network)



```
  N.        BSSID        CHANNEL  PWR   ENC    ESSID
-------------------------------------------------------
  1)   7C:76:68:ED:15:68    4     14%   WPA2   ameba
  2)   CC:A2:23:3B:1F:28    2     26%   WPA2   Dunja
  3)*  EA:40:F2:F3:67:65    6      0%          (Hidden Network)
  4)*  08:96:D7:A9:A6:5C   11     29%   WPA2   (Hidden Network)
  5)   48:5F:99:38:B0:6F   11     14%   WPA2   (Hidden Network)
  6)   E8:DF:70:A3:9A:51    6     28%   WPA2   (Hidden Network)
  7)*  90:F6:52:99:71:00    6     30%   WPA2   TP-LINK_997100
  8)   4A:5F:99:38:B1:60   11     14%   WPA2   UniFi

(*) Network with clients
-------------------------------------------------------
Select target network:
> 7
You have a valid WPA/WPA2 target network selected. Script can continue...
Press [Enter] key to continue...
```

**Figure 4. network interfaces and target selection**

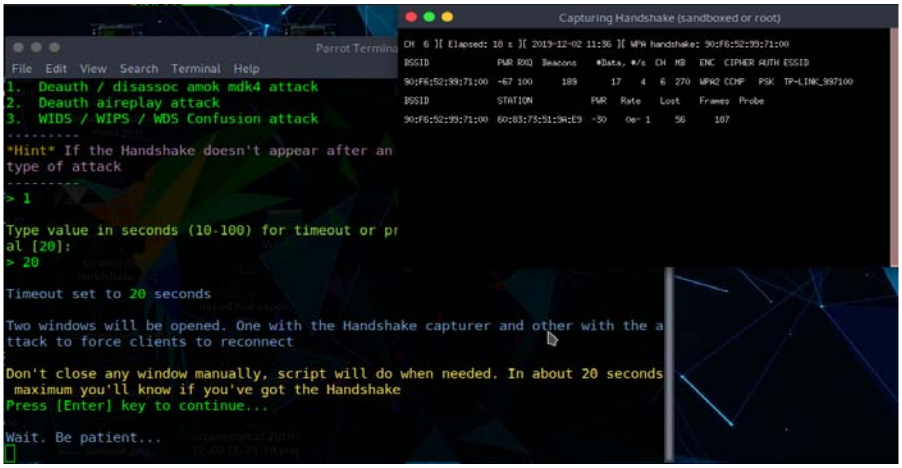
The signal strength is highest on our test network where we perform an attack, proving that the router being tested is the closest physically to the location from which the scan is performed. We can move on as the scan has been successful. The next step is where we select the attack that will compromise the security of the access point.



```
Interface wlan0mon selected. Mode: Monitor. Supported bands: 2.4Ghz
Selected BSSID: 90:F6:52:99:71:00
Selected channel: 6
Selected ESSID: TP-LINK_997100
Type of encryption: WPA2

Select an option from menu:
---------
0.  Return to Handshake tools menu
---------
1.  Deauth / disassoc amok mdk4 attack
2.  Deauth aireplay attack
3.  WIDS / WIPS / WDS Confusion attack
---------
*Hint* If the Handshake doesn't appear after an attack, try again or change the
type of attack
---------
> 1

Type value in seconds (10-100) for timeout or press [Enter] to accept the propos
al [20]:
> 20
```

**Figure 5. User deauthentication options**

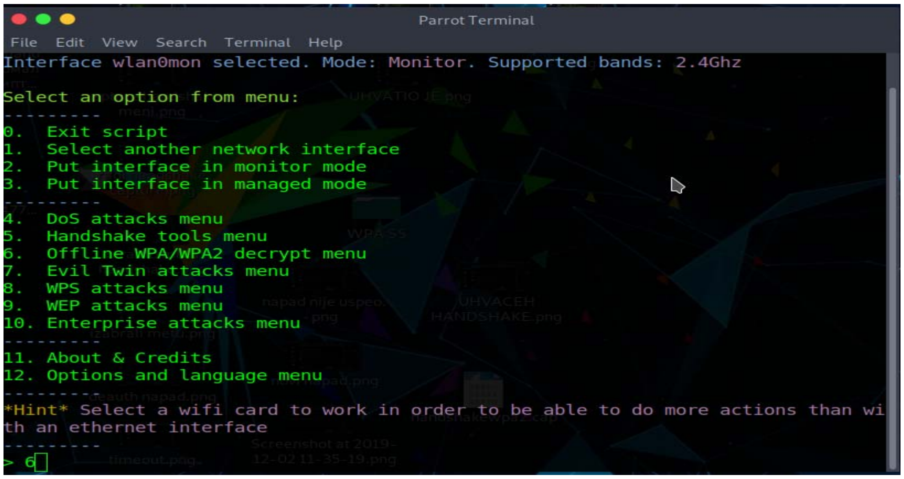
We select the attack that will elicit a handshake between the users and the access point. Figure 18 shows the options for de-authenticationattacks. A mobile phone and its MAC address are connected to the network, and all other data are visible in Figure 5. This file needs to be saved and a brute force attack to be launched.



```
Capturing Handshake (sandboxed or root)

CH  6 ][ Elapsed: 18 s ][ 2019-12-02 11:36 ][ WPA handshake: 90:F6:52:99:71:00

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

90:F6:52:99:71:00  -67 100      189       17    4   6  270  WPA2 CCMP   PSK  TP-LINK_997100

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

90:F6:52:99:71:00  60:83:73:51:9A:E9  -30    0e- 1    56      107
```

```
Parrot Terminal
1.  Deauth / disassoc amok mdk4 attack
2.  Deauth aireplay attack
3.  WIDS / WIPS / WDS Confusion attack
---------
*Hint* If the Handshake doesn't appear after an
type of attack
---------
> 1

Type value in seconds (10-100) for timeout or pr
al [20]:
> 20

Timeout set to 20 seconds

Two windows will be opened. One with the Handshake capturer and other with the a
ttack to force clients to reconnect

Don't close any window manually, script will do when needed. In about 20 seconds
 maximum you'll know if you've got the Handshake
Press [Enter] key to continue...

Wait. Be patient...
```

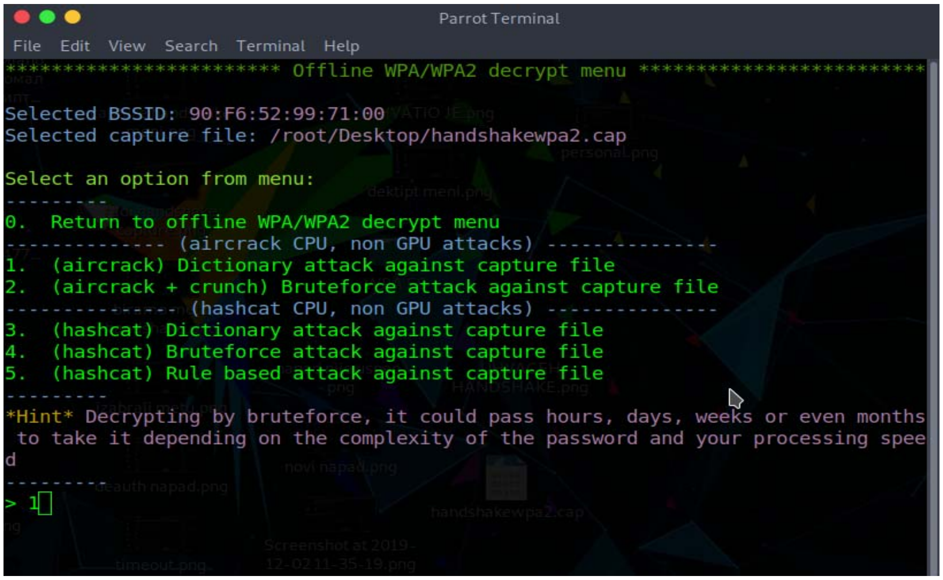
**Figure 6. Re-authentication of users**



```
Parrot Terminal
Interface wlan0mon selected. Mode: Monitor. Supported bands: 2.4Ghz

Select an option from menu:
---------
0.  Exit script
1.  Select another network interface
2.  Put interface in monitor mode
3.  Put interface in managed mode
---------
4.  DoS attacks menu
5.  Handshake tools menu
6.  Offline WPA/WPA2 decrypt menu
7.  Evil Twin attacks menu
8.  WPS attacks menu
9.  WEP attacks menu
10. Enterprise attacks menu
---------
11. About & Credits
12. Options and language menu
---------
*Hint* Select a wifi card to work in order to be able to do more actions than wi
th an ethernet interface
---------
> 6
```

**Figure 7. Option for offline decryption**

It is necessary to open the decryption menu and select offline decryption since the file with handling is saved. Figure 7 shows these options, and Figure 8 shows after this option has already been selected and attacks to decrypt the captured and saved file.

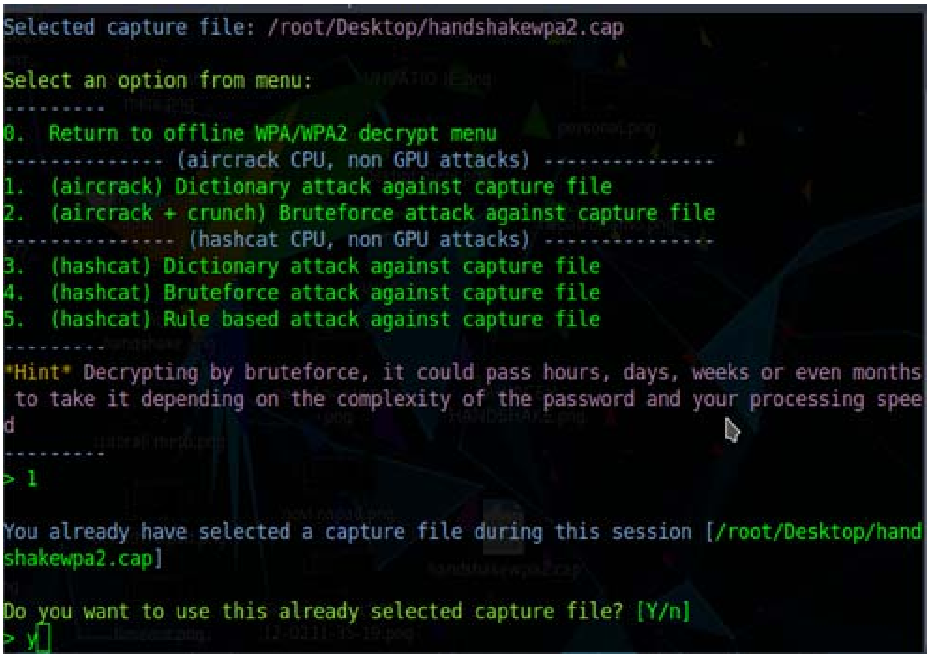


```
************************ Offline WPA/WPA2 decrypt menu ************************

Selected BSSID: 90:F6:52:99:71:00
Selected capture file: /root/Desktop/handshakewpa2.cap

Select an option from menu:
---------
0.  Return to offline WPA/WPA2 decrypt menu
-------------- (aircrack CPU, non GPU attacks) ---------------
1.  (aircrack) Dictionary attack against capture file
2.  (aircrack + crunch) Bruteforce attack against capture file
--------------- (hashcat CPU, non GPU attacks) ---------------
3.  (hashcat) Dictionary attack against capture file
4.  (hashcat) Bruteforce attack against capture file
5.  (hashcat) Rule based attack against capture file
---------
*Hint* Decrypting by bruteforce, it could pass hours, days, weeks or even months
 to take it depending on the complexity of the password and your processing spee
d
---------
> 1
```

**Figure 8. Attack vectors using a dictionary on captured packets**

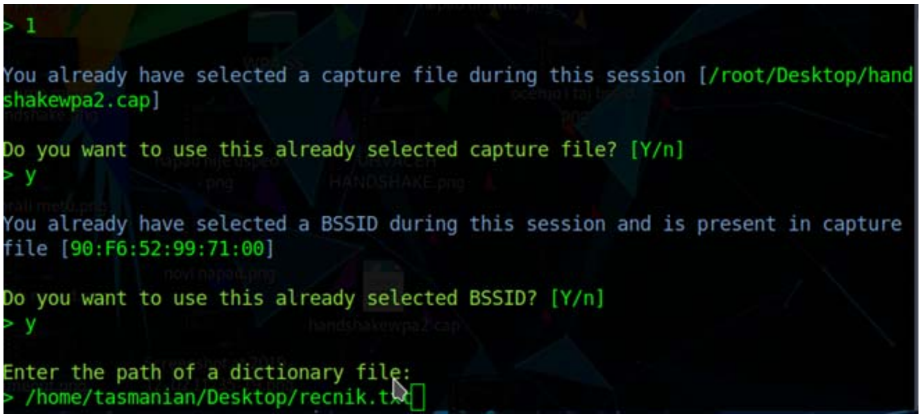
The attack is performed using an arbitrarily created dictionary. Hash values are compared. Since the file is saved, the program offers the option to use that file immediately. The file in which this data is stored is has a .cap extension, and it's the standard extension for captured packets. We select the default option to save and use it, and it’s shown in Figure 9.

The dictionary that will be used for the attack is loaded into the program (Figure 10). The dictionary used in this attack is a dictionary that we generated in a regular .txt file.



```
Selected capture file: /root/Desktop/handshakewpa2.cap

Select an option from menu:
---------
0.  Return to offline WPA/WPA2 decrypt menu
-------------- (aircrack CPU, non GPU attacks) ---------------
1.  (aircrack) Dictionary attack against capture file
2.  (aircrack + crunch) Bruteforce attack against capture file
--------------- (hashcat CPU, non GPU attacks) ---------------
3.  (hashcat) Dictionary attack against capture file
4.  (hashcat) Bruteforce attack against capture file
5.  (hashcat) Rule based attack against capture file
---------
*Hint* Decrypting by bruteforce, it could pass hours, days, weeks or even months
 to take it depending on the complexity of the password and your processing spee
d
---------
> 1

You already have selected a capture file during this session [/root/Desktop/hand
shakewpa2.cap]

Do you want to use this already selected capture file? [Y/n]
> y
```

**Figure 9. File selection options**



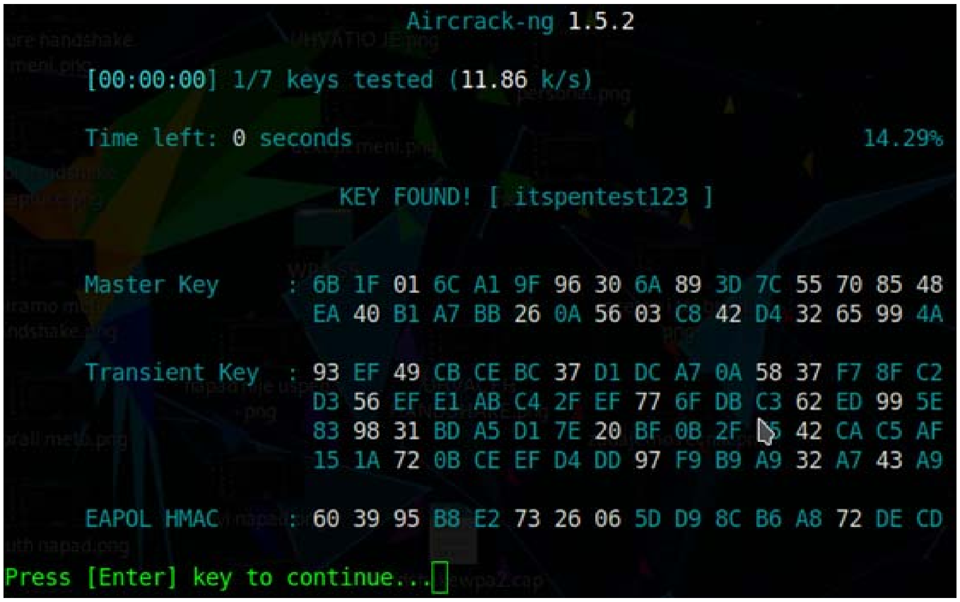
```
> 1

You already have selected a capture file during this session [/root/Desktop/hand
shakewpa2.cap]

Do you want to use this already selected capture file? [Y/n]
> y

You already have selected a BSSID during this session and is present in capture
file [90:F6:52:99:71:00]

Do you want to use this already selected BSSID? [Y/n]
> y

Enter the path of a dictionary file:
> /home/tasmanian/Desktop/recnik.txt
```

**Figure 10. Entering the path of the file with the created dictionary**

The recnik.txt file will be used solely to demonstrate the weaknesses of the WPA2 network protocol and will have no other purpose. When the file path is entered, the program will automatically recognise which data *(hash)* file we captured we need to compare it to. The file path is / home / tasmanian / Desktop / recnik.txt. (Figure 10). After pressing the enter key, decryption is performed.

After a successful attack, it took less than a second to compare the keys and get the result. The password was found successfully, and it is **itspentest123** (Figure 11). After this, the password can be saved in another file or memorized.

This successful attack showed that WPA2 has major shortcomings and that wireless computer networks must be protected from such attacks. WPA2 does not currently provide adequate protection, and this can compromise data integrity. The results can be seen in Figure 24. The attack was successfully performed, and the result obtained is exactly the password set during the route configuration. Figure 11 also shows the keys (*hashes)* that were compared.



```
                    Aircrack-ng 1.5.2

    [00:00:00] 1/7 keys tested (11.86 k/s)

    Time left: 0 seconds                               14.29%

                 KEY FOUND! [ itspentest123 ]


    Master Key     : 6B 1F 01 6C A1 9F 96 30 6A 89 3D 7C 55 70 85 48
                     EA 40 B1 A7 BB 26 0A 56 03 C8 42 D4 32 65 99 4A

    Transient Key  : 93 EF 49 CB CE BC 37 D1 DC A7 0A 58 37 F7 8F C2
                     D3 56 EF E1 AB C4 2F EF 77 6F DB C3 62 ED 99 5E
                     83 98 31 BD A5 D1 7E 20 BF 0B 2F [illegible] 42 CA C5 AF
                     15 1A 72 0B CE EF D4 DD 97 F9 B9 A9 32 A7 43 A9

    EAPOL HMAC     : 60 39 95 B8 E2 73 26 06 5D D9 8C B6 A8 72 DE CD
Press [Enter] key to continue...
```

**Figure 11. Successful WPA decryption**

### 1.5 Solution to a security issue

A specific solution to protect the wireless network from the previously described and performed attack is to set a strong password. When we talk about a strong password, we mean a password that contains a capital letter, a sign, letters and numbers in combination. Since the attack itself is practical because it guesses the words that the user can enter as a password, for security purposes, it is simply better to generate a password that does not have a special meaning and connect numbers, capital letters and characters with it. The problem with these passwords is that they are harder to remember, but they are significantly safer than just a few letters of an ordinary common word. Given that it was previously mentioned that users often choose a word that is close to them, it is very likely that the word will be contained in the dictionary used for the attack. On the other hand, there is the possibility of "capturing" an encrypted key, and with the help of very powerful computers, it is possible to "break" even a hashed key. The attack is made more difficult by more complex codes, which is why this is considered the only solution.

Complex passwords and adequate settings will protect every user from these types of attacks. Also, suppose you do not need to add new users to the network often. In that case, it is possible to include an option on the router where the router will deny access and authentication to any new user, even those that know the password. If the company needs to use a wireless computer network, it is preferred that they be handled by a professional, i.e. a system administrator. For companies, a network system via wired cabling is otherwise recommended, as it is a structured approach that makes it easier for company administrators to do the job.

Wireless computer networks have lower data transfer speeds than networks that use cables, so we should use wired computer networks for better speed and greater reliability. However, using a network via cable is certainly far safer because eavesdropping is, in this case, possible only through a cable attached to the existing network; that is why this type of connection to the networks is best if it is company business. It is best to set a strong password, turn off older encryption systems, and update the network device regularly for individual use. The last option is to upgrade is to use the latest WPA3 protocol, which significantly improves the encryption of all data.

### 2. WPA3 and the future of network protection

WPA3 is the latest security protocol that appeared in January 2018. [7] The wifi alliance identified it as the official deputy for WPA2. It is not yet globally applicable, but some manufacturers have already started making routers with this type of encryption. Some manufacturers are working on releasing new updates for older devices that can use this new protocol.

Given that technology is evolving at high speed, it is noticeable that security protocols are also evolving at high speed. Problems that arise with newer technologies should be adequately remedied, and newer types of data protection should be introduced. The fact is that some new types of attacks appear every day, which seriously endangers the safety of users. For example, the KRACK attack on the WPA2 network is now well known [9]. Exposure to this attack also led to the immediate release of a new technology that should completely replace WPA2. The KRACK attack is a highly destructive recurrence attack on the WPA2 network discovered in 2016 by Belgian researchers Mattie Vanhoeff and Frank Piesens [9]. They demonstrated this attack at the University of Leuven. The group that discovered this attack published the details in October 2017. The weakness in this system comes from the wifi standard itself, not from the way the product works or because of the implementation [9]. This contributes to the fact that any correct implementation of WPA is incorrect because it can eavesdrop on such a network due to a bad version of the standard itself. This eavesdropping attack is feasible on all operating systems, and it is currently impossible to regulate this problem with this standard. That's why the wifi alliance started making a WPA3 security protocol before this attack was eased, so in practice, it could endanger a potentially huge number of users.

### 2.1 Functionality of WPA3

The new WPA3 standard, like the previous one, has two modes: WPA3 Personal and WPA3 Enterprise. However, WPA3 Personal uses AES-128 in CCM mode while WPA3 Enterprise comes with an additional AES-256 in GCM mode and SHA-384 as HMAC data encryption [7]. This type of encryption is the most modern standard in the field of cryptography. In addition, this system guarantees confidentiality, so that session keys will not be compromised even when the server key is compromised. The wifi Alliance also states that this protocol will address security issues with weak passwords and make it easier to configure devices without a display interface [7].

Due to advanced secrecy, this standard allows the establishment of an individualized network in the sense that even when someone has a wireless network code, they will not be able to eavesdrop on other people's traffic. Advanced privacy will be enabled by wifi Enhanced Open technology, allowing users maximum privacy [7]. In addition, this network will be open, which means that no password will be required to access the data. This feature, in itself, can bring quite widespread use, but there are already potential drawbacks associated with this particular mode of operation.

The latest technology that should replace the already known WPS is wifi Easy Connect, which enables easier connection of devices that do not have an interface and many other devices. This will make it much easier to connect to IoT devices and significantly improve their functions. Furthermore, when installing WPA3, it will be possible to scan the QR code for easier connection to a secure computer network [7]. These options represent new aspects in security and will certainly be of great importance to users.

### 2.2 New problems in the latest technology

As WPA3 technology emerged very soon after the successfully demonstrated attack on the WPA2 protocol, it was noticeable that it came on the market rapidly. Unfortunately, when it comes to technology and security, this is not the best practice because attacks can occur at an early stage of implementation, and errors in the system can be easily found in the system that is not well developed [8]. Therefore, good and advanced systems are developed over a longer period. Although the real situation is that WPA2 is already quite outdated, as it has been on the market for more than fourteen years, it is still in use, as many updates have been made, in the meantime, that have fixed the problems that existed.

The biggest threat under the WPA3 protocol is an attack called Dragonblood. This threat can cause downsizing attacks, side-channel attacks, brute force password passwords, and DOS access point attacks. Mattie Vanhoeff discovered these attacks from the New York University in Abu Dhabi and Eyal Ronen from the University of Leuven. Their scientific work explained these attacks and a theoretical review of the shortcomings in the latest protocol [8].

The big danger comes from the wifi Enhanced Open mode in which WPA3 works. This mode should instil confidence in users that the use of public open networks is now really safe. However, in practice, this does not work best. This type of connection is limited because it still does not solve the problem of fake access points. Attackers can create a fake network with the same name, such as the latest WPA3 protected network, and by an already known method can lead users to their fake access point. Suppose users are not connected to the access point used by the attacker. In that case, the attacker will simply "download" those users from the access point with de-authentication attacks, and the users will automatically connect to a malicious network. It is concluded that the security of the public network is very debatable, so users must be careful how they approach this idea. The attackers will surely try to use the latest and most diverse methods to determine how they will further violate the integrity of this latest technology.[10]

It has been a while since WPA3 appeared, and several theoretical attacks have already emerged that threaten to virtually compromise the security of wireless computer networks. This could potentially lead to discoveries and may change the way we look at wireless technology today.

## Conclusion

The future of wireless computer networks will face major changes, as has been the case before. Wireless frequencies must achieve a high level of reliability to make average use and e-commerce safer. In addition, the rapid development of information technologies has also led to rapid development in wireless computer network security. As a result, they can expect numerous changes at the same level, as is the case in all other areas of information technology.

What is important for all users is to follow the trends and take advantage of every new technology available with the latest standards. What is outdated should be replaced, and what is a newer trend should be carefully studied and only then used. When it comes to security, the fact is that no security system can ever be said to be perfect and impenetrable, and even in this area of security protocols, on the examples of attacks, it can be seen that they are not completely safe. Therefore, it is up to the users to decide how they will use these technologies, how careful they will be, and how they will protect themselves from the malicious actions of individuals or groups.

The security of wireless computer networks is compromised, and you should think about it more often. To approach these problems, first of all, you need to be aware that this problem always exists, and only then should you use the knowledge gained by following new trends. The security protocols of computer networks have never been more diverse. However, the great development and availability of information technologies have led to their integrity being compromised. This topic could be very interesting in the future because there is great potential for improving knowledge in this area. Many types of different attacks occur from day to day, and therefore it would be good to perform practical tests as much as possible. Also, there is potential to test WPA3 in the future, and it will surely be realized very soon.

## References

[1] Beaver K., Davis P.,Hacking wireless networks for dummies, Indianapolis, Wiley Publishing 2005.

[2] Jevremović S., Bezbednost elektronskog poslovanja, Beograd, ITS, 2015.

[3] Jevremović S.,Sigurnost i zaštita informacionih sistema, ITS, 2015.

[4] Macaulay T., Hardening IEEE 802.11 wireless networks, Canada, EWA, 2002.

[5] Monte M., Network attacks and exploitation, Indianapolis, John Wiley & Sons Inc., 2015

[6] Osterhage W., Wireless network security, Frankfurt, Goethe-Universität, 2018

[7] Wifi certified WPA3, https://www.wi-fi.org/discover-wi-fi/security (visited on28.11.2020)

[8] Dragonblood: Analyzing the DragonflyHandshake of WPA3 and EAP-pwd, https://eprint.iacr.org/2019/383.pdf (visited on04.12.2020)

[9] Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2, https://papers.mathyvanhoef.com/ccs2017.pdf (visited on02.12.2020)

[10] Saračević M., Selimi A., Plojović Š., Some Specific Examples of Attacks on Information Systems and Smart Cities Applications, in Book: Cybersecurity and Secure Information Systems, Springer Nature Switzerland AG, 2019.