AN ANALYSIS OF WIRELESS NETWORK SECURITY IN THE CITY OF ZAGREB AND THE ZAGREB AND KARLOVAC COUNTIES

Davor Janić
Ministry of Defense, Sarajevska 7, Zagreb, Croatia, davor.janic@morh.hr
Dr. sc. Dragan Peraković
Faculty of Transport and Traffic Sciences, Vukelićeva 4, Zagreb, Croatia, dragan.perakovic@fpz.hr
Vladimir Remenar
Faculty of Transport and Traffic Sciences, Vukelićeva 4, Zagreb, Croatia, vladimir.remenar@fpz.hr

ABSTRACT
Wireless LAN has become widely used in recent years, in business as well as household, educational and other settings. Since the onset of wireless communication its popularity has been on the rise. Users opt for it primarily because of its ease of use, i.e. the fact that it does not require physical cables. The most sensitive issue arising in connection with wireless network use is security.. If the wireless network has no adequate protection system, any computer within range may access the network. Potential attackers may use malignant software for unauthorised access to the network and misuse it in a variety of ways. The most important form of protection lies in encryption methods for wireless networks. Initially developed in 1999 as a method of protection for wireless networks based on the 802.11 standard, WEP has proved vulnerable in several ways and has not been considered an adequate solution for a number of years. Attempts to address the inadequacies of WEP led to the development of more advanced encryption methods such as WPA and WPA2 in 2004. These, in combination with adequate security settings, constitute an efficient and practically unavoidable form of protection in terms of wireless traffic security. However, despite these facts regarding the reliability of wireless network protection, research results indicate a disappointingly high proportion of wireless networks using inadequate protection. Research on the use of protection methods was carried out in the middle of 2012.

KEYWORDS
WEP, WPA, WPA2, Wi-Fi, WLAN, security

ANALIZA SIGURNOSTI BEŽIČNIH RAČUNALNIH MREŽA NA PODRUČJU GRADA ZAGREBA, ZAGREBAČKE I KARLOVAČKE ŽUPANIJE

ABSTRACT
Bežični LAN je posljednjih godina postao široko rasprostranjen kako u poslovnim sredinama tako i u domaćinstvima, školstvu itd. Otkada se pojavila mogućnost bežične komunikacije njezina popularnost ne prestaje rasti. Korisnici je prije svega odabiru zbog jednostavnosti upotrebe koja ne zahtijeva uspostavljanje žičnih veza. Najosjetljiviji pitanje prilikom korištenja bežičnih računalnih mreža je sigurnost. Ukoliko bežična mreža nema adekvatan sustav zaštite, na mrežu se može spojiti svako računalo koje je u njezinom dosegu. Potencijalni napadač može korištenjem zlođudnih programa ostvariti neovlašten pristup mreži, te ga zlorabiti na mnogo načina. Najvažniji vid zaštite predstavljaju enkripcijske metode zaštite bežičnih mreža. Prvotno razvijen WEP 1999. godine, kao metoda zaštite bežičnih mreža temeljenih na standardu 802.11 dokazano je da je ranjiv na mnoge načine, te ne predstavlja adekvatno rješenje već duži niz godina. Uslijed uočenih propusta WEP-a, 2004. godine razvijene su naprednije enkripcijske metode kao WPA i WPA2, koje uz adekvatne sigurnosne postavke predstavljaju učinkovitu, gotovo nezaobilaznu sigurnosnu mjeru u smislu sigurnosti bežičnog prometa. Međutim, usprkos navedenim činjenicama vezano za pouzdanost zaštite bežičnih mreža, rezultati istraživanja primjene zaštitnih metoda dobiveni istraživanjem sredinom 2012. godine ukazuju na poražavajuće visok udio neadekvatno zaštićenih bežičnih mreža.

KEYWORDS
WEP, WPA, WPA2, Wi-Fi, WLAN, sigurnost

1. WIRELESS NETWORK PROTECTION METHODS.

There are several wireless network protection methods. Less secure methods for protection against unauthorised network access include static IP address filtering, MAC address filtering and SSID hiding, as well as limiting signal range or routing the access point signal. However, these methods are relatively easy to circumvent. More efficient wireless network protection is achieved by using specially formulated authentication and encryption protocols such as Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA).

The idea behind introducing WEP in 1999, while developing the 802.11 standard, was to provide wireless communication with the same level of protection that wired networks had. It was thought that this may be achieved by encrypting communication and authenticating wireless network access. However, as early as 2001, the WEP algorithm was seen to be vulnerable. Nowadays, mere minutes are necessary to bypass WEP security with the aid of publicly available tools and computers with average specifications. In due course, WEP was replaced in 2004 by the new WPA standard, two versions of which were developed (WPA and WPA2), and two forms of authentication, Pre-shared Key (PSK) and Radius.

2. ENCRYPTION METHODS OF WIRELESS NETWORK PROTECTION

WEP protection is used at the physical and data layers of the OSI model in a computer network, and is based on the encryption of data between end points. The WEP algorithm is symmetrical and uses standard 64-bit, 128-bit and 256-bit cryptographic keys. The same key is used to encrypt and decrypt data. The original data packet is processed so that the data are encrypted and protected from unauthorised modification. Although this is not defined by the 802.11 standard, prevention of unauthorised access is also considered to be a feature of WEP. The encryption process begins when the secret 40-bit key (in case of 64-bit encryption) combines with a 24-bit initialisation vector (IV), which results in a 64-bit key. In the case of 128-bit WEP keys, a 24-bit IV is added to a 104-bit key in order to get a 128-bit RC4 key. The primary purpose of IV's is to use a different key for the encryption of each packet which travels through the network. A 64-bit key is used by the Pseudo-random Number Generator (PRNG) to generate a sequence of random numbers which constitute the encryption key or keystream, based on the entry key. Encryption is achieved when the XOR operation is performed on the generated number sequence and entry data. Protection from unauthorised data modification is performed on the original data packet using an integrity algorithm (CRC-32), which results in an ICV. The ICV does not ensure message integrity in the cryptographic sense; it is merely an additional protection measure from incidental data modification during transport. The ICV is appended to the end of the useful content of the data packet in question. The WEP decryption process is encryption in reverse. The encrypted text is matched to the keystream using the XOR algorithm in order to recover the original text. Message authenticity is checked by performing an integrity algorithm on the received message and comparing the ICV2 with the ICV1.

The insecurity of the WEP standard is primarily a result of the vulnerability of the authentication process when a shared key is used. The authentication process is initiated when the client computer sends an authentication frame to the access point. The Access Point (AP) then responds by sending an authentication frame containing 128 octets of random text. In the third step, the station which has initiated the connection copies the text it has received into the authentication frame, encrypts the text with the shared key and sends the frame to the access point. In the fourth and final step, the AP decrypts the text using the same shared key and compares this with the original text. If the texts are identical, the AP will authenticate the communication. If the comparison fails, authentication has not been successful.

The procedure above indicates that the client receives a text which needs to be encrypted from the access point, and thus sends it back encrypted. This kind of authentication is vulnerable to "man-in-the-middle" attacks. The attacker monitoring the communication may intercept the text which the AP has sent the client, as well as the encrypted text, which

means that with these two texts and the IV the attacker may acquire the elements to access the network.

As early as 2003, WEP – the initial standard for network protection – proved to be insecure. In order to enhance security and make use of the equipment which the WEP mechanism employed, protection was improved by the WPA mechanism.

To create a more secure mechanism based on the hardware employed for WEP, a new protocol was introduced. This was the Temporal Key Integrity Protocol (TKIP) composed of three elements: the Message Integrity Code (MIC), better known as Michael, a packet counter and the new function of changing keys for every packet sent. WPA uses RC4 with a 128-bit basic key and a 64-bit authentication key. Soon after the WPA mechanism was introduced, the first version saw certain improvements. WPA2 uses a new encryption method called Counter Mode with CBC-MAC Protocol (CCMP), based on the Advanced Encryption Standard (AES), which is cryptographically more advanced than the RC4 that had been previously been used. WPA/WPA2 relies on two possible authentication methods: PSK and Radius. The PSK mode generates a 256-bit PSK, or pre-shared key, from open key text. Together with the SSID, and depending on its length, the PSK creates a mathematical basis for the Pairwise Master Key (PMK). PMK is used for the 4-way handshake and generating the Pairwise Transient Key (PTK), or key to the session initiated between the client device and the access point. Enterprise access control authenticates clients according to: “client device-access point-authentication server”. In this case the access point monitors the connection and routes the authentication packets to the proper server, usually a RADIUS server. More advanced cryptographic methods such as EAP and the Radius protocol were used to attempt to create a protocol that would be completely resistant to attacks which the WEP standard had not been able to stand up to. Weaknesses of WPA authentication were observed in PSK mode; however, RADIUS has shown itself to be almost unavoidable as a security measure.

Despite the scientifically demonstrable security flaws of the WEP protocol, the WEP wireless network protection method is nevertheless still widely used. This claim is supported by research results obtained from measurements carried out on 25 May 2012. The results are presented in the following section of the paper.

3. MEASUREMENTS

Measurements carried out in May 2012 sought to investigate the use of encryption methods of wireless network protection in the Karlovac County area (the city of Karlovac, Draganić Municipality), the Zagreb County area (Jastrebarsko Municipality, Samobor Municipality, the city of Samobor, Sveta Nedelja Municipality) and the city of Zagreb.

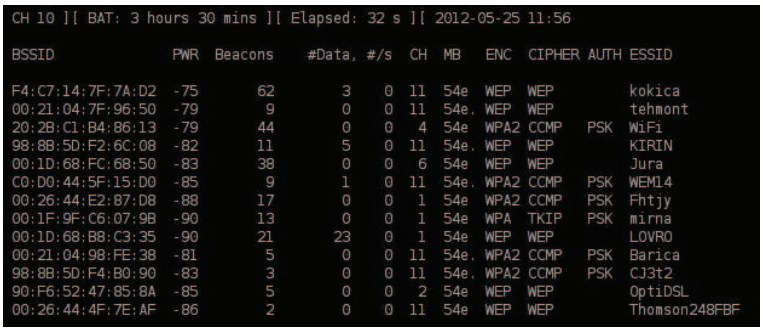
Determining and testing wireless network configurations is called “wardriving”. Wardriving refers to the gathering of statistical data on wireless networks in a particular area by using a device and an antenna to monitor publicly accessible broadcast frames of available access points. Wireless access points broadcast their location in a particular time interval (usually 100 ms) by broadcasting data packets, which also contain their SSID’s.

The software required for wardriving runs on a portable computer or a handheld device. Wardriving is done on the move. The software uses an antenna to gather data broadcast by available access points.

Some of the applications intended for wardriving offer the option of gathering information on current location, which is received by GPS, and allows the position of the detected access points to be presented cartographically.

The software used in this research was the publicly available Back Track 5 operating system. Specifically, the airodump-ng tool, available in this particular operating system, was used. This tool allows for the gathering of data which the detected access point has made publicly available. Figure 1 shows the airodump-ng display during scanning, showing the data broadcast by the access point. These are: the network name, the MAC address of the

access point, the number of the broadcast data and beacon frames, the access point channel, as well as the protection standard and the authentication method used.



```
CH 10 ][ BAT: 3 hours 30 mins ][ Elapsed: 32 s ][ 2012-05-25 11:56

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

F4:C7:14:7F:7A:D2  -75       62        3    0  11  54e  WEP  WEP         kokica
00:21:04:7F:96:50  -79        9        0    0  11  54e. WEP  WEP         tehmont
20:2B:C1:B4:86:13  -79       44        0    0   4  54e  WPA2 CCMP   PSK  WiFi
98:8B:5D:F2:6C:08  -82       11        5    0  11  54e. WEP  WEP         KIRIN
00:1D:68:FC:68:50  -83       38        0    0   6  54e  WEP  WEP         Jura
C0:D0:44:5F:15:D0  -85        9        1    0  11  54e. WPA2 CCMP   PSK  WEM14
00:26:44:E2:87:D8  -88       17        0    0   1  54e  WPA2 CCMP   PSK  Fhtjy
00:1F:9F:C6:07:9B  -90       13        0    0   1  54e  WPA  TKIP   PSK  mirna
00:1D:68:B8:C3:35  -90       21       23    0   1  54e  WEP  WEP         LOVRO
00:21:04:98:FE:38  -81        5        0    0  11  54e. WPA2 CCMP   PSK  Barica
98:8B:5D:F4:B0:90  -83        3        0    0  11  54e. WPA2 CCMP   PSK  CJ3t2
90:F6:52:47:85:8A  -85        5        0    0   2  54e  WEP  WEP         OptiDSL
00:26:44:4F:7E:AF  -86        2        0    0  11  54e  WEP  WEP         Thomson248FBF
```

Figure 1 Airodump-ng tool

Wardriving does not involve attempts to access the detected access points. The restrictions defined by the network owners are observed. If the network beacon broadcast has been disabled the access point is not detected, nor is it included in the research. In order to use the tool specified in the research, the wireless network adapter must support the Back Track operating system.

Wardriving was first developed and used in this manner by Pete Shipley in April 2001. Prior to that, research had been carried out by listening to beacon packets of available access points and taking notes by hand. Pete was the first to automate wardriving by using GPS-integrated software created for that particular purpose.

It is often thought that wardriving is not a legal activity. It is certainly against the law to connect to and use a network without permission of the owner, i.e. to engage in unauthorised network access. Wardriving may appear in a negative context, such as, for instance, if hackers use it in order to access unprotected or inadequately protected wireless networks. In order to stay within the law while wardriving, it is essential to comply with the positive legislation which is currently in force. It is against the law to connect to a network illegally, to explore network content, to alter network settings or engage in unauthorised internet access. It is important to emphasise the difference between the legal use of wardriving software and its misuse by hackers.

Driving no faster than 50-60 km/h when wardriving is recommended, since the Airodump-ng tool, as well as other applications used for this purpose, require a certain time to detect an access point and record it. Driving too fast means that certain access points will not be in range long enough and, consequently, it will not be possible to detect them.

This particular research was carried out by scanning available wireless networks at a speed of 50 km/h. The portable HP Probook 4710s was used, including the already installed Back Track 5 operating system and the wireless USB network card Aqproks 150nano2, which supports packet sniffing. Scanning was carried out along the following route: city of Karlovac-Draganići-Jastrebarsko-Samobor-Zagreb. The total length of the route is 75 km, as can be seen in Figure 2 and Figure 3. Points along the route were recorded with a standard iPhone application, version 5.01, and were used to create a cartographic presentation of the route.

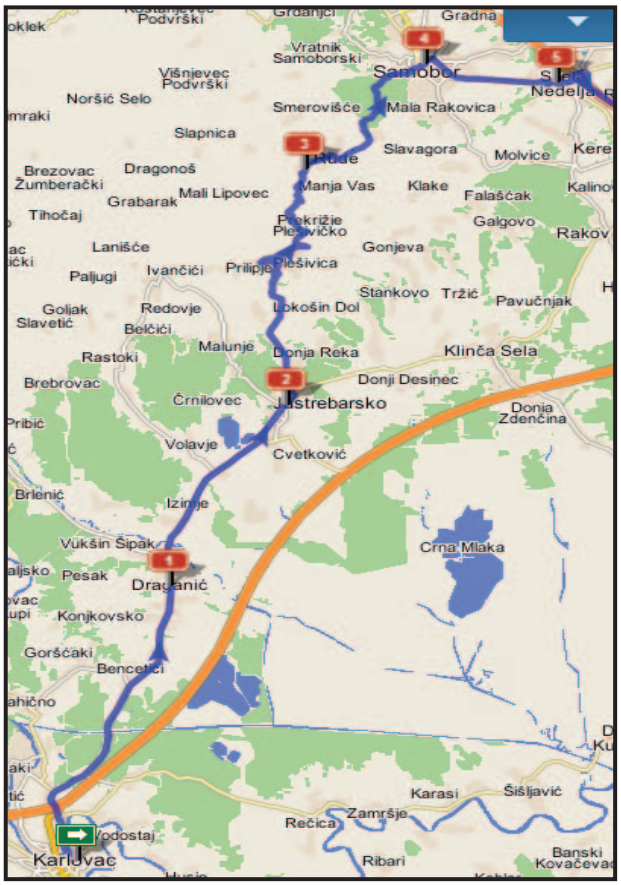


Figure 2 Route Karlovac to Zagreb

Testing was carried out along 75 km of the route shown on the map, which is 90 km long in total. They were not carried out between point 5 - Sveta Nedjlja and point 6 – Lanište, 15 km in length, because this area is sparsely populated and driving speed along the motorway was well above recommended for scanning purposes.

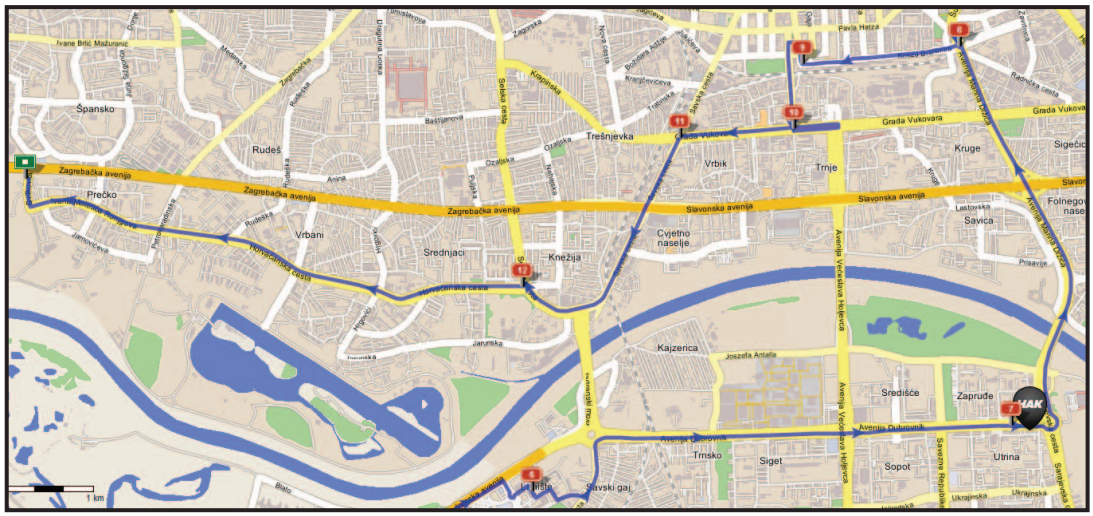


Figure 3 Zagreb route

A total of 3000 wireless networks were detected along the route. However, 100 of those detected were not fully scanned and saved, and as such were not included in the analysis. Out of the 2900 successfully scanned access points, it was determined that 5% had no

protection at all, 37% used the WEP encryption method, and 59% used the WPA encryption method. The results can be seen in a chart in Figure 4.

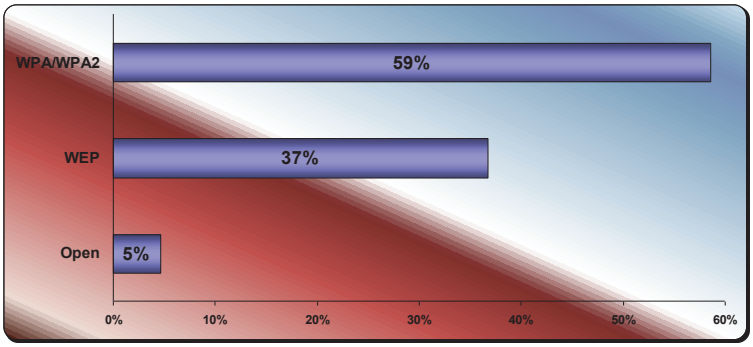


Figure 4 All Access Points

Most of the route along which the testing was carried out runs through a sparsely populated, rural area – 50 km in length (66%) – while only a shorter segment runs through a more heavily populated, urban area – 25 km (33% of the total). Still, the proportion of access points detected in urban areas amounts to merely 15% of the total access points detected.

Spatial analysis of the results indicates that more heavily populated, i.e. urban areas use more advanced protection methods compared with rural, i.e. more sparsely populated areas.

According to the 2001 census, population density figures for the municipalities included in the research are as follows: Draganić Municipality 50 inhabitants/km2, Jastrebarsko Municipality 75 inhabitants/ km2, the city of Karlovac 122 inhabitants/ km2, the city of Samobor 145 inhabitants/ km2, and the city of Zagreb 1215 inhabitants/km2.

Research results indicate a correlation between the data on population density and wireless network protection; specifically, more heavily populated areas seem to employ more advanced protection methods.

Results obtained in the Draganić and Jastrebarsko Municipality areas, shown in Figure 5, point to a relatively high level of WEP protection use. As many as 51% of users employ WEP in the Jastrebarsko Municipality area. It was determined that 11% of the access points detected in the Draganić Municipality area were completely open. It is important to note that an analysis of the SSID names indicates that these are not available hot-spots, but inadequately protected wireless networks.

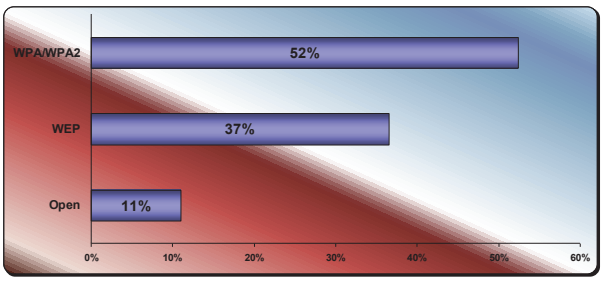


Figure 5a Draganić County

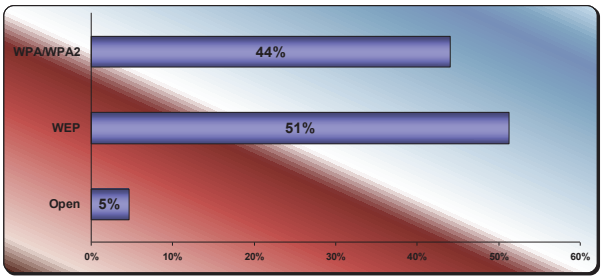


Figure 5b Jastrebarsko County

Results obtained in cities and the surrounding areas show a use of protection methods with greater resistance to unauthorised access. Results for the city of Samobor and the city of Karlovac, as well as their immediate surroundings, can be seen in Figure 6.

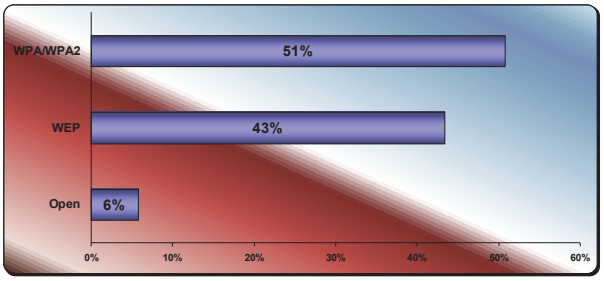


Figure 6a City of Samobor

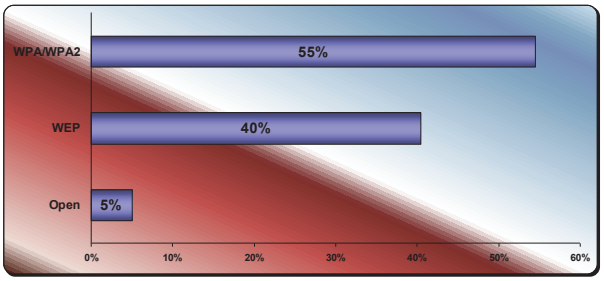


Figure 6b City of Zagreb

The city of Zagreb (Picture 7) shows a more significant proportion of users of advanced protection measures. The WPA encryption method is employed in almost 60% of the access points detected.

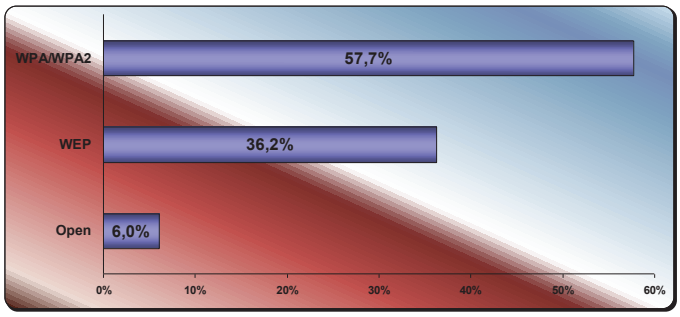


Figure 7 City of Zagreb

4. CONCLUSION

Wireless network security is a fast-developing area. Communication technologies are specific in that ordinary users today cannot do without them, yet they are complex in terms of allowing users to understand the way in which they operate. Consequently, people sometimes use systems they do not entirely comprehend, which brings about the possibility of incorrect use.

On the other hand, network security is an issue users generally do not pay much attention to. This could be due to the fact that they are under-informed and insufficiently aware of the dangers which arise from an inadequately protected wireless network.

Several wireless network protection methods are available, but even if all the available security measures have been taken this still does not mean that the required level of security has been attained. Absolute security is impossible to achieve. This is because security standards have a number of flaws and inefficiencies which are only recognised or detected after the standard has been introduced.

However, it is necessary to point out that, unfortunately, available security measures are simply not employed in a large number of cases, which is confirmed by the results of this research. This is likely to be a result of the fact users are insufficiently educated and unaware of the possible dangers which they have failed to protect themselves against. The biggest problem lies in the carelessness of network users and owners who do not employ these measures. The results of this research show that the first network protection standard to be developed is still widely used as a security measure, despite the weaknesses it has shown.

Security risks which arise in the case of inadequately protected wireless networks are the following: unauthorised access to the an internal network via a wireless network, interception of sensitive (and unencrypted) information transmitted over the wireless network, identity theft and deliberate misuse of the legitimate owner's identity, attacks on a wireless network or device, using the wireless network to launch anonymous attacks on other networks, creating fake access points, and others in similar vein.

REFERENCES

[1] WPA2 protection, CCERT-PUBDOC-2009-06-267, CARNet CERT, 2009
[2] Overview of Wireless Network Security, NCERT-PUBDOC-2010-12-001, CARNet CERT, 2010
[3] Mirza, D., Hack Proofing Your Network, Second Edition, Syngress, 2010
[4] Manzuik, S., Network Security Assessment, Syngress, 2007
[5] York, D., Seven Deadliest Unified Communication Attacks, Syngress, 2010
[6] Chen, Y., Security and Privacy in Communication Networks, Springer, 2009
[7] Schmidt, A., Security and Privacy in Mobile Information and Communication Systems, Springer, 2009