

A Method for Comparing and Analyzing Wireless Security Situations in Two Capital Cities

Dalibor Dobrilovic¹, Zeljko Stojanov¹, Stefan Jäger², Zoltán Rajnai³

¹ University of Novi Sad / Technical Faculty “Mihajlo Pupin”, Djure Djakovica bb, 23000 Zrenjanin, Serbia, dalibor.dobrilovic@uns.ac.rs; zeljko.stojanov@uns.ac.rs

² University of Jena/Department for Communication and Computer Engineering; IT-Security, Ernst-Abbe-Platz 1, 07743, Jena, Germany, m4jast@uni-jena.de

³ Óbuda University/Doctoral School on Safety and Security Sciences, Népszínház u. 8, H-1081 Budapest, Hungary, rajnai.zoltan@bgk.uni-obuda.hu

Abstract: An increasing number of wireless Internet users and deployed wireless access points over the past several years and have raised the importance of wireless security issues. The absolute majority of wireless users are not IT professionals, but a population unaware of wireless security types, settings and importance. Wireless security assessment and analytics can help in raising the security awareness of users and in increasing their skills, leading to improvement of the entire security situation. In this paper a short overview of wireless security assessment and history is presented. The methodology and tools for a more accurate wireless security assessment, including data acquisition, processing and analysis, are offered. The proposed methodology and tools are used for processing wireless scan results for the two capital cities, Hungary (Budapest) and Serbia (Belgrade). The possibility of access point configuration changes and security improvement has also been investigated. The research results and potential improvements of wireless security situation are discussed.

Keywords: wireless network security; Wardriving; wireless security assessment;

1 Introduction

This paper focuses on wireless security issues. Motivation for this research rests in the fact, that in recent years, we have been witnesses of a rapid growth in the number of Internet users, who mainly use wireless technology. The advances in wireless technology, decline in the price of wireless equipment and ease of its

usage, have resulted in the deployment of a large number of wireless access points in most locations (homes, offices, public buildings, etc.). Although wireless access has become accessible to most everyone, the majority of wireless users are not skilled or educated in wireless security issues. This has led to the creation of the biggest security hole in computer systems since the beginning of the computing revolution. The importance of the assessment of wireless networks security, comes from the need to tackle the problem in order to identify the major causes of security faults and to find ways to prevent or minimize them.

This paper outlines the history of wireless security assessment, with examples from around the World, Europe and the regions where the research was conducted. The methodology and tools for data analysis are presented. Collected and processed data for two capital cities, Hungary (Budapest) and Serbia (Belgrade) are presented and compared. The possibility of access point configuration changes and security improvements are also investigated. Finally, the recommendations for further assessments are proposed.

2 Wireless Security and Wardriving

A widely accepted process for wireless security assessment is called “Wardriving” [1, 2]. This term comes from the term “wardialing” mentioned in the famous hacking movie “War Games” from 1983, where it was used for the process of calling a pool of telephone numbers in order to find a computer with a modem attached [1]. The Wardriving became world famous starting with Peter Shipley, a computer security consultant at Berkeley. He conducted a survey in Berkeley, California and reported the results at DefCon hacker conference in July 2001, aimed at raising the awareness of wireless security importance. The popularity of Wardriving continued to grow starting from 2002, when the first worldwide event called WWWD (World Wide War Drive) was held, with the total of 9,734 scanned access points. The participants in this event were from 6 countries and 2 continents. In the following events the number of participants and scanned access points increased: WWWD2 in September 2002 (24,958), WWWD3 in 2003 (88,122) and WWWD4 in 2004 with 228,537 discovered access points. Since these events, academy researchers, security experts and consultants have performed similar scans worldwide.

2.1 Research on Wireless Security

Since 2001, wardriving has become the activity practiced by enthusiasts, hobbyists, security experts and malicious hackers. This section presents only the Wardriving activities related to academic research [3, 4, 5]. The Wardriving has been widely accepted by academic researchers. It was performed all over the

world, e.g. in Malaysia in 2005 [6], La Plata, Argentina in 2008 [7], Australia in 2011 [8, 9] and New Zealand in 2013 [10, 11]. This research field is also popular in the region, where recent and up to date statistical reports and analyses from Croatia in 2013 [12, 13], Romania in 2015 [14] and Serbia since 2010 [15, 16, 17, 18, 19] were published. The experiences from the presented research, acquisition tools and analysis techniques are used for shaping the methodology in this research work.

2.2 Wireless Security Settings

Basically, wireless network or access point (AP) security can be classified in five or seven categories. The five categories are: Open, WEP, WPA, WPA2 and mixed-mode networks. Mixed-mode networks support both WPA and WPA2. Those five categories can be expanded further by dividing the WPA and WPA2 categories to subcategories such as: WPA-Personal and WPA-Enterprise. The categories are defined by the encryption methods and by the authentication mechanism they use. The encryption methods and the authentication mechanisms will be explained in the following subsections.

Generally, WEP uses WEP encryption, WPA uses TKIP, and WPA2 uses CCMP. There is a possibility that WPA or WPA2 method uses both TKIP and CCMP due to the vendor's attempt to maintain legacy compatibility. The personal WPA and WPA2 use PSK (Pre-shared key) for local authentication and Enterprise WPA and WPA2 use 802.1x (EAP) and an external authentication server (RADIUS). All these methods will be explained in the following subsections.

Open network uses neither encryption nor authentication. In this research, with the used tools, open networks are identified as networks with the absence of encryption and authentication data, only with the data about the network type: [ESS] or extended service set (Table 1, item no. 7) for infrastructure networks and [IBSS] or independent basic service set for ad-hoc networks. In addition, they have an indicator whether WPS is used or not, with the presence or absence of [WPS] mark (see Table 1, item no. 15, in Research methodology section). Those networks do not have WEP, WPA, WPA2, TKIP, CCMP, EAP or PSK marks.

2.3 Wi-Fi Protected Setup (WPS)

WPS was designed by the Wi-Fi Alliance, to enable easy authentication despite the use of a complex password. The user-unfriendly typing of long and complex passwords is eliminated by the use of WPS. There are several variants of the use of WPS. From a security perspective, the PIN is to be regarded as critical [20].

Access Points which support this method have a WPS button. If this is pressed, the WPS PIN must be entered on the client device within a short period (usually 60 seconds). This PIN is usually found on a label on the access point. The problem

with this approach is the weak structure of the 8-digit PINs, which consist only of numbers. Thereby, brute force attacks can be performed very effectively within the allowed time frame. If there are no other security mechanisms for attacks against WPS, such attacks will be repeated within a few hours [21]. Since the WPS PIN does not change automatically, the attack can be interrupted and continued at a different time. Unlike attacks against WPA2, the attack must necessarily be directed against the Access Point.

There are several free tools specialized in this type of attack, for example, Reaver. The security mechanisms implemented in AP can block WPS mode in case there are too many PIN-tries, within a short time period. Reaver can circumvent these mechanisms and other safeguards. If the Reaver tool is successful, the Wi-Fi password will be returned as plain text.

In most Access Points, WPS is enabled by default in the PIN mode. Since most users assume that a strong WPA2 password is sufficient for a secure network, they often forget to turn off WPS. For safety considerations, the analyzed networks, therefore, must be checked for encryption on one side and for activation of WPS on the other.

2.4 Wireless Encryption Methods

Three encryption methods operating at Layer 2 of the OSI model are defined by 802.11-2007 standards. The three methods are: WEP, TKIP and CCMP. They are used to encrypt MAC Protocol Data Unit (MPDU) payload or the data contained in IP packets. All three methods use symmetric algorithms. WEP and TKIP use the RC4 cipher (stream cipher), while CCMP uses the AES (Advanced Encryption Standard) cipher (block cipher) [22]. The 802.11-2007 standards define WEP as a legacy encryption method, for pre-RSNA security, while TKIP and CCMP are considered to be compliant Robust Security Network (RSN) encryption protocols. The next difference between WEP on one side and TKIP and CCMP on the other side, is that WEP uses a preconfigured static key that is liable to attacks. Alternatively, TKIP and CCMP use encryption keys, dynamically generated by the 4-Way Handshake [22].

2.4.1 WEP

Wired Equivalent Privacy (WEP) is the simplest form of wireless security. It is a Layer 2 security protocol, that uses the Rivest Cipher 4 (RC4) streaming cipher [22]. It uses two variants of relatively small shared key: 64-bit and 128-bit. Standard 64-bit WEP uses a 40-bit key (also known as WEP-40), which is concatenated with a 24-bit initialization vector (IV) to form the RC4 key. This method of security is only a little bit more secure than clear-text passwords. The reason is the weakness in the WEP protocol. The WEP protection can be

compromised in several minutes, using free and widely available tools on the Internet [23]. If enough data packets are recorded, the password can be determined in any case. Because of this, the networks and Access Points using WEP will be considered extremely unprotected in this research.

2.4.2 WPA

WPA (Wi-Fi Protected Access) is based on the IEEE standard 802.11i. It was introduced in April 2003 by the Wi-Fi Alliance. The usage of TKIP encryption is defined within the standard as an enhancement of WEP aimed at overcoming its weaknesses. It uses Rivest Cipher 4 (RC4) streaming cipher for encryption and decryption processes. TKIP modifies WEP with longer 128-bit per-packet key that dynamically generates a 48-bit initialization vector (IV) with Message Integrity Check (MIC) for each new packet. MIC is designed for preventing active or passive man-in-the-middle attacks. Because WPA is designed as an interim short-term solution to enhance wireless security, it has its own weaknesses [24, 25]. WPA should only be used on legacy hardware that is not capable of supporting AES-CCMP. TKIP is mandatory when WPA is used [23].

2.4.3 WPA2

WPA2 is based on the IEEE 802.11i/WPA2 or IEEE 802.11i-2004 standard defined on June 24th, 2004 and it is a stronger version of WPA. It uses AES (Advanced Encryption Standard) cipher (block cipher) with Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP). AES accepts keys with size of 128, 192, and 256 bits [24]. The usage of AES-CCMP is mandatory for WPA2. Still, in order to maintain compatibility with the legacy equipment, vendors allow TKIP to be used with the clients not supporting AES-CCMP.

2.5 Wireless Authentication

As described in the beginning of this section, both WPA and WPA2 support two methods of authentication: personal and enterprise. The personal method is local authentication, which is commonly used. The enterprise authentication is server based and much less present in access point configuration, because it requires a separate authentication server and it is designed primarily for companies.

2.5.1 Personal Networks

Personal WPA and WPA2 networks are intended to be used for ad-hoc configured access points and home networks. They use a pre-shared key (PSK) which is vulnerable to password/passphrase guessing using dictionary attacks [26]. PSK must start with the definition of passphrase at the access point (AP) which will be

used for generating encryption keys. In this operational mode, there is no authentication exchange and a single private key can be assigned to entire network or to one client. In order to create a secure passphrase, the recommendation is to compose a very complex one with more than 20 characters. The dictionary words should not be used and a passphrase must contain lower and upper case letters, numbers, and symbols. If the recommendations are not followed, networks are easier to crack [27, 28]. Personal networks will be identified in this research as [WPA-PSK.....] (Table I, column 2, first three rows).

2.5.2 Enterprise Networks

The enterprise authentication uses 802.1x and an external authentication server such as Remote Authentication Dial In User Service (RADIUS). Therefore, the three standards define this process: EAP, 802.1x, and RADIUS.

The Extensible Authentication Protocol (EAP) is a layer 2 process that allows a wireless client to authenticate to a network. There is a version of EAP that is used in LAN environments called EAP over LAN (EAPoL) and a version for wireless networks. EAP defines a standard way for encapsulating authentication information, such as a username and password or a digital certificate that the AP can use to authenticate the user. The authentication process is taking place beyond AP in communication with authentication server. EAP has several extensions: EAP-MD5, EAP-TLS, LEAP (Lightweight EAP), PEAP (Protected EAP), EAP-FAST and EAP-GTC [29].

802.1x and RADIUS define packets for EAP information, e.g. 802.1x standard defines transport from a client to a network access device (AP, switch, router, etc.). These data are passed using RADIUS protocol to an authentication server. The server will authenticate the user and allow his access to the network.

2.6 Wireless Security Assessment Tools

A numerous software tools can be used for performing Wardriving. The usage of tools also depends on hardware and software platforms. Only a small segment of Wardriving tools will be presented here, while a more detailed overview is given in [15]. In case of using PC or laptop computer and Windows operating system the possible tools are Vistumbler, InSSIDer, etc. In case of using Linux operating system, Kismet [30] presents almost de-facto standard. Great expansion of possible tools for Wardriving was influenced by the introduction of Android smart phone platform, which gave access to the variety of Wardriving tools such as: Wigle WiFi [31], War-drive, G-Mon, WiFi finder, WiFi tracker, etc. The iOS platform (available for iPhone and iPad) has the similar software tools, e.g. WiFiFoFum and WiFi Explorer.

The new minimized computer boards such as Raspberry Pi, Beagle Bone or Arduino Yun opened new horizons in building Wardriving platforms, as presented for Raspberry Pi in [32]. The added value is, inter alia, the fact that these mini computers combine the benefits of computers and smart phones. They can perform the tasks of computers, but they are as small and light, as a smart phone. Thus, these devices can not only, locate and scan networks, they can also perform security and penetration tests.

3 Research Methodology

The research methodology contains the following components: data acquisition tool, data processing tools and a method for data acquisition and analysis of results. Android application Wigle WiFi, designed for usage on smart phones, was used as the data acquisition tool.

The reason for using the Wigle application in this research is the positive experience of researchers in using this application in the long period in the past. Wigle application has a capability to export retrieved wireless access point (AP) or wireless networks data in KML (XML file format for geocoordinates) and CSV format. Basically, a wireless network and a wireless AP represent the same thing in this research. CSV format is used, in the following form:

```
AA:AA:AA:AA:AA:AA, BB, [WPA-PSK-TKIP][ESS], 6/20/2015 13:57, 6, -97,  
44.8185463, 20.3735048, 0, 336, WIFI
```

The first column represents access point MAC address which is unique in the whole world for the corresponding device (used MAC address is fictional). The second column represents SSID (network name). The third column is the most important for this research, representing security type of the scanned AP. In this research, 86 different security types were identified in Belgrade and Budapest. The partial list of detailed security types is given in Table 1. The next data are date and time of scanning, channel or frequency used by the wireless network (1–13), RSSI or received signal strength in dBm, latitude, longitude, altitude, accuracy in meters and type of detected network (WIFI or GSM).

3.1 Data Processing Application

Data processing application called WDStat v2.0, is built with C#. This application allows import of Wigle CSV format, and some other formats as well (GPX). This software parses a Wardriving log downloaded from Android smart phones, aimed at creating a database. The additional data added to the database are locations of APs using the GPS coordinates from Wardriving logs, and determination of the

geographical location according to these coordinates. Description of a geographical location and association of the scanned network with the cities, towns, regions and countries is presented in [16].

Acquired data are further processed and statistically analyzed in order to make statistical reports. The reports summarize the following statistics: channel usage, SSID statistics, grouped security stats (e.g. Open, WEP, WPA, WPA2, and Mixed-mode), CCMP usage stats for WPA, WPA2 and Mixed-mode networks, WPS usage statistics, Ad-hoc or infrastructure network statistics, geographical locations statistics, detailed security statistics as described in Wigle CSV format and vendor statistics. The vendor statistics is built on MAC address allocation according to IEEE MAC address allocation list [33]. The results for Budapest 2015/2016, Belgrade 2015/16 and Belgrade 2013/2014 research scans for channels and security type usage are given in Fig. 1.

The application simplifies the security settings description, making security change analysis easier. The simplification is performed from security type description shown in Table 1, which is the original security type derived from Wigle WiFi scan log, to the simplified version shown in Table 8 and the most generalized one shown in Table 7.

For example, original security types, such as [WPA-PSK-TKIP+CCMP][WPA2-PSK-TKIP+CCMP][WPS][ESS] can be simplified as Mixed_TKIP_CCMP_PSK_WPS and further simplified as Mixed and WPS security groups. The next example: [WPA2-EAP-CCMP][ESS] can be simplified as WPA2_CCMP_EAP_noWPS and further simplified as WPA2 and no_WPS security groups.

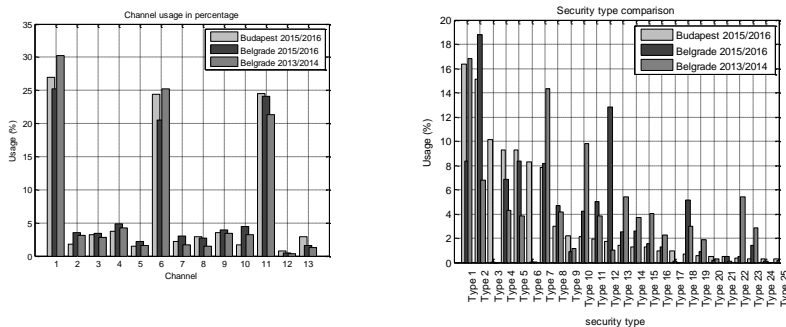


Figure 1

- a) Wireless channel usage comparison
- b) The most used wireless security settings comparison

The top 25 detailed security analysis results are presented in Fig. 1 b) and in Table 1. The pair of columns represents the number of discovered access points and their percentage in accordance with the total discovered APs. The data are given for the Budapest 2015/2016, Belgrade 2015/2016 and Belgrade 2013/2014 scans, respectively.

Table 1
Comparison of the top 25 wireless security settings

Type No.	Security type / City	Budapest 2015/2016		Belgrade 2015/2016		Belgrade 2013/2014	
		No.	%	No.	%	No.	%
1	[WPA-PSK-CCMP+TKIP][WPA2-PSK-CCMP+TKIP][WPS][ESS]	2,336	16.35	1,513	8.37	4,926	16.84
2	[WPA-PSK-CCMP+TKIP][WPA2-PSK-CCMP+TKIP][ESS]	2,162	15.13	3,398	18.8	1,991	6.81
3	[WPA-EAP-CCMP+TKIP][WPA2-EAP-CCMP+TKIP][ESS]	1,449	10.14	2	0.01	0	0
4	[WPA2-PSK-CCMP][WPS][ESS]	1,330	9.31	1,243	6.88	1,253	4.28
5	[WPA2-PSK-CCMP][ESS]	1,328	9.3	1,507	8.34	1,253	3.81
6	[WPA2-EAP-CCMP+TKIP][ESS]	1,186	8.3	4	0.02	10	0.03
7	[ESS]	1,123	7.86	1,474	8.16	4,199	14.36
8	[WPA-PSK-CCMP][WPA2-PSK-CCMP][WPS][ESS]	427	2.99	842	4.66	1,225	4.19
9	[WPA2-PSK-CCMP+TKIP][ESS]	317	2.22	162	0.9	346	1.18
10	[WPA-PSK-TKIP][ESS]	304	2.13	768	4.25	2,860	9.78
11	[WPA-PSK-CCMP][WPA2-PSK-CCMP][ESS]	277	1.94	909	5.03	1,115	3.81
12	[WPA2-EAP-CCMP][ESS]	247	1.73	2,315	12.81	290	0.99
13	[WPA-PSK-CCMP+TKIP][WPA2-PSK-CCMP+TKIP-preauth][ESS]	202	1.41	461	2.55	1,592	5.44
14	[WPA2-PSK-CCMP+TKIP][WPS][ESS]	186	1.3	466	2.58	1,077	3.68
15	[WEP][ESS]	180	1.26	283	1.57	229	0.8
16	[WPA-PSK-TKIP][WPA2-PSK-TKIP][ESS]	139	0.97	228	1.26	658	2.25
17	[WPA-EAP-CCMP][WPA2-EAP-CCMP][ESS]	131	0.92	22	0.12	0	0
18	[WPA-PSK-CCMP][ESS]	102	0.71	929	5.14	867	2.96
19	[WPS][ESS]	76	0.53	158	0.87	545	1.86
20	[WPA-PSK-CCMP+TKIP][WPA2-PSK-CCMP+TKIP-preauth][WPS][ESS]	74	0.52	33	0.18	80	0.27
21	[WPA2-PSK-CCMP-preauth][ESS]	66	0.46	92	0.51	23	0.08
22	[WPA2-PSK-CCMP+TKIP-preauth][ESS]	50	0.35	89	0.49	1,592	5.44
23	[WPA2-PSK-TKIP][ESS]	46	0.32	251	1.39	843	2.88
24	[WPA2-PSK-CCMP][ESS][SEC80]	42	0.29	22	0.12	0	0
25	[WPA-PSK-TKIP][WPA2-PSK-CCMP+TKIP][ESS]	38	0.27	26	0.14	57	0.19

Note: The grouped security types are: Open = type 7 and type 19, WEP = type 15, WPA = type 18, WPA2 = type 4, type 5, type 6, etc., Mixed-mode = type 1, type 2, type 3, etc.

The grouped security statistics are given in Fig. 2 a) and WPS and CCMP statistics are given in Fig. 2 b).

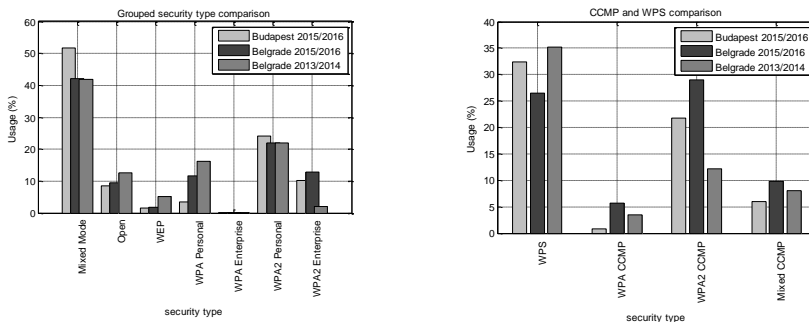


Figure 2

- a) Security type comparison b) WPS and CCMP encryption usage comparison

3.2 Data Acquisition

Data acquisition was performed with several Android devices using different versions of the Wigle WiFi application. The Wardriving sessions were made in two separate periods. The first session was organized during 2013/2014 in larger parts of Serbia. The results of this Wardriving session were partially published in [15]. The second session was organized in Serbia in 2015/2016 and Hungary 2015/2016. The Hungarian session took place, mainly, in Budapest and the surrounding area.

For this research, the Hungarian 2015/2016 and Serbian 2015/2016 scans were used for analysis and comparison of wireless security situations in two capital cities. In order to determine the possibility, rate and quality of improvements of access point security through the changes during the usage period, the Serbian 2013/2014 session data for the city of Belgrade were used for comparison and determination of improvement rate of the wireless security of once configured access points. The quality of sample used for these analyses is justified with the number of scanned networks, number of appearances of the scanned networks and number of networks scanned in both research periods.

In this research the Wigle WiFi was used. Fig. 3 presents the part of the scanned wireless networks or access points with their locations in Budapest and Belgrade. Google maps are used for visualization. The part of scanned networks is presented in similar areas in Belgrade. The city center and its close surroundings are presented in these images. The profile of wireless users should be the same in these regions.

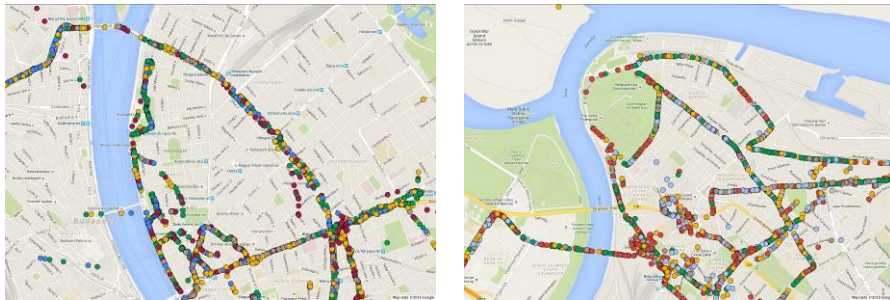


Figure 3

a) Part of scanned networks in Budapest 2015/2016 b) Part of scanned networks in Belgrade 2015/2016

3.3 Results

During both research sessions, 31,928 different networks were discovered. The networks were identified by their unique MAC addresses. After removing duplicates, 10,285 networks (APs) were discovered in both Wardriving sessions which can be used for security change analysis.

Table 2 presents the statistics of number of appearances of 10,285 networks scanned in two periods. It is important to point out that the 66.52% were scanned more than 5 times (first four rows in the table).

Table 2

The number of appearances of scanned access points in the 2013/2014 and 2015/2016 period

No. of appearances	No of APs	(%)
9	100	0.97
8	640	6.22
7	2,217	21.56
6	3,885	37.77
5	652	6.34
4	1,204	11.71
3	83	0.81
2	1,504	14.62
Total	10,285	100.00

Only 936 networks among 10,285 were detected to have changed their configuration compared to the initial scanning. The number of appearances of changed configuration networks is given in Table 3 in order to justify the quality of sample. Since 62.50% of networks were scanned 7 or more times (the first three columns in the Table) the sample can be qualified as good for analysis.

Table 3

The number of appearances of scanned access points in the 2013/2014 and 2015/2016 period

No. of appearances	No of APs	(%)
9	30	3.21
8	125	13.35
7	430	45.94
6	12	1.28
5	64	6.84
4	11	1.18
3	8	0.85
2	256	27.35
Total:	936	100.00

The number of changes is summarized and presented in Table 4. The majority of networks were changed only once – 916, which makes 97.86% of changed networks and only 8.91% of total networks. Only 20 networks were changed 2 or 3 times. These statistics clearly show that configuration changes are not likely to happen during the access point usage.

The configuration change analytics, together with the details of data acquisition, is given in the following section.

Table 4
The number of configuration changes per access point

No. of Changes per AP	No. of Aps	%	% (Total)
1	916	97.86	8.91
2	16	1.71	0.16
3	4	0.43	0.04
Total	936	100.00	9.11

4 Discussion

4.1 Comparison of Wireless Security in Two Capital Cities

The results presented in Fig 2 a) are summarized in Table 5. For researches in period 2015/2016, the same device and the same software have been used. According to the results presented in the table, the security situations in Budapest and Belgrade are similar. The percentage of Open and WEP security access points is similar. The only difference is that in Belgrade, there is a higher percentage of WPA-Personal networks, 7.97% more than in Budapest. On the contrary the percentage of Mixed-mode networks in Budapest is 9.61% higher than in Belgrade. This gives slightly better security result in favor of Budapest. The percentage of most secured networks (WPA2-Personal and WPA2-Enterprise) is similar for Budapest (34.5%) and Belgrade (34.83%).

Table 5
The grouped security types

City and period	Number	Open (%)	WEP (%)	WPA-Per (%)	WPA-Ent (%)	WPA2-Per (%)	WPA2-Ent (%)	Mixed Mode (%)
Budapest 2015/2016	14,287	8.62	1.45	3.56	0.06	24.18	10.32	51.81
Belgrade 2015/2016	18,070	9.49	1.9	11.53	0.03	21.96	12.87	42.22
Belgrade 2013/2014	13,621	12.71	5.14	16.2	0.12	21.91	2.06	41.86

Table 6 summarizes the results showed in Fig. 2 b) with the percentage of WPS enabled access points, and furthermore with the percentage of access points with the support for only CCMP encryption. The situation regarding the two security statistics is in favor of Belgrade, where the percentage of WPS-enabled networks is 5.91% lower. Considering the WPS vulnerabilities, the smaller percentage is better. The access points enabling only CCMP are also in favor of Belgrade, meaning that 15.97% networks in Belgrade are more secure since they use exclusively this encryption method.

Table 6
WPS and CCMP security statistics

City and period	Number	WPS (%)	WPA_CCMP (%)	WPA2_CCMP (%)	Mixed CCMP (%)
Budapest 2015/2016	14,287	32.44	0.8	21.78	5.91
Belgrade 2015/2016	18,070	26.53	5.63	28.97	9.86
Belgrade 2013/2014	13,621	36.74	3.19	14.27	8.71

4.2 Access Points Configuration Changes

Scanning of wireless networks considered for the configuration change analyses took place in Belgrade from November 2013 to February 2016. During this period 79,947 different scans were collected, among which 31,928 unique networks were identified. For this research it is important that 10,285 networks appear more than once in the retrieved data. These networks were scanned at least twice and up to 9 times. One to up to tree changes were detected on analyzed networks. The detailed overviews of appearances of scanned networks are given in Table 2 for the discovered networks in both research periods and in Table 3 for the networks with detected changes.

For this research, the grouping which is described later was made according to the first and the last change, so that the last change is considered as a final change of a configuration. For example, some networks were changed 3 times, meaning that the changes were tracked in the following format: Configuration1 → Configuration2 → Configuration3 → Configuration4. In this research, the change of configuration is made according to Configuration1 → Configuration4 format, i.e. only the first and the last configurations are considered for the transition.

All scanned data were sorted according to the date and time of data acquisition, before data analysis with the software tool built for that purpose. This was made in order to avoid confusion with the timeline of configuration changes and to avoid possible data inaccuracy. For example, if the collected data are not sorted according to timeline, the configuration change might be accidentally identified as a change from a higher to a lower level of configuration.

Among the scanned networks, there are several recorded cases where configuration transition is as follows: WPA2→Open, Mixed→Open, WPA→Open, WPA2→WEP, WPA→WEP, Mixed→WEP, WEP→WEP and Open→WEP. In all these cases, the settings which might be qualified as secure are changed to less secure settings, even using obsolete encryption type such as WEP. Since there is a little possibility to justify reconfigurations from WPA/WPA2 secured to Open networks, the explanation for transition from WPA/WPA2 secured to WEP networks is not possible, especially in the period between 2013 and 2016. Therefore, there is space for thinking that there might be an error in acquired data, sorting process or even in analyzing software itself. So far, the errors have not been identified and all statistical data can be considered accurate. If the errors

exist, the important thing is that they do not significantly affect the results and analysis since the number of listed cases is 62 or 0.6% of total networks. The other explanation is that AP was reset to factory settings and after this the provider or owner failed to configure AP again.

The software identified 936 networks with changed configurations, which makes only 9.1% of all analyzed networks. Furthermore, the analysis tried to identify if these changes were generally made for better, worse or similar security levels. In order to do these analyses, the three criteria are defined. One criterion divides a large number of security types shown in Table I and Fig. 2b) in 25 categories according to transition from one grouped security level such as: Open, WEP, WPA, WPA2 and Mixed. The number of 25 means that each of 5 groups can be changed to the same 5 groups, e.g. Open→Open, Open→WPA2 or WEP→WPA2. The presented transitions are given in Table 7.

Table 7
The types of security setting changes and their percent in analyzed networks

No.	Group change	No. of APs	(%)	Ch	No.	Group change	No. of APs	(%)	Ch
1	Mixed→Mixed	371	39.64	N	14	WPA→WPA	17	1.82	N
2	Mixed→WPA2	61	6.52	B	15	Mixed→Open	16	1.71	W
3	WPA2→Mixed	61	6.52	W	16	Open→Open	14	1.50	N
4	Open→Mixed	53	5.66	B	17	WEP→Mixed	14	1.50	B
5	Open→WPA2	49	5.24	B	18	WPA→Open	14	1.50	W
6	Mixed→WPA	48	5.13	W	19	WEP→Open	5	0.53	N
7	WPA2→WPA2	39	4.17	B	20	WPA2→WEP	4	0.43	W
8	WPA→WPA2	36	3.85	B	21	WPA→WEP	3	0.32	W
9	Open→WPA	31	3.31	B	22	Mixed→WEP	3	0.32	W
10	WPA→Mixed	30	3.21	N	23	WEP→WEP	2	0.20	N
11	WPA2→WPA	26	2.78	W	24	WEP→WPA	2	0.20	B
12	WPA2→Open	18	1.92	W	25	Open→WEP	2	0.20	N
13	WEP→WPA2	17	1.82	B		Total	936	100	

The first analysis shows that a total of 936 changes of configurations were made. Further analysis shows that only some changes can be qualified as improvements in configurations. For this research, those changes are defined as: Mixed→WPA2, Open→Mixed, Open→WPA2, WPA2→WPA2, WPA→WPA2, Open→WPA, WEP→WPA2, WEP→Mixed and WEP→WPA. According to this definition, only 302 access points have been configured to match better security level, which makes only 32.26% of changed APs, and only 2.94% of all analyzed access points (10,285). In Table 7 in the column Ch, changes qualified as changes to better are marked with B, changes to worse are marked with W and with neutral impact on higher security with N (none).

The second criterion is defined by considering changes to WPS configuration. Only 4 categories are defined here: noWPS→WPS, WPS→WPS, noWPS→noWPS, and WPS→noWPS. Again, the results are similar. Only 344 or 36.75% of the changed APs are scanned with improved settings, which is only 3.34% compared to the total number of analyzed APs. Only the transition from WPS to noWPS is considered as a transition to a higher security level.

The third criterion defines 228 different security groups. Those groups are more detailed compared to 5 groups given in Table 7. The most frequent changes between groups (15 in total) are presented in Table 8. As in Table 7, changes in Table 8 in column Ch are marked with B for changes qualified as better, with W for changes qualified as worse and with N for changes without improvement.

According to these analyses 652 detailed security groups were improved (a wide range of changes to betterment was considered, even the very small improvements), which makes only 69.66 % of changed APs, and only 6.34% of all scanned and analyzed networks.

Table 8

The detailed types of security setting changes and their percent in the total number of analyzed networks

No.	Detailed Security Group	No. of APs	(%)	Ch
1	Mixed_TKIP_CCMP_PSK_WPS→Mixed_TKIP_CCMP_PSK_noWPS	284	30.34	B
2	Mixed_CCMP_PSK_noWPS→WPA_CCMP_PSK_noWPS	18	1.92	W
3	Open_noWPS→WPA2_CCMP_PSK_noWPS	18	1.92	B
4	WPA_TKIP_PSK_noWPS→WPA2_TKIP_PSK_noWPS	16	1.71	B
5	Open_noWPS→WPA2_TKIP_PSK_noWPS	15	1.6	B
6	Open_noWPS→WPA_TKIP_PSK_noWPS	15	1.6	B
7	Mixed_TKIP_CCMP_PSK_noWPS→Mixed_TKIP_CCMP_PSK_WPS	14	1.5	W
8	Open_noWPS→Mixed_TKIP_CCMP_PSK_preauth_noWPS	12	1.28	B
9	Open_WPS→Mixed_TKIP_CCMP_PSK_WPS	12	1.28	B
10	WPA_TKIP_PSK_noWPS→Open_noWPS	11	1.18	W
11	Open_noWPS→WPA_CCMP_PSK_noWPS	11	1.18	B
12	Mixed_TKIP_CCMP_PSK_WPS→Mixed_CCMP_PSK_WPS	10	1.07	B
13	WPA2_CCMP_PSK_noWPS→WPA_CCMP_PSK_noWPS	10	1.07	W
14	Open_noWPS→Mixed_TKIP_PSK_noWPS	9	0.96	B
15	WPA2_CCMP_PSK_WPS→Mixed_CCMP_PSK_WPS	8	0.85	W

In all three cases, the percentage of changes to a higher level of security ranges from 2.94% to 6.34%. The percentage is given in comparison with all scanned networks discovered more than once for the period of 3 years. These results definitely confirm that, once the access point is installed and wireless network is configured, there is less than a 10% chance that the system will be configured again. The chances that the access point configuration will lead to better security settings are even smaller, since only 2.94 to 6.34 percent of configuration changes actually raise the security level.

4.3 Limitations of the Study

Certain limitations were identified during this study. The research lacks the second scan in the city of Budapest in the period after 1-2 years. This second scan will allow analysis of the configuration change rate for Budapest, as well as comparison of this wireless security aspect between Budapest and Belgrade.

Careful planning for the Wardriving routes is also missing in this research. For example, by distinguishing tourist, business and residential areas, this research can enable carrying out a more accurate and more productive analysis, allowing deeper understanding of problems and leading to more suitable solutions for specific areas of human living. The separate analytics of enlisted areas will also provide a good starting point for further analysis, and possible inclusion of sociologists, urban and economic experts in multidisciplinary research projects.

Conclusions

This paper presents the results of the wireless security circumstances in Budapest and Belgrade, by using a methodology based on Wardriving. The research was conducted from November 2013 to February 2016. The first part of the research is from 2015/2016 period and it is used for comparison of wireless security in Budapest and Belgrade. The total of 14,287 networks in Budapest and 18,070 networks in Belgrade were discovered during this period.

The wireless security situation in the cities of Budapest and Belgrade shows a lot of potential for improvement. The highest level of security (WPA2 with CCMP) is not present in a desired range. The situation in Belgrade is better regarding this parameter as 44.46% of the networks use CCMP in WPA, WPA2 or Mixed-mode, compared to 28.49% in Budapest. It still accounts for less than 50% of all networks and this should be improved. The situation in Belgrade is also better comparing the WPS features, since 26.53% networks in Belgrade and 32.44% networks in Budapest use this vulnerable feature. In both cities, the situation has to be significantly improved by reducing the number of WPS enabled access points.

The percentage of Open and WEP security access points is similar in both capital cities. The only difference is that in Belgrade there is a higher percentage of WPA-Personal networks, 7.97% higher than in Budapest. On the contrary, the percentage of Mixed-mode networks in Budapest is 9.61% higher than in Belgrade. This gives a slightly better security result in favor of Budapest while the total percentage of the most secured networks (WPA2-Personal and WPA2-Enterprise) is similar in Budapest (34.5%) and Belgrade (34.83%).

The second phase of research compared Belgrade Wardriving statistics for period 2013/2014 and period 2015/2016. Findings of this research clearly point out that the wireless security situation is not perfect, but it has changed through time. This conclusion can be made by comparing results in Belgrade in periods 2013/2014

and 2015/2016. The improvement in the security situation was made by deploying new and cost-effective access points over the time, where the newly deployed access points were configured with more expertise and attention. The configuration of once deployed access points changes very rarely (ranging from 2.94% to 6.34%).

The final conclusion is that the best way for raising the overall security of wireless networks is to raise the awareness of wireless users and wireless network providers regarding the threats, vulnerabilities and best methods for security settings.

In future work the presented methodology for security change analysis, can be improved, by making changes in the software for security analysis and reporting. For example, development of more detailed criteria for rating improvements of security changes can also be useful, leading to creation of better policies in deploying new APs, as well as, finding the main reasons for the less secure APs settings. In addition, the discussed limitations of the study open challenging directions for further research through considering different aspects of human living and composing multi-disciplinary research teams.

References

- [1] Chris Hurley, Frank Thorton, Michael Puchol, Russ Rogers: *WarDriving: Drive, Detect, Defend: A Guide to Wireless Security*, Syngress Publishing, Inc., Rockland, USA, 2004
- [2] Hira Sathu: *Wardriving: technical and legal context*. In *Proceedings of the 5th WSEAS international conference on Telecommunications and informatics (TELE-INFO'06)*, Stevens Point, Wisconsin, USA, pp. 162-167, 2006
- [3] Tsui, A. W. T.; Wei-Cheng Lin; Wei-Ju Chen; Polly Huang; Hao-Hua Chu: *Accuracy Performance Analysis between War Driving and War Walking in Metropolitan Wi-Fi Localization*, *IEEE Transactions on Mobile Computing*, Vol. 9, No. 11, pp. 1551-1562, Nov. 2010, doi: 10.1109/TMC.2010.121
- [4] Sagers, G.; Hosack, B.; Rowley, R. J.; Twitchell, D.; Nagaraj, R.: *Where's the Security in WiFi? An Argument for Industry Awareness*, *Proceedings of 48th Hawaii International Conference on System Sciences (HICSS)*, pp. 5453-5461, 5-8 January, 2015, doi: 10.1109/HICSS.2015.641
- [5] Said, H.; Guimaraes, M.; Al Mutawa, N.; Al Awadhi, I.: *Forensics and War-Driving on Unsecured Wireless Network*, *Proceedings of International Conference for Internet Technology and Secured Transactions (ICITST)*, pp. 19-24, 11-14 December 2011
- [6] Issac, B.; Jacob, S. M.; Mohammed, L. A.: *The Art of War Driving and Security Threats - a Malaysian Case Study*, *Networks, 2005*. Jointly held with the 2005 IEEE 7th Malaysia International Conference on

- Communication, 2005 13th IEEE International Conference on , Vol. 1, No., pp. 6-pp., 16-18 Nov. 2005
- [7] Díaz, Javier F.; Robles, Matías; Venosa, Paula; Macía, Nicolás; Vodopivec, Germán: Wardriving: an Experience in the City of La Plata, Proceedings of XIV Congreso Argentino de Ciencias de la Computación CACIC 2008, October 8-10 2008
- [8] Lucas Jacob, Damien Hutchinson, Jemal Abawajy: Wi-Fi Security: Wireless with Confidence, in Proceedings of the 4th Australian Security and Intelligence Conference, pp. 88-06, 5th-7th December, Perth, Australia, 2011
- [9] Niloufer Selvadurai, Md. Rizwanul Islam, Peter Gillies: Unauthorised Access to Wireless Local Area Networks: The Limitations of the Present Australian laws, *Computer Law & Security Review*, Vol. 25, Issue 6, November 2009, pp. 536-542, ISSN 0267-3649, <http://dx.doi.org/10.1016/j.clsr.2009.09.003>
- [10] Nisbet, A.: A Tale of Four Cities: Wireless Security & Growth in New Zealand, Proceedings of International Conference on Computing, Networking and Communications (ICNC), pp. 1167-1171, January 30 2012-February 2 2012, doi: 10.1109/ICCNC.2012.6167391
- [11] Nisbet, A.: A 2013 Study of Wireless Network Security in New Zealand: Are We There Yet?!, in the Proceedings of the 11th Australian Information Security Management Conference, Perth, Western Australia, 2nd-4th December, 2013
- [12] Redzepagic, J.; Studen, D.; Gavranic, V.; Tekovic, A.: Security of End User Wireless Networks in Zagreb Area, Proceedings of 38th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), pp. 1613-1616, 25-29 May, 2015, doi: 10.1109/MIPRO.2015.7160529
- [13] Davor Janić, Dragan Peraković, Vladimir Vukelić: An Analysis of Wireless Network Security in the City of Zagreb and Zagreb and Karlovac County, In Proceedings of 7th International Conference on Ports and Waterways - POWA 2012, pp. 216-223
- [14] Ionescu, V.; Smaranda, F.; Sima, I.; Diaconu, A.: Current Status of the Wireless Local Area Networks in Romania, Proceedings of 11th International Conference (RoEduNet) in Roedunet, pp. 1-4, 17-19 January 2013, doi: 10.1109/RoEduNet.2013.6511752
- [15] Stefan Jäger, Dalibor Dobrilovic: Tools for WLAN IEEE 802.11 Security Assessment, In proceedings of 2nd International conference of Applied Internet and Information Technologies ICAIT 2013, pp. 56-62, Zrenjanin, Serbia, 25th October, 2013
- [16] Dalibor Dobrilovic, Borislav Odadzic, Zeljko Stojanov, Zlatko Covic: Approach in IEEE 802.11 Security Analytics and its Integration in

- University Curricula, in Proceedings of the 3rd regional conference Mechatronics in Practice and Education – MECHEdu 2015, pp. 41-46, December 5-6, Subotica, Serbia, 2013
- [17] Dušan Švenda, Miroslav Djordjević: Mapping of IEEE 802.11 Wireless Networks in Belgrade (In Serbian: Mapiranje IEEE 802.11 bežičnih mreža u Beogradu), 18. Telecommunication forum TELFOR 2010 Serbia, Belgrade, November 23-25, 2010
- [18] Saša Adamović, Marko Šarac, Dalibor Radovanović: Wireless Network IEEE 802.11 Security Analysis on the area of city of Belgrade (In Serbian: Analiza sigurnosti bežičnih mreža IEEE 802.11 na teritoriji grada Beograda, INFOTEH-JAHORINA Vol. 10, Ref. B-III-1, pp. 191-194, Bosnia and Herzegovina, Martch 2011
- [19] Dalibor Dobrilović, Borislav Odadžić: Comparative Indicators of Security of Wireless IEEE 802.11 Networks in Parts of Serbia in Comparison to the Region and the World (In Serbian), Informaciona bezbednost 2013, 5. June, Belgrade, Serbia 2013
- [20] Durmus Ali Avci, Kemal Hajdarevic: Security of Wi-Fi Networks, In IBU Journal of Science and Technology, Vol. 2, No. 1, pp. 133-144, 25 Sep 2014
- [21] Pranav S. Ambavkar, Pranit U. Patil, Dr.B.B.Meshram, Pamu Kumar Swamy: WPA Exploitation in The World of Wireless Network, In International Journal of Advanced Research in Computer Engineering & Technology, Vol. 1, Issue 4, June 2012
- [22] David D. Coleman, David A. Westcott, Bryan E. Harkins, Shawn M. Jackman: CWSP® Certified Wireless Security Professional Official - Study Guide Study Guide, Wiley Publishing, Inc., Indianapolis, USA, 2010
- [23] Gary A. Donahue: Network Warrior, O'Reilly Media, Inc., Sebastopol, USA, 2011
- [24] Mark Ciampa: CWNA Guide to Wireless LANs, Course Technology, Cengage Learning, USA 2013
- [25] Johnny Cache, Joshua Wright, Vincent Liu, Hacking exposed™ wireless: wireless security secrets & solutions, 2nd, The McGraw-Hill Companies, 2010
- [26] Eric Cole, Ronald Krutz, James W. Conley: Network Security Bible, Wiley Publishing, Inc., Indiana, USA, 2005
- [27] Randy Weaver, Dawn Weaver, Dean Farwood: Guide to Network Defense and Countermeasures, 3rd, Course Technology, Cengage Learning, USA, 2014
- [28] Richard Deal: CCNA® Cisco® Certified Network Associate Study Guide (Exam 640-802), McGraw-Hill Companies, 2008

- [29] C. Hurley, R. Rogers, F. Thompson, D. Connelly, B. Baker: *WarDriving and Wireless Penetration Testing*, Syngress Publishing, Inc. Rockland, USA, 2007
- [30] Haines, B., Thornton, F.: *Kismet Hacking*, Syngress Publishing, 2008
- [31] Wigle - <http://www.wigle.net>, seen on 2016.03.12
- [32] Stefan Jäger: *Wardriving – die unterschätzte Gefahr*, FIF-Kommunikation 4/15, "Cybercrime" (in German), 2015
- [33] <http://standards-oui.ieee.org/oui.txt>, Public MAC-list of vendors, seen on 2016.03.12