DE GRUYTER OPEN
RIGA TECHNICAL UNIVERSITY
Applied Computer Systems
ISSN 2255-8691 (online)
ISSN 2255-8683 (print)
May 2017, vol. 21, pp. 38–45
doi: 10.1515/acss-2017-0005
https://www.degruyter.com/view/j/acss

Security Evaluation of Wireless Network Access Points

Rūdolfs Kalniņš[1], Jānis Puriņš[2], Gundars Alksnis[3]
[1,2]*Riga State German Grammar School, Latvia*
[3]*Department of Applied Computer Science, Riga Technical University, Latvia*

***Abstract* – The paper focuses on the real-world usage of IEEE 802.11 wireless network encryption and Wi-Fi Protected Setup (WPS) function. A brief history on the development of encryption methods and WPS is given. Wireless scanning of 802.11 networks in a capital city has been performed, and the results of it have been analysed. To ascertain the knowledge about the security of wireless networks of the average user, an online survey has been conducted. To test the security of encryption methods and WPS function, practical attacks against private test wireless networks have been made. The authors conclude that the safest way to set up 802.11 network with a pre-shared key is to use Wi-Fi Protected Access 2 (WPA2) encryption without support for WPS function. Statistics in Riga shows that networks are often configured otherwise and thus vulnerable to attacks. Survey results prove that respondents are not well informed regarding the security of wireless networks.**

***Keywords* – Network security, unauthorised access, wireless networks.**

I. Introduction

Security of wireless networks is a topical issue all over the world, especially in the recent years [1]. People start increasingly using wireless networks at school, work, cafés, parks and in other places. A new trend is connecting appliances and other devices to the Internet. It is called Internet of Things (IoT), and often this connectivity is made possible using wireless networks. It makes these devices portable, but also security risks are created [1]. Data sent through wireless networks can be captured and analysed for illegal purposes, for example, acquiring credit card information. It is the reason why the present research focuses on the security of wireless network access points and controllers. If unauthorised access can be prevented, data breaches can also be prevented. The research problem is defined as the security of wireless network access points. Goal of research is to determine the configuration of wireless networks in a city. Five tasks have been set:

1. to identify the safest possible wireless network configuration;
2. to ascertain knowledge about the security of wireless networks of the average user via an online survey;
3. to determine the security methods used in the wireless networks of the capital city of Latvia – Riga downtown and Agenskalns areas.
4. to make unauthorized access attempts to wireless networks, which use the safety methods of the wireless networks in Riga downtown and Agenskalns areas.
5. to examine the expert's opinion on wireless network configuration.

Hypothesis: Most users are not well informed about the security of wireless networks.

II. Summary of 802.11 Encryption Methods and Wi-Fi Protected Setup

A. Overview

The first wireless network encryption standard Wired Equivalent Privacy (WEP) was introduced as part of the original 802.11 specification ratified in 1997. Vulnerabilities in this encryption method were discovered in 2001, which required the development of a new encryption standard [2]. In 2002, Wi-Fi Alliance released a new encryption method Wi-Fi Protected Access (WPA), which was compatible with old hardware and thus only required software upgrade [3]. However, this was only a temporary workaround and Wi-Fi Alliance kept on improving WPA. The wireless specification 802.11i was ratified in 2004 and it included the improved Wi-Fi Protected Access 2 (WPA2). Since then no new encryption standards have been ratified, but in 2007 Wi-Fi Alliance created an additional safety method – Wi-Fi Protected Setup (WPS). WPS makes it possible to connect to a wireless network just by pressing a hardware button, thus avoiding entering a password altogether [4]. It should be noted that since the focus of the research is the security of wireless networks using pre-shared key encryption methods, the security of enterprise networks has not been researched. The 802.1x authentication method is used in enterprise-grade networks. Instead of using one pre-shared key, unique user names and passwords are distributed to clients of the network, increasing the overall security of the wireless network [4].

B. WEP Encryption

WEP encryption was the first method to secure a wireless network [4]. Before data are encrypted, a checksum is created to perform an integrity check, and then the data frame is encrypted using the stream cipher RC4 algorithm. Since this encryption method is outdated and can be easily decrypted, numerous vulnerabilities exist, such as the FMS attack, PTW attack and others [5]. The present research includes a review of vulnerability, which reveals the password of a WEP network. Research from TU Darmstadt proves that it is possible to acquire a password of a WEP network in just 60 seconds [6].

C. WPA/WPA2 Encryption

Due to high vulnerability of WEP networks, Wi-Fi Alliance created a new encryption method WPA, which was improved by WPA2 [7]. WPA encryption was a temporary workaround until a safer encryption method was developed. Since it had to be supported by the same hardware that supports WEP, very strong encryption could not be introduced due to a lack of processing power, but there were significant improvements over WEP, for example, the introduction of Temporal Key Integrity Protocol (TKIP) and others. As described in a publication by TU Dresden, manipulation of sent data packets in a WPA network is possible, along other vulnerabilities [8].

With the ratification of 802.11i specification in 2004, the improved encryption standard WPA2 is released and WEP/WPA standards are made deprecated [4]. WPA2 is still the safest 802.11 wireless network encryption available at the time of writing. It is not perfect, as vulnerabilities still exist. For example, the 4-way handshake (which is also used in WPA) enables an offline dictionary attack, which makes a brute force password guessing attempt up to several thousand times faster [4]. The University of Central Florida has reviewed a possibility of an online dictionary attack, which incorporates emulation of wireless network clients, each with a different MAC address, and each emulated client attempts to try a password. Such an attack is up to 100 times faster than a traditional online brute force attack [9]. It should be noted that the only way to acquire the password of a WPA2 network (without WPS support) is guessing it, and these vulnerabilities only speed up the guessing process.

D. Wi-Fi Protected Setup (WPS) Vulnerability

WPS was created to make it easier for an average user to create a safe wireless network. It is often used – according to the Wi-Fi Alliance product finder, 18,894 devices are certified for WPS usage [10]. There are serious implementation flaws, which make it possible to gain unauthorised access to an otherwise safe network. WPS uses a Private Identification Number (PIN) code to authorise access to a network. If a network is using WPS with the Push-Button-Connect method, the process is automated and the user does not have to enter any code himself. However, there are WPS methods, which require a manual PIN code input. The PIN code is 8 digits long, thus there should be 10^8 (=100.000.000) different possible codes. If one WPS check would need only 1.3 seconds, a full brute force attack would require 115.74 days [11]. That is not the case – the last digit of the code is a checksum, and the first four digits are checked separately from the last three digits. This method of checking the PIN code is flawed because it makes possible to perform a full brute force attack in just $10^4 + 10^3$ (=11.000) tries. It means, that if one PIN check would take only 1.3 seconds, a full brute force attack would require only 3.06 hours [11]. It should be noted that in live situations one PIN check can require several seconds.

III. Interview with Peter Johansson (WatchGuard)

An interview with WatchGuard Regional Manager in Northern Europe and Baltics Peter Johansson was conducted within the framework of the research. WatchGuard is an enterprise network security solution provider, and because of that the opinion of WatchGuard representative is competent and valuable. The interview was conducted during the international IT conference DSS ITSEC 2016 [12].

During the interview, questions were asked regarding the awareness of network security of the general population, the security of wireless networks in real life and network security as such. Peter Johansson pointed out that the security of wireless networks depends on the manufacturers of wireless routers and IT professionals. Most users do not want to spend time learning about security of wireless networks or do not care about it and their routers are using factory-given service set identifiers (SSIDs) and passwords. If the manufacturer creates a different password and SSID for each router, and uses WPA2 encryption without WPS function, then the private network will be safe. If the manufacturer does not apply safe default settings, most users will not be bothered to change them and private networks will not be safe. However, if an IT professional sets up the network, in most cases it will be safe. In such cases, it may be worth thinking of additional safety measures, such as firewalls and Wireless Intrusion Prevention Systems (WIPS). While firewalls are often included in software and only require the knowledge of an IT professional to be set up, WIPS are expensive systems, starting at 1000 USD for one access point, so it is very unlikely for an average home user to even consider it. Since firewalls are software solutions, they are a great way to increase the security of devices connected to a wireless network. Setting up a firewall increases the network security even if a malicious user tries to perform attacks in the network.

IV. Survey – Awareness of Network Security of the General Population

A survey was conducted online with the goal to determine the knowledge about network security of the public, and their attitude towards it. Survey was popularised using the social networks Facebook and Twitter; thus, respondents were people using the Internet and social networks on a regular basis. Survey had 140 respondents, of which 93 (66.4 %) were female and 47 (33.6 %) were male. The average age of respondents was 16.3 years. Respondents were divided in two groups: those who had a private wireless network, and those who did not. Only three respondents did not have a private wireless network. As a reason, two respondents said that wireless networks posed a risk to human health, and one respondent did not specify a reason. Out of the remaining 137 respondents, only two answered that their wireless network was not secured with a password, and neither of them specified any reason for the lack of password.

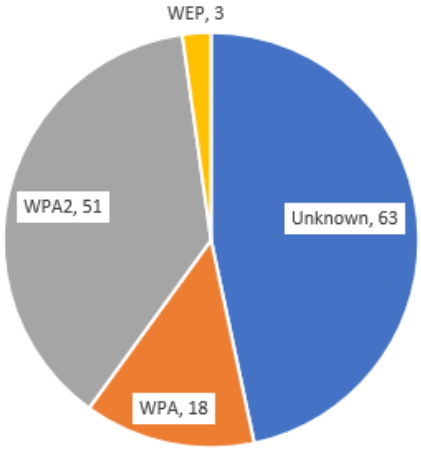

Fig. 1. The answers of 135 respondents to the question "Please pick the encryption method of your private W-Fi network". Amount of times each answer has been picked is given after the answer.

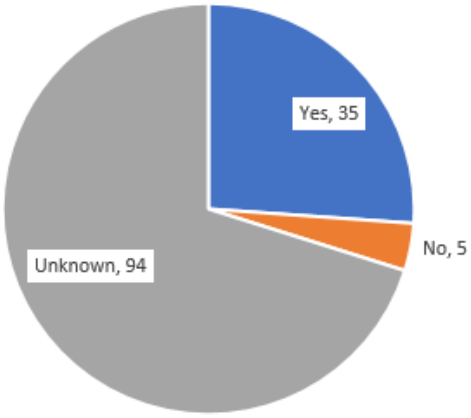

Fig. 2. The answers of 135 respondents to the question "Is the WPS function enabled in your private Wi-Fi network?". Amount of times each answer has been picked is given after the answer.

As depicted in Fig. 1, almost half of respondents did not know which encryption was used in their private wireless network. However, more than 50 % answered that either WPA or WPA2 encryption was used. This statistic is positive, because WPA2 is the safest wireless network encryption method followed by WPA. Even though almost half of respondents did not know the encryption used, it might be assumed that in most cases WPA or WPA2 encryption was used because of the statistics acquired later in wardriving.

A strong contrast to the statistics of Fig. 1 can be seen in Fig. 2. Almost ¾ (~70 %) of respondents did not even know whether the WPS function was enabled in their private network or not. More than ¼ (~26 %) respondents knew that the WPS function was enabled and only 5 respondents knew that it was not enabled. This statistic implies that most respondents did not know enough about wireless network security. While the most respondents knew the encryption used, a high number of respondents who did not know whether the WPS function was enabled or not only showed that the respondents did not know enough about wireless network security.

V. Wardriving (Wireless Network Scanning)

Wardriving is the act of scanning for wireless networks in an area, and recording the obtaining data. In 2012, 2013 and 2015 Squalio performed wardriving in Riga downtown area. Each year, information of about 2000–2500 networks was obtained [13]. The results showed that the number of networks using WPA/WPA2 encryption had never dropped below 72 %. The number of WEP networks was decreasing at a high rate. In 2012, WEP networks accounted for 7 % of all networks; in 2013 – 5 % and in 2015 – only 1 %. The number of unsecured wireless networks is relatively high. It can be explained by the fact that *Lattelecom* is setting up free Wi-Fi hotspots all around Riga and Latvia [14]. It should be noted that no information about WPS usage has been collected during the wardriving of Squalio [13].

In the year 2012, a wardriving experiment was performed in Berlin, Germany, in which data about 1,850 unique wireless access points were collected [15]. The number of WPA/WPA2 secured wireless networks was higher than in Latvia in 2012: in Berlin 91 % (1,683 networks) of networks were using WPA/WPA2 encryption, while in Latvia only 78 %. Another significant difference was in the number of unsecured networks. In Berlin, there were even more WEP protected networks than unsecured networks (95 networks with WEP encryption and 72 unsecured networks). In Riga, 15 % of networks were unsecured and 7 % used WEP encryption [13], [15].

A wardriving experiment of larger scale was conducted in Clitheroe, England, in 2013, during which data about 7,514 wireless networks was collected [16]. The number of unsecured networks was higher in Clitheroe than in Riga or Berlin: 38 % of networks did not use any encryption. It should be noted that most of the unsecured networks were *BT Wi-Fi Hotspots*, which required *BT* account credentials to use the Internet. Since the network is unsecured, even people without any account credentials can perform various attacks against anyone using the network [16]. The rest of networks were secured. 58 % of networks used WPA/WPA2 encryption and less than 4 % used WEP encryption. While more networks in Riga and Berlin used WPA/WPA2 encryption, the relative number of WEP networks was lowest in Clitheroe – less than 4 % [16]. This low statistic was beaten in Riga in 2015, when only 1 % of networks used WEP encryption [13]. The collection of data about WPS function was unique in this experiment. Out of 7,514 networks 2,858 networks (38 %) had the WPS function enabled [16].

One interesting aspect is historical statistics. A wardriving experiment was conducted at CeBIT 2006 in Hannover [17]. This wardriving experiment collected data on approximately 300 access points. Since this is an old experiment, wireless networks were not widespread and they used either WEP encryption or no encryption at all, even though IEEE 802.11i had already been ratified in 2004, which included WPA2 encryption. The results of this wardriving show that most networks did not use encryption: 55.67 % of networks were unsecured and 44.33 % of networks used WEP encryption.

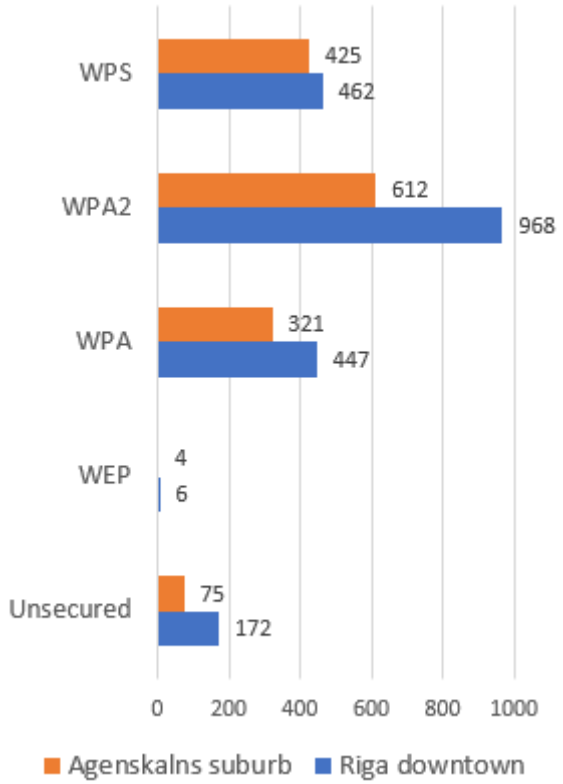

Fig. 3. Diagram showing statistics acquired in wardriving.

The present research also included wardriving. It was performed in the downtown area of Riga and the suburb area of Riga Agenskalns. The data were collected using a Samsung GT-I8160 smartphone with the application "Wi-Fi Tracker". At the end of wardriving, information about 1,989 networks (1,172 in the downtown and 723 in Agenskalns suburb) was collected. The trend observed by Squalio can be observed in the results of this wardriving: most networks use either WPA or WPA2 encryption. More networks in the downtown area (14.6 %) do not have a password than in Agenskalns suburb (10.4 %). This difference can be explained by the fact that a downtown area features more cafes, hotels and shops than Agenskalns suburb. As an example, the cafe network *Coffee-inn* can be mentioned. Out of 14 *Coffee-inn* cafes in Riga, 10 are located in the downtown area, while the others are in shopping malls outside of downtown area [18]. Most of public objects in Riga feature the free Wi-Fi hotspot *Lattelecom-Free* [19]. In the downtown area, 31 networks with the SSID "Lattelecom-free" were discovered, but in Agenskalns suburb – only 12.

It should be noted that most wireless networks use the PSK (*pre-shared key*) authentication method. The number of networks that use *enterprise-grade* encryption is very low – only ~4 % of all networks. To set up a WPA/WPA2 network with *enterprise* encryption, an additional authentication server must be created to deploy user names and passwords [4]. Since the setup of an *enterprise* network requires an additional server, only people with competent skills in IT can set it up, and those people are most likely well informed about the security of wireless networks. Due to this reason and their low number in wardriving results, this review did not focus on *enterprise* network security. The research focused on WEP, WPA/WPA2-PSK network security and the vulnerability of WPS function. Data acquired when wardriving were similar to wardriving results worldwide. According to statistics provided by WiGLE, 186,687,893 (57.36 %) networks worldwide use WPA2 encryption [20]. The second most common encryption is WPA, which is used by 24,493,139 (7.52 %) networks. According to the statistics provided by WiGLE, 64,951,400 (19.94 %) networks use an unknown encryption method, which is depicted as (????) at the WiGLE website. This was not discovered in Riga. The unknown encryption type can be attributed to errors in data processing, since information about wireless networks to the WiGLE project can be submitted in different data formats. WiGLE is one of the largest wireless network scanning projects, which compiles statistics about wireless networks in the whole world. The WiGLE project has been active since 2001, and it has collected information about more than 320 million wireless networks [20].

When comparing the statistics acquired in wardriving experiments in other cities, a trend can be seen that over time more networks are using encryption, and with time safer encryption methods are being used. What stood out is the fact that in Berlin there was relatively the lowest number of unsecured networks, meanwhile Clitheroe had the highest number of unsecured networks. Even though the unsecured networks used a login portal to grant access to the Internet, a safer alternative would have been the usage of enterprise-grade encryption. Overall, a similar trend can be seen in all wardriving results of recent years – most networks use WPA/WPA2 encryption, a large fraction of networks is unsecured and only a small part of networks uses WEP encryption. The usage of WPA/WPA2 encryption is increasing and the usage of WEP encryption is decreasing.

VI. Practical Attacks against Different Encryption Methods and the WPS Function

Practical attacks were done with the goal to acquire pre-shared keys of the networks. Attacks were carried out using freely available tools included in Kali Linux distribution and targets of attacks were dedicated test wireless networks created specifically for the experiments performed.

A. Acquiring the Key of a WEP Network

Practical test was carried out with the WEP network set up in the infrastructure mode. The wireless router used in testing was TP-Link TL-WR340G, which had an Apple iPhone 5s connected to it, and it was streaming video from YouTube. Attack was performed with Samsung NC110 netbook, which had standard Kali Linux distribution installed (Kali 2016.2). The hardware used was chosen because the author had already owned it, and the netbook wireless card was compatible with hacking software found in Kali Linux. It was chosen to use Kali Linux distribution because it contained a collection of security and forensics tools and it was being frequently updated [21]. The only factor which could interfere with the practical test was signals of other wireless networks. The test

was carried out in laboratory settings, where it could not be avoided. During testing, there were no errors caused by the presence of other wireless networks.

Using a Random String Generator, the wireless network was set up with an auto generated SSID and password at the website www.random.org. The generator was set to use capital and standard-case letters and digits. The wireless password key type was set to 128 bit in the settings of the wireless access point.

Name of wireless access point: 19mDy9tm5hmVKpaw

WEP password: IbsAQvCNK1ghf

At the beginning of the attack, the wireless network card had to be set in the monitor mode to enable the capturing of packets sent in the WEP network. This was done by executing the command "airmon-ng start wlan0" in a terminal emulator of Kali Linux. With the card set in the monitor mode, the MAC address had to be required to perform an attack. Since Samsung NC110 is equipped with Intel Centrino Wireless-N 130 network card, no further configuration was needed because Kali Linux supported it natively. Acquiring of the MAC address was done by executing the command "airodump-ng wlan0mon". Since the network had a client device attached to it, which actively transmitted WEP encrypted data packets, they had to be captured in order to be decrypted [22].

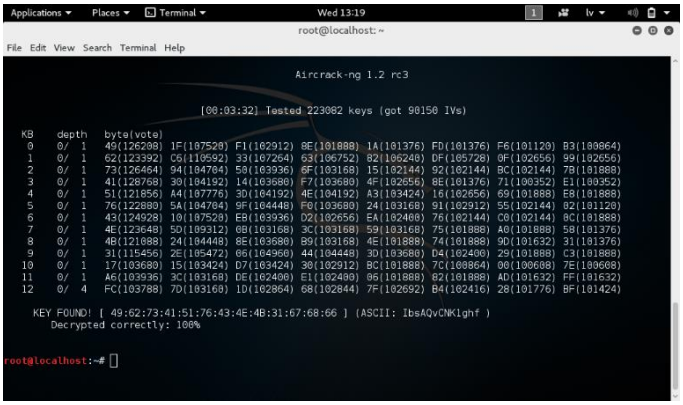

Fig. 4. Screenshot of Kali Linux terminal emulator with the acquired WEP key using aircrack-ng.

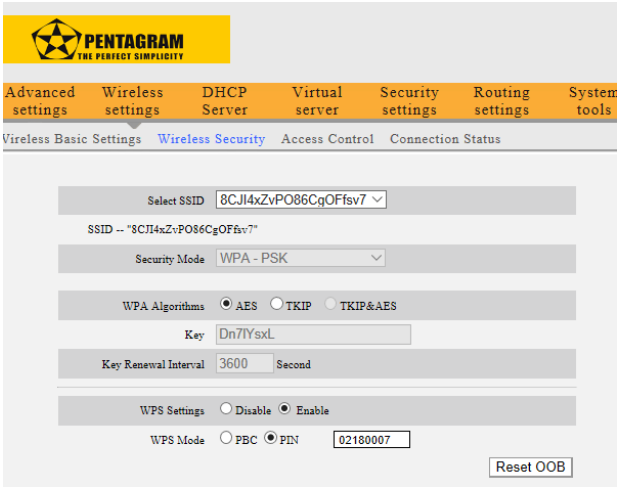

Fig. 5. Screenshot of the security settings page of the test network used to test the WPS function.

Data packet capturing was performed by executing the command "airodump-ng –w paketes -c 1 --bssid 54:E6:FC:A1:28:A2 wlan0mon". The encryption of wireless network key can be done simultaneously with data packet capturing. It was done by executing the command "aircrack-ng paketes-01.cap". When enough data packets are captured, the key is gained in a hexadecimal format, and if it is possible, it is transformed to ASCII format [23]. The WEP key was gained in 3 minutes and 32 seconds after executing the command "aircrack-ng paketes-01.cap".

B. Acquiring the Key of a WPA Network Using WPS

The practical test was made against Pentagram Cerberus P 6363 wireless router, which was set up with WPA encryption and the WPS function enabled. Wireless network was set up with randomly generated SSID and password, which were randomly generated using a Random String Generator at the website www.random.org. The SSID was 20 characters long whereas the password was only 8 characters long. This is due to the way the firmware for the Pentagram Cerberus P 6363 has been made – the firmware allows only 8-digit long WPA passwords, even though a WPA password can be up to 63 ASCII-encoded character long [24]. The router firmware allows using longer passwords for WPA2 encryption, but the only way to set the WPS function is to use WPA encryption, even though it should be possible to use WPS alongside WPA2 [11]. However, since the encryption method and length of the password do not impact the WPS vulnerability in any way, this was not a problem [11].

Name of wireless access point: 8CJI4xZvPO86CgOFfsv7

WPA password: Dn7lYsxL

Another interesting fact about the firmware used in the Pentagram Cerberus P 6363 router is that it requires the user to manually enter the PIN code for the WPS function, even though a PIN code is provided on the sticker attached to the router itself. The firmware of this router can be a good example for poorly configured default settings. In the wireless security page of its settings it is written that "*Our company has optimised wireless encryption. Select WPA-AES and you can prevent others from access to your network*." As the router also supports WPA2 encryption it is unclear why it is not recommended, and why the WPS function cannot be enabled when using WPA encryption. When prompted to enter a PIN code for the WPS function, the PIN code written on the attached sticker was chosen.

Attack against this network was performed with Samsung NC110 netbook, which had standard Kali Linux distribution installed (Kali 2016.2). The program Reaver was used in the attack. The attack was started by executing the command "time reaver -i wlan0mon -b 54:E6:FC:E4:04:54 -v". Command time measures the execution time of the program specified in the parameters (in this case, Reaver). With Reaver the WPA key was acquired in 11 minutes and three seconds. In the range of the laptop, there was another wireless network, which used WPA2 encryption and had the WPS function enabled. The same attack was performed on this network, and the only difference was the change of MAC address in the

executed command. The password of the wireless network was acquired in 184 minutes, and it consisted of two words and two digits, separated by an underline. This password cannot be found in the "rockyou.txt" password list file. This means, if this network did not have the WPS function enabled, it would be impossible to acquire its password with the tools included in Kali Linux distribution. It should be noted that the password could be gained by using a bigger wordlist than "rockyou".

C. 4-way Handshake Vulnerability of WPA/WPA2 Networks

WPA2 networks are vulnerable only if the password can be guessed [4]. Any network with a guessable password can be hacked – it is only a matter of time. There is the 4-way handshake vulnerability, which makes it possible to check multiple passwords per second, and it also enables an offline attack [25]. Any network that uses a password that is easy to guess can be hacked due to brute force attacks. However, this vulnerability increases the speed of brute force attack – in the practical test passwords were tested against the handshake at a speed of 100–500 passwords per second. It should be noted that a relatively weak and outdated central processing unit (CPU) was used – a dual core Intel Atom with the clock speed of 1.5 GhZ. Using a more powerful CPU or dedicating a graphics processing unit (GPU) to the testing can increase rate at which passwords are checked. Since only the captured 4-way handshake is required to perform the attack, it can be done offline [25]. A plausible real world scenario would be acquiring the 4-way Handshake with a mobile device, and performing the offline attack with a more powerful stationary device. Due to a lack of dedicated GPU, CPU was used to perform the attack. If a GPU would have been available, the password guessing process would have been much faster. An AMD Radeon R9 290X GPU could check as many as 180000 passwords per second [26]. It should be noted that it would require using other program than coWPAtty, which would have support for GPU processing. Since no GPU was available, there was no need to use another program. In the example with Radeon R9 290X GPU, the program oclhashcat was used [26].

This vulnerability was tested three times using the wireless router Cerberus P3636, and each time a different password was set for the network:

- A word found in a dictionary (password);
- A word found in a dictionary with a number at the end (batman25);
- Randomly chosen 20-character long digit string (cOvrDwAQVKst3fDwlAWp).

The first step was capturing the 4-way handshake, and it was sent on the network when a device connected to it, and the data packet capturing was started by executing the command "airodump-ng –-bssid 54:E6:FC:A1:28:A2 -c 1 -w gencap wlan0mon". After the 4-way Handshake was captured, it was possible to perform a brute force dictionary attack against it. It was done using the program CoWPAtty. The password "password" was acquired in less than a second after starting CoWPAtty, "batman25" was acquired in 1174 seconds, but "cOvrDwAQVKst3fDwlAWp" could not be acquired because it could not be found on the word list. The time in which these passwords were acquired should not be taken as definitive. The processing power in the netbook used is low when compared to today's standards, and as mentioned earlier, the process could be made remarkably faster by using a dedicated GPU. It should be noted that this is not the only vulnerability that can increase the speed at which the password of a WPA2 network is guessed. In the conference proceedings by the University of Central Florida, the parallel active dictionary attack has been reviewed. But due to the complexity of it, it was not tested in the research [9].

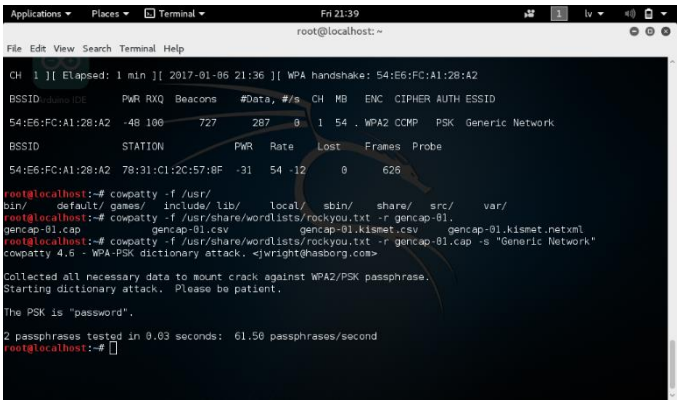

Fig. 6. Screenshot of Kali Linux terminal emulator with the acquired WPA2 key using coWPAtty.

D. Social Engineering Attack

Another method of attack on wireless networks and networks, in general, is social engineering. In social engineering, the hacker retrieves credentials and login information from the end user applying deceiving social dialog and/or messaging.

Using social engineering can be the only way to hack the password in such cases, when there are not any technical vulnerabilities:

- WPA2 encryption is used;
- WPS function is disabled;
- The password is long and cannot be guessed.

During the research, a social engineering attack was carried out at the National Library of Latvia on 7 January 2017. The attack was made against the network "Briivpieeja", which had WPA2 encryption and the WPS function was disabled. The wireless password for this network is freely distributed at the library, and the name of network in English is "Free access". Attack was done as a proof of concept of social engineering, without any malicious intent. The "Briivpieeja" network was actively used at the time of attack because unsecured networks in the library did not provide the Internet access. The attack was performed using the tool Fluxion, which was not included in Kali Linux. It is free software and can be acquired free of charge from its Github page [27]. At first, a malicious network was set up. The malicious network imitates the real network, even though it does not have the Internet access. The

malicious network was set up using the wireless card in Samsung NC110 netbook. Then, data packet capturing on the real "Briivpieeja" network was started, with the goal of acquiring the 4-way handshake. Deauthorisation packets were sent on the real network with the goal of forcing users to connect to the malicious network. When a user connects to a malicious network and tries to access the Internet, a phishing website shows up, which asks to enter the password. After a password is sent on the phishing website, it is checked against the 4-way handshake. If the password is the real password of the network, the malicious network is shut down. Otherwise, it continues to function until the real password is entered. The password of "Briivpieeja" network was acquired in 46 minutes.

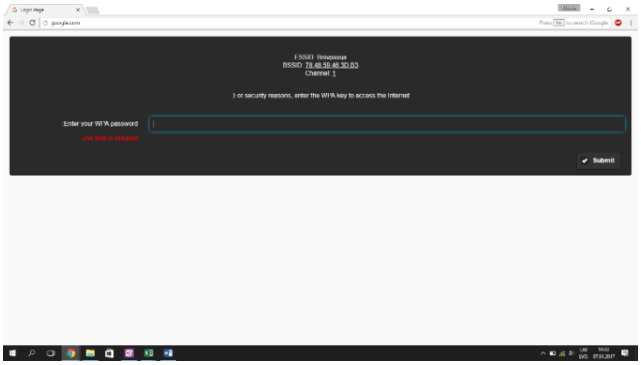

Fig. 7. Screenshot of the phishing website used in the social engineering attack.

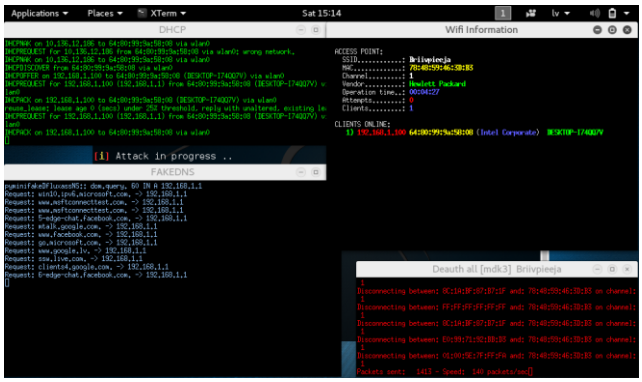

Fig. 8. Screenshot of the program Fluxion hosting a malicous wireless access point, sending deauthorisation frames in the real "Briivpieeja" network and forwarding all trafiic sent in the malicious network to the phishing site.

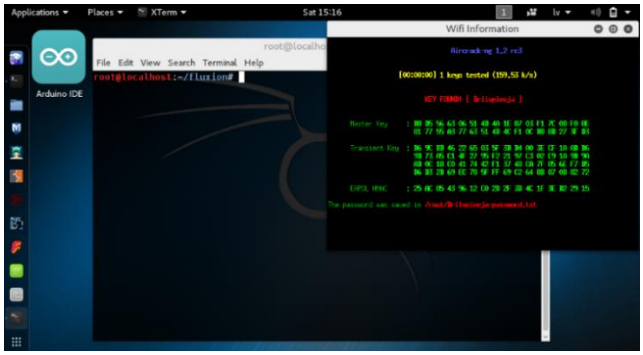

Fig. 9. Screenshot of Kali Linux destkop with the acquired password of the "Briivpieeja" network. The malicous network has been shut down because the pasword has been acquired.

VII. Results and Conclusion

Hypothesis has been proven to be true – most users are not well informed about the security of wireless networks.

The safest PSK wireless network configuration is WPA2 without the support for WPS function. Networks that use enterprise-grade encryption are safer, because each user has a unique user name and password (whereas in the personal mode a pre-shared key is used, which is the same for all users, and there are no usernames) and an additional server needs to be set up to handle password distribution. Due to the fact, that they are very uncommon and the technical knowledge is required to set up such networks, the security of such networks was not researched.

Results of the conducted survey show that the respondents are not well informed about the security of wireless networks. More than 69 % of respondents do not even know if the WPS function is enabled or not. Since the vulnerability of the WPS function makes even WPA2 networks vulnerable, the nescience about it only proves that respondents do not know enough about wireless network security.

The results of conducted wardriving show that the most used encryption methods in Riga is WPA/WPA2. This statistic correlates to results of wardriving worldwide. Contrary to this statistic, 47 % of networks had the WPS function enabled. A conclusion can be made that most private networks use factory settings, since the WPS function is often enabled by default.

Focus of the research was the practical test of the safety of different wireless encryption methods and the WPS function. The password of WEP secured network was acquired in a short time span and without any problems. Passwords of WPA/WPA2 networks could only be acquired if they could be found in a password list (The password list "rockyou.txt" was used in the research) or if they had the WPS function enabled.

The conducted interview has shown another perspective of wireless network security – the security of wireless networks does not end with encryption. Users are vulnerability of any network – they can tell the wireless network password to unauthorised people or fall victim to a social engineering attack and enter the password in a phishing site. Firewalls provide additional security to the network – if there is a breach and unauthorised people gain access to the network, a firewall can prevent damage to devices connected to the compromised network. The average owner of a private wireless network is not competent enough to set up the network as safe as possible and often factory settings are used. That is the reason why the security of an average private wireless network is dependent on the manufacturers of wireless routers. If the manufacturer ships its wireless routers with a unique and randomly generated password and with disabled WPS function (or no support for it at all), then the private network is safe as long as the password is not disclosed to malicious people or no vulnerabilities are found in the software of the router. Further research on this topic can be conducted: wardriving experiments can be performed on a larger scale and in cities of different size, more interviews and surveys can be conducted, practical attacks against wireless networks can be made using

alternative hacking tools, for example, a closer look could be taken at hacking tools that operate in Windows operating systems, rather than Linux.

REFERENCES

[1] "Internet of Things - Lietiskais internets (IoT)," May 2016. [Online]. Available: https://cert.lv/uploads/Ieteikumi/OUCH-201605_lv.pdf [Accessed: January 25, 2017]. (in Latvian).
[2] S. Fluhrer, I. Mantin, and A. Shamir, "Weaknesses in the key scheduling algorithm of RC4" *Lecture Notes in Computer Science*, pp. 1–24, 2001. https://doi.org/10.1007/3-540-45537-x_1
[3] Wi-Fi Alliance, "Wi-Fi Protected Access: Strong, standards-based, interoperable security for today's Wi-Fi networks," *White paper, University of Cape Town*, 2003. [Online]. Available: http://www.ans-vb.com/Docs/Whitepaper_Wi-Fi_Security4-29-03.pdf [Accessed: May 5, 2017].
[4] K. Benton, "The evolution of 802.11 wireless security," *Informatics-Spring*, 2010. [Online]. Available: http://homes.soic.indiana.edu/ktbenton/research/benton_wireless.pdf [Accessed: January 25, 2017].
[5] J. R. Vacca, *Computer and Information Security Handbook*. Morgan Kaufmann, 2007, pp. 172–173.
[6] E. Tews, R.-P. Weinmann, and A. Physkin, "Breaking 104 bit WEP in less than 60 seconds," in *Cryptology ePrint Archive, Report 2007/120* [Online]. Available: Cryptology ePrint Archive http://eprint.iacr.org/2007/120 [Accessed: January 25, 2017].
[7] Wi-Fi Alliance [Online]. Available: http://www.wi-fi.org/ [Accessed: May 5, 2017].
[8] E. Tews and M. Beck, "Practical attacks against WEP and WPA" in *Proceedings of the second ACM conference on Wireless network security – WiSec'09*, pp. 79–86, 2009. https://doi.org/10.1145/1514274.1514286
[9] O. Nakhila, A. Attiah, Y. Jinz, and C. Zoux, "Parallel Active Dictionary Attack on WPA2-PSK Wi-Fi Networks," *MILCOM 2015 – 2015 IEEE Military Communications Conference*, October 26-28, 2015, Tampa, FL, USA. https://doi.org/10.1109/milcom.2015.7357520
[10] Wi-Fi Alliance. "Product finder" [Online]. Available: http://www.wi-fi.org/product-finder-results?sort_by=default&sort_order=desc&certifications=39 [Accessed: January 25, 2017].
[11] S. Viehböck, "Brute forcing Wi-Fi Protected Setup" [Online]. Available: https://sviehb.files.wordpress.com/2011/12/viehboeck_wps.pdf [Accessed: January 25, 2017].
[12] "DSS ITSEC 2016: Cyber, Connected Things and Insecurity: The Largest Cyber Security Event in Baltics," 2016. [Online]. Available: https://www.dssitsec.eu/ [Accessed: May 5, 2017].
[13] "WIFI pētījums. Atvērto bezvadu tīklu drošības riski – Wi-Fi research. Security risks of open wireless networks," Oct. 27, 2015. [Online] Available: https://blogs.squalio.com/2015/10/27/wifi-petijums-atverto-bezvadu-tiklu-drosibas-riski/ [Accessed: January 25, 2017]. (in Latvian).
[14] "Lattelecom vēsture – History of Lattelecom" [Online]. Available: https://www.lattelecom.lv/par-lattelecom/par-mums/vesture [Accessed: January 25, 2017]. (in Latvian).
[15] "Wardrive in Berlin" [Online]. Available: http://www.gehaxelt.in/blog/wardrive-in-berlin/ [Accessed: May 5, 2017]. (in German).
[16] S. Helme, "WiFi (in)Security – Is your network on the map and is it secure?" [Online]. Available: https://scotthelme.co.uk/wifi-insecurity-wifi-map/ [Accessed: May 5, 2017].
[17] A. Gostev and R. Schouwenberg. "War-driving in Germany – CeBIT2006" [Online]. Available: https://securelist.com/analysis/36076/war-driving-in-germany-cebit2006/ [Accessed: May 5, 2017].
[18] "Where to find us" [Online]. Available: http://coffee-inn.lv/#find [Accessed: January 25, 2017].
[19] "Map of Lattelecom Wi-Fi" [Online]. Available: https://wifi.1188.lv/ [Accessed: January 25, 2017]. (in Latvian).
[20] "WiGLE Statistics" [Online]. Available: https://wigle.net/stats [Accessed: January 28, 2017].
[21] "DistroWatch: Kali Linux" [Online]. Available: https://distrowatch.com/table.php?distribution=kali [Accessed: May 5, 2017].
[22] "Airodump-ng documentation" [Online]. Available: https://www.aircrack-ng.org/doku.php?id=airodump-ng [Accessed: January 25, 2017].
[23] "Aircrack-ng documentation" [Online]. Available: https://www.aircrack-ng.org/doku.php?id=aircrack-ng [Accessed: January 25, 2017].
[24] IEEE Standarts Association, "IEEE 802.11i-2004: Medium Access Control (MAC) Security Enhancements" [Online]. Available: http://standards.ieee.org/getieee802/download/802.11i-2004.pdf [Accessed: May 5, 2017].
[25] A. Tsitroulis, D. Lampoudis, and E. Tsekleves, "Exposing WPA2 security protocol vulnerabilities," *International Journal of Information and Computer Security*, vol.6, no.1, pp. 93–107, 2014. https://doi.org/10.1504/ijics.2014.059797
[26] "Brute-Force WPA/WPA2 via GPU" [Online]. Available: https://null-byte.wonderhowto.com/how-to/brute-force-wpa-wpa2-via-gpu-0170474/ [Accessed: May 5, 2017].
[27] "FLUXION" [Online]. Available: https://github.com/wi-fi-analyzer/fluxion [Accessed: May 5, 2017].

Rūdolfs Kalniņš was born in 1999. He is a student at Riga State German Grammar School, Riga Latvia. He has been part of Latvian delegation MILSET Expo Sciences International 2017.
He has internship experience as a Junior System Administrator at translation company "Nordtext". Fields of interests include system administration and cyber security.
E-mail: ruudolfsk@gmail.com

Jānis Puriņš was born in 1964. The degree obtained: *Mg. sc. ing.* (1999) – University of Latvia.
He is a Teacher of Informatics at Riga State German Grammar School, Riga, Latvia. Special interests: cross-platform development.
E-mail: janis.purins@lu.lv

Gundars Alksnis received *Dr. sc. ing.* in information technologies (system analysis, modelling and design) from Riga Technical University, Latvia, in 2008.
He is an Assistant Professor and Researcher at the Department of Applied Computer Science, Riga Technical University. His research interests include modelling in the context of model-driven software development and IT security.
E-mail: gundars.alksnis@rtu.lv