EAI Endorsed Transactions
on Security and Safety

Research Article EAI.EU

Overview of Romania 802.11 Wireless Security & Statistics

Cristian Liviu Leca[1,*]

[1]Military Technical Academy, 39-49 George Cosbuc Ave., Sector 5, 050141, Bucharest, RO

Abstract

This paper presents a study of wireless network security and statistics in Romania aimed at raising public awareness on security issues and highlighting the prevalence of known vulnerabilities in commercial equipment. The data used for the study consist of wireless network broadcast data acquisitioned by the technique of war-driving. In order to ensure a thorough overview, the data collected includes more than 100000 unique wireless networks gathered in Bucharest, major urban areas and the surrounding rural areas. The results of the study cover security protocol usage, the percentage in which known vulnerabilities are still deployed in wireless networks and statistics regarding channel and band usage, common SSIDs in Romania, top equipment manufacturers and the situation of provider wireless access points. The study also shows that provider wireless access points on average offer better security than private networks.

Received on 28 January 2017; accepted on 20 April 2017; published on 28 December 2017

Keywords: wireless security, vulnerabilities, Romania, war-driving

doi:10.4108/eai.28-12-2017.153518

1. Introduction

Personal wireless networks have become increasingly popular ever since smartphones and related mobile devices have penetrated daily life. The 802.11 set of specifications has backed up the rapid expansion of wireless networks. The falling costs and high availability of both wireless equipment and that of broadband internet [1] in Romania has also enabled the growth in number of wireless networks.

Users in Romania can choose between using a cable internet broadband connection and setting up their wireless network with off the shelf wireless access points or they can choose to buy wireless network access as a service from an internet provider which will supply the customer with a ready-to-go branded wireless access point connected to cable or mobile internet connection.

Although 802.11 specifications have enabled the rapid growth of personal wireless networks, the security protocols and technologies have shown weaknesses that can be exploited in order to gain unauthorized access to the network and the encrypted communication data. Although weaknesses and exploits have been made known to the public, users often choose to ignore security recommendations. The use of outdated security protocols or the failure to address weak spots in their access points creates security risks for unaware users.

The data for the study was gathered during the months of October and November 2016 by collecting wireless network broadcasted data in Bucharest completed by ten major urban areas and their surrounding rural areas. The data set contains approximately 100000 unique wireless access points and was gathered by driving around 3000 km in Romania.

The data collected for the study is compared with world data obtained from the Wireless Geolocation Engine [2]. Data from a previous study [3] published in 2012 is used in order to determine the evolution of wireless security in Romania. We also focus on highlighting weaknesses that allow well-known attacks and exploits to succeed by analyzing statistics regarding their existence in personal wireless networks in Romania. Because these exploits are well known, patching them up has become an easy job for most users. As long as users are not aware of the security concerns for running their own private network they

[*]Corresponding author. Email: cristian.liviu.leca@gmail.com

will continue to make bad security choices, for example: choosing the WEP protocol for authentication or using the default SSID of the equipment. By highlighting these weaknesses and showing their wide existence in wireless networks in Romania, we hope to raise the public awareness on wireless security and make users take better decisions when installing private networks, not only in Romania for users worldwide. The study also compares provider wireless networks and their security with privately set up wireless networks and shows that the first offer increased security protection, which means that low-skilled users can fare better on security by choosing provider services.

Personal wireless networks in Romania are analyzed using the following criteria: percentage of unencrypted wireless networks in Romania, types of encryption in use, existence of WPS (Wi-Fi Protected Setup) feature, most common network ESSID (Extended Service Set Identification), band and channel usage, provider wireless networks security and top wireless access point manufacturers sold in Romania. The results are compared between the Bucharest area, the major urban areas and the rural areas scanned in the process.

Previous work in the field includes a study of computer networks done in Romania in 2012 [3] and similar studies done in other parts of the world [4–11].

Reference [3] have gathered a database consisting of approximately 38000 access points gathered through wardriving in Romania. Their results show that rural areas adopted WPA security directly when compared to urban areas that have made the transition from WEP to WPA and still use legacy equipment. They also show that rural areas have more open networks and less security when compared to urban areas.

Reference [7] analyze a total of 29250 networks in Serbia, while other articles use a database with less than 10000 AP [4, 6, 12]

The work in [13] is also concerned with highlighting known vulnerabilities and their spread. The authors of [13] divide the collected data into commercial or residential areas, similar to our urban/rural division. The goal of the study is to collect statistically significant data from representative areas of Romania that would ensure an objective overview of the wireless security situation in Romania. The research questions were aimed at:

- drawing a comparison between wireless security in Romania and the rest of the world;
- determining the existence of an improvement of the wireless security in Romania;
- highlighting differences between urban and rural areas;
- highlighting the existence of known vulnerabilities;
- analyzing the security of provider wireless networks.

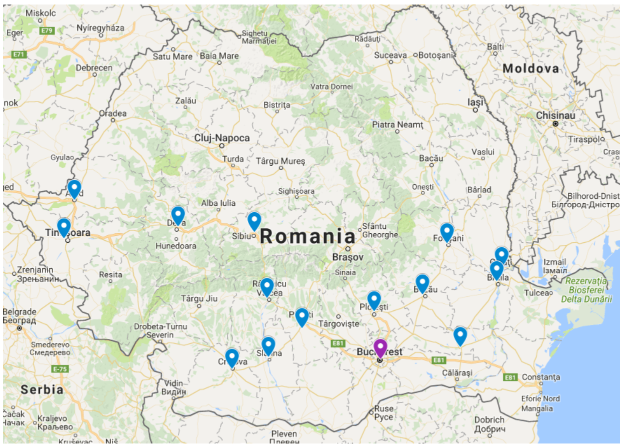

Figure 1. Areas scanned

The data gathering process ensured a large data set with statistical significance, that allows a deep insight into wireless network statistics in Romania. The study shows that wireless network security has improved significantly in Romania when compared to the results of a previous study in 2012. Wireless security statistics bear similarities to that resulting from worldwide data gathered by the Wigle project [2]. Particularly, the study presents results regarding the spread of known vulnerabilities in wireless networks. Results also show that provider wireless networks have increased security and a larger WPA Enterprise deployment percentage when compared to private owned networks.

2. Methodology for data gathering and analysis

Data collection was enabled by the use of the Wireless Geolocation Engine (Wigle) [2] android application. The Wigle project is aimed at collecting information about wireless hotspots from around the world by the process of crowd-sourcing. The goal of the project is to create awareness for the security needs of running wireless networks. The project allows users a limited number of queries for the location of an SSID or MAC address which causes privacy concerns. Wigle offers full database access under a commercial license.

The Wigle android application will log visible wireless networks and the geographic coordinates of the point where the scanning took place at a specified interval. The wireless information gathering process was achieved by wardriving [14] and warwalking [15]. Wardriving is defined in [16] as the act of searching for Wi-fi wireless networks by a person in a moving vehicle using a portable computer, smartphone or personal digital assistant.

The data was collected over the course of October and November 2016. The gathering process was aimed at

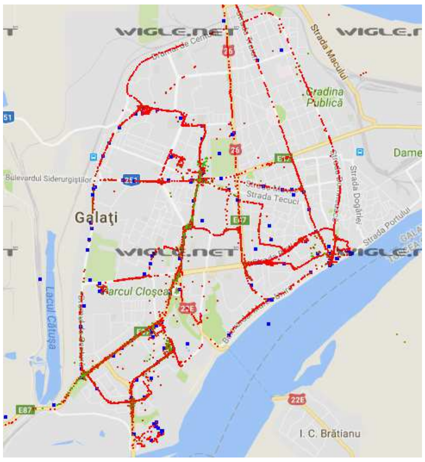

Figure 2. Wardrive results in Galati

collecting data from all Romania's major regions, while also covering both urban and rural areas as shown in figure 1.

The resulting dataset contains approximately 100000 distinct wireless networks of which: 55% were collected in Bucharest, 31% were collected in major urban areas and 14% were collected in the neighboring rural areas. Fig.1 presents the major urban areas that were sampled in the data collection process with blue pins while Bucharest is marked with a purple pin.

Figure 2 presents the results of war-driving in the city of Galati by depicting scanned wireless networks with colors between green and red (green indicates more measurements of the same network).

The resulting logs from all the devices running the Wigle app were merged into a single PostgreSQL database. The records for each distinct network were then spatialized according to the logged GPS coordinates. The aim of the spatialize operation was to allow for precise selection of the networks located in Bucharest or in urban areas, while the networks belonging to the rural areas where filtered by an inverse selection operation.

The logs were completed with information regarding the 802.11 channel number according to the logged frequency. We also included information about the manufacturer of the wireless access point. Manufacturer information is available freely from the Wireshark project [17] and the IEEE Standards Association [18].

The statistics were generated using PostgreSQL queries, that were plotted or inserted into tables.

The data was analyzed primarily based on security protocol usage. The security protocols in use for 802.11 wireless networks are WEP, WPA, WPA2 and WPA2-Enterprise. Using an open access policy with no security is highly discouraged as it offers ill-intentioned users complete access to the network and the communications inside.

Table 1. Open, WEP, WPA and mixed networks statistics for October and November 2016

Area	World	Romania	Bucharest	Urban	Rural
Open Networks	2%	6%	6%	6%	11%
WEP	5%	3%	3%	2%	3%
WPA only	7%	5%	4%	6%	8%
WPA2 or mixed	86%	86%	87%	86%	78%

WEP security has been outdated since the Wi-Fi Alliance announced WPA in 2003. The WEP protocol is easily defeated in minutes with freely available software tools [19] and commercial hardware, which makes it useless against attacks.

The WPA protocol was designed to be easily implemented on hardware running WEP and offer superior protection. WPA has shown to be vulnerable allowing attackers to decrypt short packets. Publicized attacks are not yet able to recover the password and so attackers have no access to the network.

The WPA2 protocol was introduced in 2004 to improve on WPA performances. WPA2 offers satisfactory security for the PSK (pre-shared key) authentication method but does not offer any protection or forward secrecy once an attacker manages to obtain the password. Methods that attackers use to gain access to the password include guessing a weak password using dictionary attacks or employing social engineering tactics.

Many devices, by default, offer both WPA and WPA2 security for compatibility with client devices.

WPA2 - Enterprise also known as WPA-802.1x is designed to offer security at enterprise level for businesses or Wi-Fi mobile network offload.

3. Results on security protocol usage

In this section, we present results of the study concerning wireless security. Results are compared with world data and with a previous study which gave an overview of wireless security in Romania in 2012 [3].

Available data from [2] offers statistics about Open, WEP encrypted, WPA and mixed WPA2 (WPA & WPA2 or WPA2 only) security for Wi-Fi networks scanned during the same interval as our data gathering process. We compare this information with the results of our study in Table 1.

The results in Table 1 highlight a higher percentage of open access networks in Romania compared to world statistics. The greatest percentage of open is seen in rural areas at 11%. In the case of public organizations that offer open access, this is not really an issue because even if using WPA encryption an attacker can decrypt all traffic on the network by using the provided key.

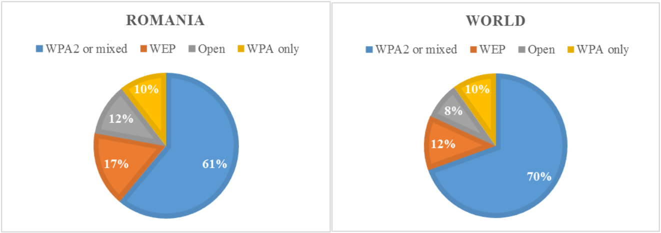

Figure 3. All-time data comparison between Romania security and World security

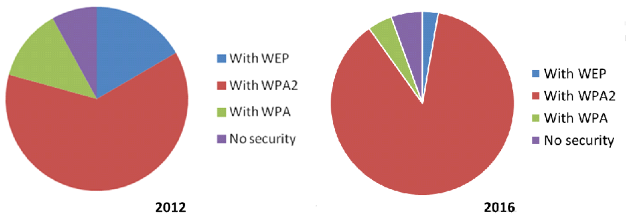

Figure 4. Bucharest area wireless security overview in 2012 vs 2016

The use of WEP encryption shows better results in Romania when compared to world data. Many of existing WEP networks use the protocol in order to ensure backward compatibility with older client equipment.

The WPA and mixed security are on average with world statistics showing the public understanding of the need for wireless security.

We also compare historic all-time data regarding Romania wireless security with world data in fig. 3.

The results concerning WPA2 or mixed security show that wireless security in Romania has improved with a fast pace. The growth is observed by comparing all-time data with the present situation. The security situation in Romania is level with present world levels as shown in Table 1.

The evolution of the security situation can be traced when comparing our data with data from a previous study in 2012 concerning the Bucharest area [3] as shown in Fig. 4.

By comparing the results in 2012 with the results of our study we see a major improvement in wireless security over the course of 4 years. This is reflected in the increase of WPA2 secured networks which closes 90% for the Bucharest area.

The use of open access has also decreased as shown in Table 2.

The results in Table 2 can be explained by the fact that urban and rural area users have increased their security awareness and gave up on allowing open access to their networks. The situation in Bucharest went largely unchanged due to two reasons: first - the high number of open networks belonging to businesses and second - users were already aware of security needs for a longer time.

Table 2. Open access networks in 2012 vs 2016

Year	Bucharest	Urban areas	Rural areas
2012	8%	14%	22%
2016	6%	6%	11%

Table 3. Detailed capabilities of WLAN in Romania

No.	Capabilities	Count
1	[WPA2-PSK-CCMP][WPS][ESS]	12651
2	[WPA2-PSK-CCMP][ESS]	10268
3	[WPA-PSK-CCMP][WPA2-PSK-CCMP][WPS][ESS]	9572
4	[WPA-PSK-CCMP+TKIP][WPA2-PSK-CCMP+TKIP][WPS][ESS]	6910
5	[WPA-PSK-CCMP][WPA2-PSK-CCMP][ESS]	6327
6	[WPA-PSK-CCMP+TKIP][WPA2-PSK-CCMP+TKIP][ESS][BLE]	5571
7	[ESS]	4120
8	[WPA-PSK-CCMP+TKIP][WPA2-PSK-CCMP+TKIP][WPS][ESS][BLE]	4013
9	[WPA-PSK-CCMP+TKIP][WPA2-PSK-CCMP+TKIP][ESS]	3745
10	[WPA2-EAP-CCMP+TKIP][ESS][BLE]	3667
11	[WPA2-PSK-CCMP][WPS][ESS][BLE]	3535
12	[WPA2-PSK-CCMP][ESS][BLE]	3213
13	[WPA-PSK-CCMP][ESS]	2886
14	[WPA2-PSK-CCMP+TKIP][WPS][ESS]	2014
15	[WPA2-EAP-CCMP][ESS]	1666
16	[WPA-PSK-TKIP][WPA2-PSK-CCMP][WPS][ESS]	1550
17	[WEP][ESS]	1443
18	[WPA-EAP-CCMP+TKIP][WPA2-EAP-CCMP+TKIP][ESS]	1195
19	[WPA2-PSK-CCMP+TKIP][ESS]	1190
20	[WPA-PSK-TKIP][ESS]	1126

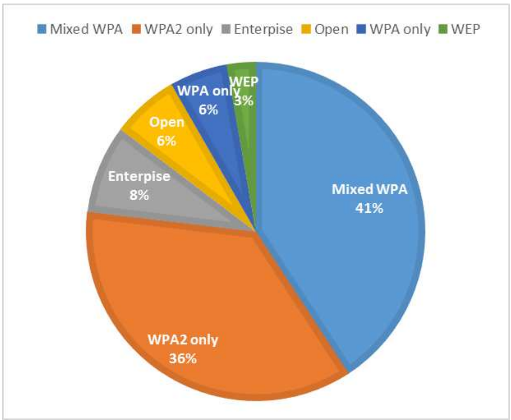

Figure 5. Analysis of Table 3 security capabilities

The gathered data also offers a detailed insight into different security setups. Table 3 presents the top 20 most used security capabilities for wireless networks in Romania. The top 20 capabilities cover 89% of wireless networks in the country while the others cover the remaining 11% of networks.

Data in Table 3 can be resumed by analyzing Enterprise WPA2 only, mixed WPA, WPA only, WEP and open networks as presented in Fig. 5.

Table 4. WPS availability in Romanian wireless networks

Area	Romania	Bucharest	Urban areas	Rural areas
Percentage	45%	42%	51%	40%

Enterprise secured wireless networks represent 8% of all scanned networks, of which 82% are WPA2-Enterprise, 17% Mixed WPA-Enterprise and 1% WPA-Enterprise. The use of EAP-SIM access points is under the threshold of 1% which shows that mobile network operators are only in the beginnings of the process of implementing mobile data offload to 802.11 networks.

4. Security vulnerabilities and their extent

This part of the study highlights the existence and scale of vulnerabilities in Wi-Fi networks in Romania. The aim is to raise awareness and to encourage users to avoid using these practices or security flaws in the configuration of their wireless network.

The most concerning vulnerability is the usage of the Wi-Fi Protected Setup protocol. WPS has been shown to be vulnerable to online [19] and offline brute force attacks while also depending heavily on physical security for all implementations (PIN labeled on the device, pushbutton, near field or USB transfer). Online brute force attacks can recover the WPA2 key in under four hours [19] with no notification to the user that an attack is in place. The attacker gets full access inside the network despite best efforts by the users to use WPA2 security. WPS statistics are presented in Table 4.

The use of the WPS feature is not entirely insecure due to various security patches introduced by manufacturers in the original implementation, but proving a WPS implementation is secure is difficult for the majority of users. Resulting statistics show that 45% of networks in Romania have WPS enabled. Taking into account the available exploits and the difficulties in proving a WPS implementation secure we consider this to be the major vulnerability of Romanian wireless networks.

The breaking of the WEP protocol meant that old hardware was rendered useless unless a security protocol was designed that was able to use the same resources as WEP. The result was the Temporal Key Integrity Protocol implemented as WPA-TKIP [20]. The WPA-TKIP protocol has seen packet spoofing and limited packet decryption attacks which can compromise the confidentiality of the network traffic but will not grant the attacker the access key inside. Fortunately, around 4% of networks in Romania still use this security protocol in WPA only or mixed configurations, resulting in a low spread of the WPA-TKIP vulnerability.

Table 5. Top 20 most common SSIDs in use in Romania

No.	SSID	Percentage (%)
1	UPC Wi-Free	1223151
2	ASUS	0.799311363
3	dlink	0.777791441
4	Telekom Fon	0.558493196
5	netis	0.450893589
6	AndroidAP	0.392482374
7	linksys	0.333046401
8	Acasa	0.287957042
9	TP-LINK	0.286932284
10	Home	0.235694376
11	WirelessNet	0.186505985
12	EDIMAX	0.177283161
13	alex	0.168060338
14	digi	0.16703558
15	DIGI WIFI 2.4 Web Login	0.148589933
16	Tenda	0.147565175
17	DIGI WIFI 2.4 Direct Login	0.139367109
18	default	0.131169044
19	andrei	0.121946221
20	dlink_DWR-921	0.120921463

A recently published vulnerability [21] raises concerns about the security of mobile network provider access points and the use of Voice over Wi-Fi. Mobile network operators are implementing the offloading of data and voice traffic from the mobile RAN (radio access networks) to 802.11 access points using the Enterprise WPA-EAP-SIM or WPA-EAP-AKA authentication methods.

The vulnerabilities presented in reference [21] offer an attacker access to information about the target's location and that of the IMSI of the SIM card inside the mobile device. The vulnerabilities are based on the EAP-SIM and EAP-AKA protocol which sends identity information (IMSI number) in plain. Enterprise EAP-SIM network setups represent under 1% of Enterprise networks in Romania which does not cause great concerns regarding this vulnerability yet.

Using the default SSID [22] for the wireless access point is discouraged by security experts as it offers hints to an attacker regarding the equipment manufacturer or internet provider. This information can then be exploited in order to use default credentials on forcing access to the network. Also, the use of personal information in naming the SSID favors attacks based on social engineering or facilitates the generation of passwords for more precise dictionary attacks. Our study reveals that networks using the top 20 more common SSIDs in Romania represent 12% of the total

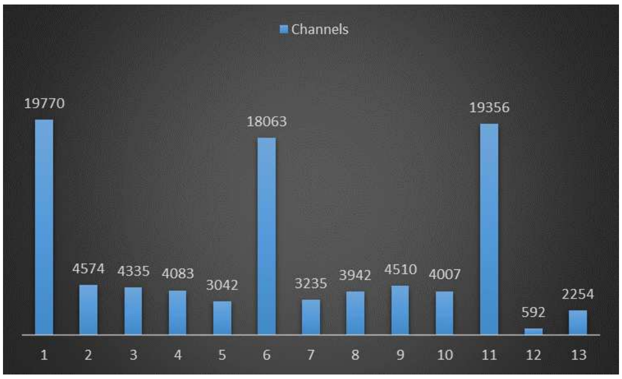

Figure 6. Channel usage in the 2.4 GHz band

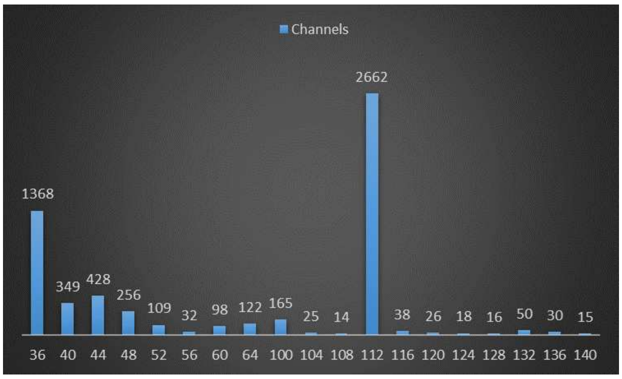

Figure 7. Channel usage in the 5 GHz band

number of networks. The top 20 SSIDs are shown in Table 5.

5. Detailed wireless network statistics

5.1. Band & Channel usage

The Wigle Android App also allows gathering information regarding the channel in use by a wireless network. This allowed us to compile statistics abound channel and band use in Romania. The 802.11 bands in use in Romania are the 2.4 GHz (802.11 b/g/n) and the 5 GHz (a/h/j/n/ac) bands. The devices used for war-driving were compatible with both bands. The results show that 94% of access points use the 2.4 GHz band while the rest of 6% function in the 5 GHz band. We take notice that these results can be biased by the fact that the 5 GHz band is affected by higher atmospheric and building attenuation resulting in less observed networks.

The use of the 2.4 GHz band generally follows the distribution of non-overlapping 802.11 channels as shown in Fig. 6. Using non-overlapping channels guarantees minimum interference between access points functioning in close proximity.

The 5 GHz band usage is presented in Fig. 7.

The 5 GHz band is subject to transmit power control and dynamic frequency selection regulations with the aim to reduce interference between neighboring networks. Channels 36 to 64 are subject to a restriction for outdoor usage resulting in a lower usage. Channel 112 is by far the preferred channel in the 5 GHz band due to default software settings of the equipment.

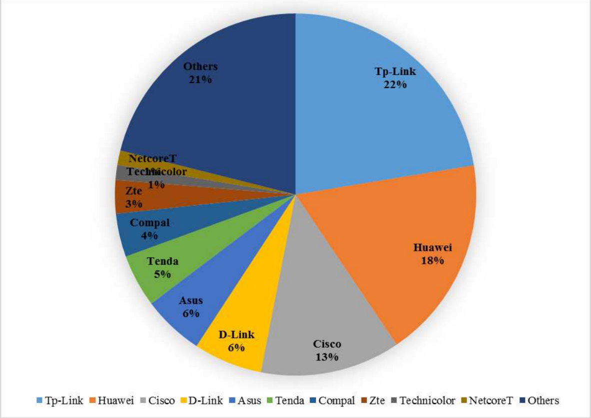

Figure 8. Top equipment manufacturers on sale in Romania

Table 6. Provider wireless networks percentage analysis

Area	Romania	Bucharest	Urban areas	Rural areas
Provider	30%	34%	24%	32%
Private	70%	66%	76%	68%

5.2. Manufacturer

By analyzing each access point's MAC addresses by its OUI (Organizationally Unique Identifier) we were able to determine the top equipment vendors in Romania. The information regarding OUIs was compiled from the databases offered by the Wireshark Project [17] and the IEEE [18].

The top 10 equipment manufacturers in Romania are plotted by their percentage in Fig. 8.

5.3. Service providers

Wireless network access is sold as a service in Romania by different internet providers. This is done by offering the client both internet access by cable or 3G/4G modem and the hardware access point that is used for wireless internet access. The providers broadcast their brand by making it a part of the SSID belonging to the leased equipment. Users are generally not able to completely remove the branding from the SSID. Instead, they can add their desired name as a suffix to the brand. This makes it easy to gather statistics about wireless internet providers in the country which show that 30% of wireless networks scanned belong to an internet provider as depicted in Table 6.

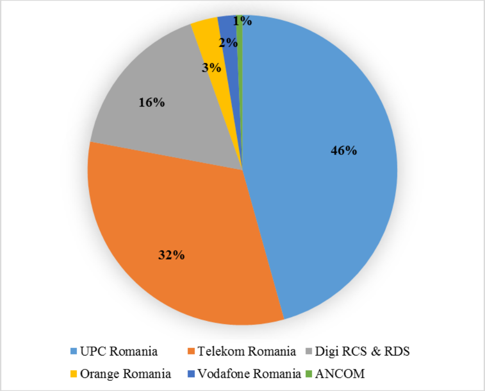

Figure 9. Provider wireless networks

Table 7. Provider wireless networks percentage analysis

	Mixed WPA	WPA2 only	Enterprise	Open	WPA only	WEP	WPS
Provider	33%	33%	25%	3%	1%	4%	31%
Private	45%	37%	1%	7%	7%	2%	66%

Moreover, we provide an analysis of the share each provider has in our data collection in Fig. 9.

Provider Wi-Fi security situation is better than that of private networks. This is reflected in Table 7.

Table 7 shows that enterprise security levels are hard for private users to implement with a percentage of around 1% of the networks. Providers on average offer better security with lower percentages of open, WPA only and of the WPS feature. Providers also offer the majority of the enterprise secured networks in Romania. WEP networks are used with a higher percentage by providers which poses a high security risk as mentioned before.

6. Conclusions

This article presents an overview of the wireless security situation in Romania. The data used in the study is statistically significant as it consists of more than 100000 unique records of wireless networks in Romania gathered in all three major regions of the country.

The study is aimed at increasing public awareness on wireless network security and to highlight existing vulnerabilities in personal networks that are simple to avoid. We compare the results concerning wireless security with world data and with results of a previous study in 2012, and we notice that the wireless security situation has improved in Romania consequently being now at level with world statistics. The increase of wireless security in recent years is also observed by similar work in the field [4, 6].

We also publish results on most common SSIDs in use, channel and band usage, equipment manufacturers, wireless internet providers. The security situation of provider wireless networks is shown to be significantly better than that of private networks. This prompts us to advise users with no technical skills to opt for provider services rather than setting up their own network, as this operation can lead to the usage of a vulnerable security setting or practice.

Further work should be concentrated on expanding the data set in order to ensure greater statistical significance. If data was to be collected on a permanent basis, the resulting database could be used to help service providers analyze market opportunities while also advertising the fact that they offer enhanced security while compared to privately setup networks. The data set could also be used to analyze the distribution of 802.11 protocols (a,b,g,n,ac).

7. Acknowledgements

This work has benefitted from the usage of the Wireless Geolocation Android App [2].

8. Copyright statement

References

[1] H. A., "The five countries with the fastest internet speeds in the world, nomad capitalist," Nomad Capitalist, online, 2013, available at http://nomadcapitalist.com/2013/12/01/top-5-countries-fastest-internet-speeds-world/.

[2] W. G. Engine. (2017) Wigle. [Online]. Available: https://wigle.net/

[3] V. Ionescu, F. Smaranda, I. Sima, and A.-V. Diaconu, "Current status of the wireless local area networks in romania," in *Roedunet International Conference (RoEduNet), 2013 11th*. IEEE, 2013, pp. 1–4.

[4] A. Sebbar, S. Boulahya, G. Mezzour, and M. Boulmalf, "An empirical study of wifi security and performance in morocco-wardriving in rabat," in *Electrical and Information Technologies (ICEIT), 2016 International Conference on*. IEEE, 2016, pp. 362–367.

[5] S. Gupta, B. S. Chaudhari, and B. Chakrabarty, "Vulnerable network analysis using war driving and security intelligence," in *Inventive Computation Technologies (ICICT), International Conference on*, vol. 3. IEEE, 2016, pp. 1–5.

[6] A. Sarrafzadeh and H. Sathu, "Wireless lan security status changes in auckland cbd: A case study," in *Computational Intelligence and Computing Research (ICCIC), 2015 IEEE International Conference on*. IEEE, 2015, pp. 1–6.

[7] D. Dobrilovic, B. Odadzic, Z. Stojanov, and Z. Covic, "Approach in ieee 802.11 security analytics and its integration in university curricula," in *International*

Conference and Workshop Mechatronics in Practice and Education, *2015 3rd*, 2015.

[8] A. Nisbet, "A 2013 study of wireless network security in new zealand: Are we there yet?" 2013.

[9] ——, "A tale of four cities: Wireless security & growth in new zealand," in *Computing*, *Networking and Communications (ICNC)*, *2012 International Conference on*. IEEE, 2012, pp. 1167–1171.

[10] H. Said, M. Guimaraes, N. Al Mutawa, and I. Al Awadhi, "Forensics and war-driving on unsecured wireless network," in *Internet Technology and Secured Transactions (ICITST)*, *2011 International Conference for*. IEEE, 2011, pp. 19–24.

[11] B. Issac, S. M. Jacob, and L. A. Mohammed, "The art of war driving and security threats-a malaysian case study," in *Networks*, *2005. Jointly Held with the 2005 IEEE 7th Malaysia International Conference on Communication.*, *2005 13th IEEE International Conference on*, vol. 1. IEEE, 2005, pp. 6–pp.

[12] A. K. Kyaw, Z. Tian, and B. Cusack, "Wi-pi: a study of wlan security in auckland city," *International Journal of Computer Science and Network Security (IJCSNS)*, vol. 16, no. 8, p. 68, 2016.

[13] L. Jacob, D. Hutchinson, and J. Abawajy, "Wi-fi security: wireless with confidence," in *ASIC 2011: Proceedings of the 4th Australian Security and Intelligence Conference*. SECAU Security Research Centre, 2011, pp. 88–96.

[14] C. S. Priya, S. Umar, and T. Sirisha, "The impact of war driving on wireless networks," *International Journal of Science*, *Engineering and Computer Technology*, vol. 3, no. 7, p. 2300, 2013.

[15] S. Abdul Halim, "Exploring wireless network security in auckland city through warwalking," Ph.D. dissertation, Auckland University of Technology, 2007.

[16] M. Kim, J. J. Fielding, and D. Kotz, "Risks of using ap locations discovered through war driving," in *International Conference on Pervasive Computing*. Springer, 2006, pp. 67–82.

[17] W. O. L. Tool. (2017) Wireshark. [Online]. Available: https://www.wireshark.org/tools/oui-lookup.html

[18] I. S. A. R. Authority. (2017) Ieee. [Online]. Available: https://regauth.standards.ieee.org/standards-ra-web/pub/view.html#registries

[19] S. Viehböck, "Brute forcing wi-fi protected setup," *Wi-Fi Protected Setup*, 2011.

[20] W.-F. Alliance, "Wi-fi alliance announces standards-based security solution to replace wep," *Press Release*, *Wi-Fi Alliance*, vol. 31, 2002.

[21] O. H. P. and B. R., "Wi-fi based imsi catcher," 2016, blackHat, London, 2016-11-03. [Online]. Available: https://www.blackhat.com/docs/eu-16/materials/eu-16-OHanlon-WiFi-IMSI-Catcher.pdf

[22] P. Singh, M. Mishra, and P. Barwal, "Analysis of security issues and their solutions in wireless lan," in *Information Communication and Embedded Systems (ICICES)*, *2014 International Conference on*. IEEE, 2014, pp. 1–6.