A Study of Wi-Fi Security in City Environment

H Valchanov¹, J Edikyan², V Aleksieva³

¹ Assoc. Professor, Head of Department of Computer Science, Department of Computer Science, Technical University of Varna, Varna, Bulgaria
² Programmer, Varna, Bulgaria
³ Assoc. Professor, Department of Computer Science, Technical University of Varna, Varna, Bulgaria

E-mail: hristo@tu-varna.bg

Abstract. Wireless networks are widely used with increasing number of users. Typically, they are based on the IEEE 802.11 standard (Wi-Fi). Because of its broadcast nature, they are very susceptible to security attacks. It is very important to study the risks and potential vulnerabilities of Wi-Fi networks, which will allow defining recommendations for users to enhance their security. This paper presents a methodology and research of the security of wireless networks in Varna city based on war-driving technique. The obtained results are analyzed and compared with those from previous research. The recommendations are given.

1. Introduction

Wireless networks allow easy to build small-sized home and corporate networks. The disappearance of the need to build cableways, additional networking devices and the possibility of mobility are the basis for their increasing use in recent years [1]. The spreading of Internet of Things is a prerequisite for increasing the number of user worldwide. Typically, the wireless networks are based on the IEEE 802.11 standard (Wi-Fi) [2]. Technologies have evolved continuously, giving faster speeds for users. But because of the nature of radio signals, the wireless networks are easily susceptible to security attacks. This may include both disconnect attacks and unauthorized access to resources on a network, stealing information or hiding behind a legitimate network for attacks against other networks. One of the main tasks of network security is to study the risks and potential vulnerabilities of Wi-Fi networks, which will allow defining recommendations for users to enhance their security [3].

This paper presents a methodology and research of the security of wireless networks in Varna city. Information was gathered using the use of the war-driving technique. The obtained results are analyzed and compared with those from previous studies.

2. Background

The wireless networks are primarily built on the 802.11 standard. It includes a number of standards that define the use of various wireless access technologies, starting with 802.11a and 54Mbs up to today's 802.11ah at 347Mbps [4]. The development of the 802.11 standard is tied up with the development of wireless network security protocols. There are 3 main protocols: WEP, WPA and WPA2 [5].

Wired Equivalent Privacy (WEP) – this is historically the first protocol to encrypt the connection between wireless devices based on a pre-shared key. This is also its main drawback, allowing the hacker to get this key after capturing a large number of packets. Its use is not recommended.
Wi-Fi Protected Access (WPA) – it improves security compared to WEP. It provides two ways for access control. For personally use it is recommended WPA Pre-Shared Key with a 256-bit key length. For enterprise solutions, WAP Enterprise (802.1x) and authentication server are used. To ensure the integrity of the data, Temporal Key Integrity Protocol (TKIP) is used to dynamically generate 128bit keys for every packet. Despite improvements, it is recommended to use WPA2.

Wi-Fi Protected Access 2 (WPA2) – it is an enhanced version of WPA, more resistant to attacks. It uses a new asymmetric Advanced Encryption Standard (AES) encryption algorithm and a new protocol replacing TKIP – Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP).

Despite the improved security of WPA and WPA2, both have the common problem – a possible attack through Wireless Protected Setup (WPS) [6]. This is a standard that makes it easy to configure wireless devices. The vulnerability is expressed in the ability of an attacker to break the used password within 2-4 hours and to get unauthorized access to the network.

3. Methodology
The purpose of the study is to answer the main question: What is the current state of the security of wireless networks in Varna? Achieving the goal requires the following tasks:

- Obtain information about a large number of wireless networks in Varna;
- Determine the percentage of encrypted networks;
- Identify the types of manufacturers and networks SSID;
- Determine the percentage of use of WPS.

To realize the tasks, the study is carried out in following phases: design of a system for scanning, collecting of data, data analysis and comparison of the results with ones of previous research.

4. Design of the system
Wireless security research has been a manual process since its creation, but due to the much available information, the process has not been effective for wider use. The first automated wireless network security research was carried out at the end of 1999 in California by Pete Shipley and first introduced at the DEFCON 9 conference in Las Vegas in 2001 [7]. The basic principle is to visit the area to be explored and walk around it (on foot, by bicycle or car) with hardware capable of collecting and recording information transmitted from wireless access points, as well as GPS information about their approximate position.

This study uses the war-driving technique to crawl larger areas for analysis [8, 9, 10]. A passive study has been performed and the conclusions about security being based on only the publicly available information broadcasted from each wireless access point [11].

![Figure 1.Wi-Fi scanning system.](image)

The data collection system is based on a single-board computer Raspberry Pi 3 Model B. It has an ARM Cortex-A53, 1.2GHz processor, built-in Wi-Fi and Bluetooth functionality, as well as increased
input current up to 2.5A. For the purpose of the conversion, it is necessary to record the position of each wireless access point. The selected GPS module is Holux M-1200E due to its support for the standard NMEA 0183, long-life battery and large memory support. To scan the wireless networks, the Wi-Fi module CanaKit is selected. To ensure uninterrupted power supply to the Raspberry Pi, a Canyon CNS-TPBP5DG portable battery with a 5000mAh capacity is used (figure 1). Such as embedded system makes it possible to use it also in various geographical locations where there is no possibility of driving by car (such as pedestrian, rural, village or industrial areas).

Wireless network scanning is done using Kismet open source software. The software has been compiled and installed under the Raspbian operating system. The Kismet data is recorded in netxml format then they are converted using a Python script in csv format. This is necessary for data to be presented in tabular format for easier processing and analysis with Microsoft Excel.

5. Data collection
The selected area of analysis includes the central part of Varna, because there are many offices and it includes a large part of the residents. Also, the area coincides with a similar study [12] to compare the obtained results (figure 2a).

![Figure 2](image)

**Figure 2.** Scanned areas of the city (a) and war-driving in action (b).

Driving the area was done by car, with a sustained speed of 0-35km/h. In order to monitor and control the process in real time, the Raspberry Pi Ethernet port connects to a laptop where, thanks to a VNC client, the state and information presented by Kismet are monitored (figure 2b).

6. Data analysis
The collected data includes information for a total of 19136 networks. For the purpose of the analysis, all networks which use channel 0 are excluded as invalid because of such a channel is incorrect. The reason for their occurrence is probably that there was not enough time to perform a full scan of such a network. Thus, the number of networks to be analyzed is reduced to 11534.

6.1. Wi-Fi security
Figure 3 shows the percentage of encryption methods used. These data lead to summarized results showing that the percentage of networks with WEP protection is negligible small. From the figure is shown that 7% use no encryption. It is more likely that these are public networks with open access than they are not configured. This is typical for restaurants and shops as for the public city areas.

![Figure 3](image)

**Figure 3.** Use of Wi-Fi encryption.
Only 6% of the networks use WPA, which is positive, but unfortunately, another 39% also support it because, besides the AES CCMP protocol (this mean that they support WPA2), they also support TKIP. In this way these networks, which appear to be secure (as they are WPA2 networks), are in fact unsecure because they actually work in mixed mode. In many cases, however, mixed mode is needed for old client devices that have not support for WPA2.

6.2. SSID use

Focusing only on WPA2 security networks and their SSIDs, it can be concluded that at least 13.3% of these devices use the default network name (SSID), this may mean that they use default password too which is known for the vendors (figure 4). This is a potential vulnerability for penetration.

![Figure 4. Commonly used SSIDs.](image)

The analysis of the SSIDs shows that only 2% of the SSID identifiers are hidden. This method for security is good because the network does not appear on a Windows/Mac OS/Linux scan, but this is not a problem for any more serious hacker. A particular problem is that 1/3 of these networks only rely on the fact that their SSID is hidden – they do not use any method of protection.

6.3. Wi-Fi manufacturers

The most commonly used brands for Wi-Fi devices in the city are shown on figure 5.

![Figure 5. Wi-Fi vendors.](image)

The TP-Link brand is on the first place – the reasons for this are both the low price and the fact that one of the largest suppliers in the city (TCV) provides models of this brand for its customers free of charge. For the second and third, Huawei and Zte, the situation is similar. Mtel provides Huawei devices, Vivacom (previously provided ZTE) in recent years also provides Huawei. For both providers, due to the type of infrastructure, the wireless router settings can be made remotely and in group. However, thanks to better default settings, only for TP-Link models the percent for WPA2-protected networks is larger than combined WPA/WPA2 method (figure 6).
6.4. **WPS support**

The figure 7 shows how many of the networks in Varna offer the WPS function. It is a very important factor for security as mentioned before. It is supposed that many users are not familiar with the problems in the technology.

When analyzing WPS support for top brands, it is noticed that for TP-Link 77% of the devices allow WPS to be used. For Mtel and Huawei devices, the default WPS is off. For Vivacom and ZTE, the situation is the opposite - WPS is implicitly switched on (figure 8).
7. **Comparison with previous research**

This study aims to compare the results obtained with similar ones obtained in 2008 [12]. The survey collected data for 688 networks. Compared with the current number of detected networks, this means that for 10 years in the city the number of networks has increased more than 16 times. The real percentage may be lower as the network card with which the scanning was performed, detected networks with the highest standard of 802.11g. But summary, the results show that for this period there was a significant increase in the use of Wi-Fi networks in Varna.

![Figure 9. Use of Wi-Fi encryption in 2008 [12].](image)

In addition to a significant increase in the number, there is also a major improvement in network security as shown on figure 9. The percentage of networks without any protection has decreased almost 4 times, from 39% to 7%, and networks with WEP protection level are virtually not found (as opposed to over 30% in 2008). The WPA level has also decreed to a small number of 6%, and the increase is directed to WPA2 (40% growth) and WPA/WPA2 mixed devices.

With regard to manufacturers, the only device brand retained and even increased its share is ZTE. All other major players in 2008 have a market share of less than 5% (now Cisco-Linksys has 2% and D-Link - 3%). The previously obtained results are shown on figure 10.

![Figure 10. Wi-Fi vendors in 2008 [12].](image)

Comparing the results from previous research can be summarized that the security level has been greatly increased. But in the same time due to the detected shortcomings in the wireless router security over the years, the number of real users with vulnerable security has also actually increased (the total number of unprotected networks and those using WEP or WPA is 1634 – 60% more than analyzed in 2008.

In Varna 47% of the networks use the current WPA2 standard and thanks to this, the wireless networks in the city have a better relative security level.

An extremely worrying fact is that 59% of the WPA2 protection networks in Varna use the WPS function, significantly reducing their security. In addition, at least 13.3% of these networks use default network names. This means that they also use a default password with a minimum length susceptible to dictionary attacks.

The budget required for implementing an attack on WEP, WPA, WPA/WPA2 mixed mode or WPS is extremely low - up to 50 EUR are needed to buy a wireless adapter that allows active mode of
operation. There are a myriad of methods and programs that make it easy to implement an attack by a few mouse clicks.

Although there is a significant improvement in security since 2008, there are still many steps to be taken to ensure good security for wireless networks in Varna. This is critical, as the growth in the number of wireless access points and devices will continue to grow in the future.

8. Conclusions

This paper presents a wireless security research carried out in Varna city. A war-driving technique was used based on a developed Raspberry Pi scanning system. The obtained results are compared with similar ones made in 2008.

The answer to the main question of the survey can be formulated as follows: The results show a significant increase in the security of the Wi-Fi networks in the city, but there is a need for further improvement.

The main recommendations can be in the following directions:
1. Increase awareness for the security issues and the effect they may have on the users.
2. Use only WPA2 method. If there is a need to support older devices, build a separate, limited network that supports mixed WPA/WPA2 mode.
3. Disable WPS for all devices.
4. Select a password of at least 12 characters with uppercase and lowercase letters and numbers.
5. Update the firmware used by the wireless router to the latest available version. Another option is the use of an alternative firmware such as OpenWRT/DD-WRT, in which security issues are generally removed much faster.

As guidelines for the future work may be the analysis of newest 802.11ac and 802.11ah networks, and study and comparison of the security level in the wide districts of Varna and region.

References

[1] Colbach G 2017 Wireless Networking: Introduction to Bluetooth and WiFi (Independently published)
[2] IEEE 802.11 Wireles local area networks http://www.ieee802.org/11/ (last visited 03.2019)
[3] Gopalakrishnan S 2014 A survey of wireless network security IJCSMC 13 pp 53–68
[4] IEEE 802.11-2019 standards https://standards.ieee.org/standard/802_11-2016.html (last visited 03.2019)
[5] NetSpot Wireless security protocols: WEP, WPA, WPA2, and WPA3 https://www.netspotapp.com/wifi-encryption-and-security.html (last visited 03.2019)
[6] Viehböck S Brute forcing Wi-Fi Protected Setup https://sviehb.files.wordpress.com/2011/12/viehboeck_wps.pdf (last visited 03.2019)
[7] DEF CON Nine Schedule https://www.defcon.org/html/defcon-9/defcon-9-speakers.html#Peter%20Shipley (last visited 03.2019)
[8] Dobrilovic D 2016 A method for comparing and analyzing wireless security situations in two capital cities Acta Polytechnica Hungarica 6 13 pp 67–86
[9] Sebbar S B 2016 An empirical study of WIFI security and performance in Morocco - wardriving in Rabat Int. Conf. on Electrical and Information Technologies
[10] Kyaw K A, Tian Z and Cisak B 2016 Wi-Pi: a study of WLAN security in Auckland city IJCSNS 8 16 pp 68–80
[11] Priya S U 2013 The Impact of War Driving On Wireless Networks IJCSET 6 3 pp 230-235
[12] Hristo Valchanov H, Ruskov I and Varbanov A 2009 A Study of the Wireless Network Security Proc of 5th Conference “Computer Science 2009” (Sofia) pp 273-278