DOI: 10.19279/TVZ.PD.2015-3-1-05

SAFETY AND SECURITY PROBLEMS OF BASIC WIRELESS NETWORK PROTECTION PROTOCOLS IN EVERYDAY LIFE

HR - SIGURNOSNI I ZAŠTITNI PROBLEMI OSNOVNIH ZAŠTITNIH PROTOKOLA BEŽIČNIH MREŽA U SVAKODNEVNOM ŽIVOTU

Tomislav Marjanović[1]

[1]Polytechnic of Zagreb

Abstract

This paper deals with the topic of safety and security of wireless networks in the Republic of Croatia, specifically in the town of Sisak (Sisačko – moslavačka županija). Types of protective protocols that users mostly use and some of the features of these technologies. Some of the major problems in the security of those technologies and the ways in which these risks can be prevented. Free tools that can infiltrate the system and thus jeopardize the privacy and security of users.

About criminal law of unauthorized access and identity theft related to wireless devices. Also on the prevalence of unprotected devices by some of the largest districts in the city of Sisak, which will be illustrated and described in this paper.

Keywords: *Wireless networks, security protocols,* WEP, WPA, WPA2*, criminal law, identity theft, protection, safety, Sisak*

Sažetak

Rad se bavi temom sigurnosti i sigurnosti bežičnih mreža u Republici Hrvatskoj, posebno u gradu Sisku (Sisačko – moslavačka županija). Vrstama zaštitnih protokola koje korisnici najčešće koriste i neke od značajki tih tehnologija. Nekim od glavnih problema u sigurnosti tih tehnologija i načinima na koji se ti rizici mogu spriječiti. Besplatnim alatima kojima se može infiltrirati u sustav i na taj način ugroziti privatnost i sigurnost korisnika.

O kaznenom zakonu neovlaštenog pristupa i krađe identiteta u vezi bežičnih uređaja. Također, na rasprostranjenosti nezaštićenih uređaja u nekima od najvećih kvartova u gradu Sisku koji će biti prikazani i opisani u ovom radu.

Ključne riječi: *Bežične mreže, sigurnosni protokli,* WPA, WEP, WEP2*, kazneni zakon, krađa identiteta, zaštita, sigurnost, Sisak*

1. Introduction

1. Uvod

Technology is growing exponentially, and so does the Internet and society with it. Their rapid development causes changes in everyday life. Lifestyle is faster and more active day by day, people adjust their activities to the things which they are surrounded. Smartphone, tablets and laptops are now standard and are used by almost everyone. For the purposes of education, work or daily life and routines, they are irreplaceable thing of every human being. With all this comes a lot of dangers and problems. This accelerated lifestyle leads to a drop in awareness among people. People do not notice some basic things around themselves They imagine or visualize something without looking around so that jeopardize their own safety The thing is that people have to snap out and live in reality, so they can be safe and secure.

The same thing is with the new technology. With rapid growth comes the risk of exploitation of the security levels of some device or software. Devices are made to last only a few years because almost every day the big companies present their new devices that are better and more advanced than the previous. In all the confusion comes to mentioned above vulnerabilities that directly affect the safety of users. Most of these vulnerabilities may lead to even bigger problems. Identity theft, sharing Internet traffic, unauthorized use of the device and even terrorism.

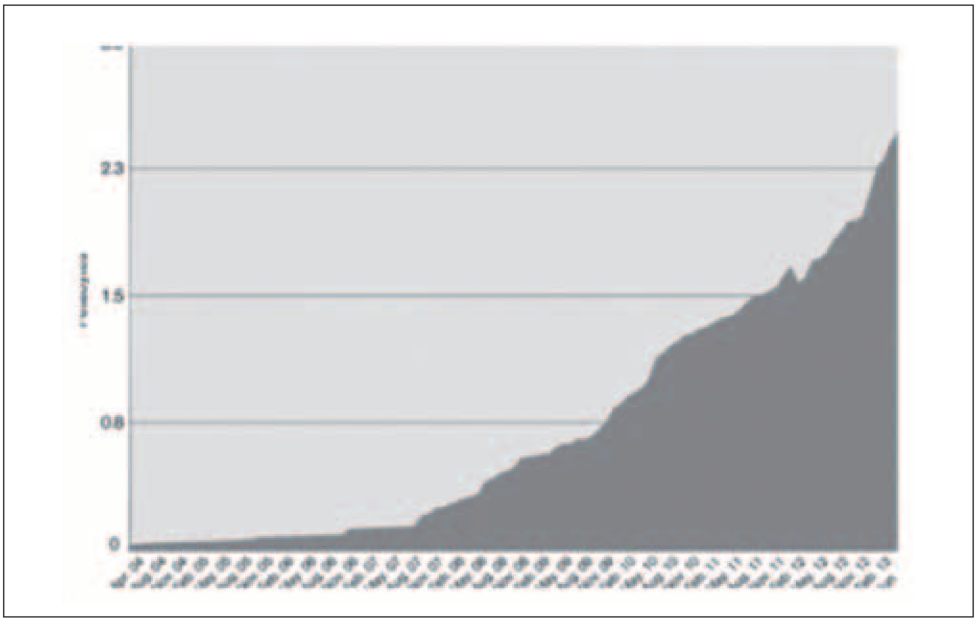


Figure 1 *Growth in Digital Collection Storage* [1]

Slika 1 *Porast količine digitalnih informacija* [1]

People have to become aware of the issues concerning them and the new technologies and they need to improve the safety of themselves and others at any cost.

The greatest danger comes from the Internet and wireless technology. Through the years it has progressed very much and almost every household now owns at least one modem / router. Newer devices have the possibility of wireless access. The word wireless dictionary is defined as "having no wires." In networking terminology, wireless is the term used to describe any computer network where there is no physical wired connection between sender and receiver, but rather the network is connected by radio waves and / or microwaves to maintain communications [2].

A. Types of Wireless Protection

A. Vrste zaštita bežičnih mreža

In the context of Wi-Fi (Wireless-Fidelity) technology, security means two things. First, controlling who can connect to and configure your network and equipment. Second, it means securing the data travelling wirelessly across your Wi-Fi network from unauthorized view [3]. Here are some of main Wireless protection protocols that most of the users have:

WEP (Wired Equivalent privacy) is the original security standard for Wi-Fi technology. The RC4 encryption algorithm that WEP is based on is no longer considered secure. WEP should not be used to secure your network [3]. It is insecure and can be exploited with a lot of open source tools available on the internet.

WPA (Wi-Fi Protected Access) is an earlier generation of Wi-Fi security certifications, it was introduced in 2003 as an interim solution. The WPA program added support for TKIP (Temporal Key Integrity Protocol) encryption. TKIP is an older form of security technology and has recently been demonstrated to have some vulnerability to cryptographic attacks. WPA is an older version of Wi-Fi security which was replaced in 2004 with more advanced protocols. Though the threat of a security compromise is small, users should not purchase new equipment which supports only WPA with TKIP [3].

WPA2 (Wi-Fi Protected Access II) is the latest version of Wi-Fi security, and it should be used to protect all Wi-Fi devices. WPA2 was introduced in 2004 and has been required in Wi-Fi CERTIFIED products since April 2006. It supports AES, the most advanced encryption standard. AES is the encryption standard endorsed by the US government. The Wi-Fi Alliance recommends that users select equipment supporting WPA2 to help protect their network from known attacks to their security and privacy [3].

There are currently many new and better types of wireless protection protocols but for this research we will not mention them. This paper will deal only with these three basic protections that are most common in the majority of users. Their relations, analysis and statistics will be described further in this paper.

B. Exploitation method

B. Metode eksploatacije

There are many open – source tools that can disrupt the privacy of users. Most of them are easily found on the Internet using a common query in the Google search engine. Not all, but most of them are free and therefore available to all who find and download it from the Internet. Versions that are paid are much more advanced, and with them the threats can seriously disrupt the privacy and security of users, as well as some companies or organizations that are the target of the attack. In this case, there is the possibility of losing large amounts of confidential information, as well as large amounts of cash, property or movable assets. These are some of the ways of exploitation:

BackTrack [4] is a Linux distribution based on Ubuntu or Debian intended for operation in the field of IT security, primarily for penetration testing, digital forensics and investigation. It uses the KDE interface and has many security and forensic tools, and collection tools can be easily upgraded and expanded by downloading from online repositories. For this method you will need to have a Linux computer operating system and knowledge in networking and programming skills. Here is the described way of how it works [5].

Aircrack-ng [6] is a network software suite consisting of a detector, packet sniffer, WEP and WPA/WPA2-PSK cracker and analysis tool for 802.11 wireless LANs. It works with any wireless network interface controller whose driver supports raw monitoring mode and can sniff 802.11a, 802.11b and 802.11g traffic. The program runs under Linux and Windows. To use this method you will need to know a lot about programming and networking. Here is the described way of how it works [7].

Dictionary attack is a method used to break security systems, specifically password – based security systems, in which the attacker systematically tests all possible passwords beginning with words that have a higher possibility of being used, such as names and places. The word "dictionary" refers to the attacker exhausting all of the words in a dictionary in an attempt to discover the password.
Dictionary attacks are typically done with software instead of an individual manually trying each password [8].

These are just some of the methods that are available and it is believed that there are a lot more that the public does not know.
Those unfamiliar modes of exploitation are the main weapon of terrorist organizations against countries and countries against ordinary people. Furthermore, the measurements will be performed with the help of some of these three methods of exploitation because these are most common and mostly used methods around the world and most familiar to users that do this kind of exploitation.

C. City of Sisak

C. Grad Sisak

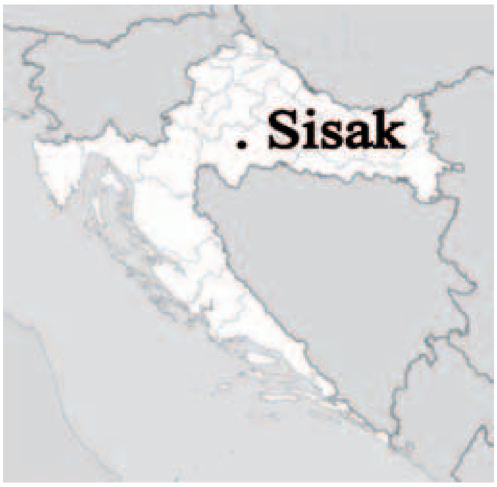


Figure 2 *Sisak location in Republic of Croatia*

Slika 2 *Lokacija Siska u Republici Hrvatskoj*

Sisak is a city in central Croatia located at the confluence of the Kupa, Sava, and Odra rivers, 57 km southeast of the Croatian capital Zagreb. The city's total population in 2011 was 47.768, of which 33.322 live in the urban settlement. Sisak is the administrative center of the Sisačko-Moslavačka županija, Croatia's biggest river port and a center of river shipping industry. It lies on the main road

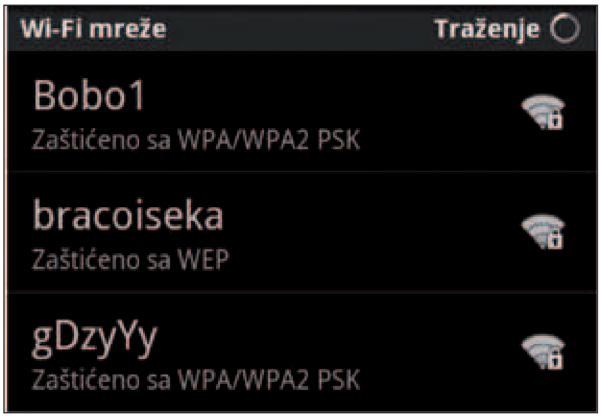
Zagreb-Sisak-Petrinja (M12.2) and the railroad Zagreb-Sisak-Sunja. Sisak is a regional economic, cultural and historical center. The second largest oil refinery in the country (after city of Rijeka) is located here [9]. Sisak has a long and turbulent history behind it. Once a center of industry in the Republic of Croatia, Sisak today shows only a faint image of what it once was. Young people are leaving the city is looking for the hope of a better and more successful life. The industry slowly deteriorates and all that was once a source of success disappears. The only hope for salvation is to find foreign investors who will restore this city to the old paths of glory. It's not impossible and it would bring future prosperity of this city.

2. Measurement

2. Mjerenje

The measurement will be carried out in one day with the help of several people. Each person will be equipped with a laptop or a Smartphone that has the ability to connect to wireless networks. Each detected networks will provide information on the name of the network and the type of protective protocol which uses (WEP, WPA/WPA2). The data will be recorded in specific files and will later be processed. Analysis of graphs will show the results obtained from these measurements.

Measurements will be performed at several measurement sites in Sisak. There will be four measurement locations will cover a specific area of the chosen sites. Places that are selected for measurement are: Zeleni brijeg, Trg, Zibel and Viktorovac. These are one of the largest communities in the city of Sisak and there are a lot of wireless networks and personal computers in that area.



Wi-Fi mreže Traženje

Bobo1
Zaštićeno sa WPA/WPA2 PSK

bracoiseka
Zaštićeno sa WEP

gDzyYy
Zaštićeno sa WPA/WPA2 PSK

Figure 3 Measurement method with Smartphone

Slika 3 Mjerna metoda uz pomoć pametnog telefona

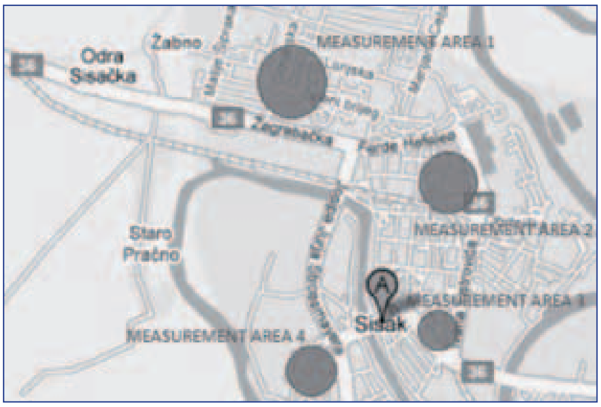


Figure 4 Measurement areas

Slika 4 Područja mjerenja

What is required from the measurements is to get a view of security of the citizens of the city of Sisak. To see whether residents are conscious about security problems in wireless networks or are not aware of this problem. Also that the actual results of measurement probes to raise awareness about the dangers that lurk in everyday life using unsafe protective protocols such as WEP.

3. Results and analysis

3. Rezultati i analita

Measurements have shown that the security of wireless networks in the Sisak is quite insecure. In contrast to the average in the world that is in the ratio of 19% for unprotected networks and 81% for protected networks, measuring in Sisak indicate a substantial deviation. Ratio of protected and unprotected networks in Sisak is 32% compared to 68% percent. It tells us that people are still not aware of the dangers that under-protected network brings. With the previously stated open-source tools better hackers could penetrate 35% to 40% of the listed wireless networks. And that would lead citizens of Sisak in potential danger.

The results also showed that the measurements carried out in the town of Sisak did not detect any open network, i.e. a network that does not have any kind of protection or default password. Such network would be free to connect to all users who would like to join her.

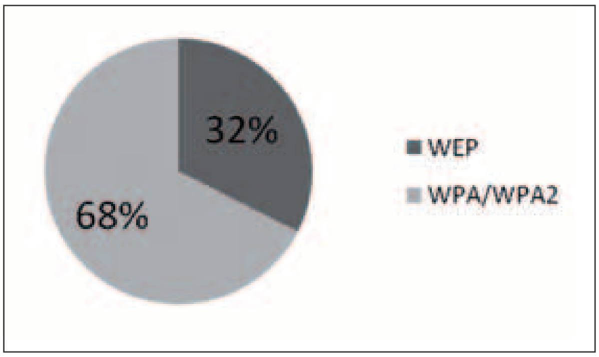


Figure 5 *The ratio of WEP and WAP/WAP2 protection in Sisak*

Slika 5 *Omjer WEP i WAP/WAP2 zaštite u Sisku*

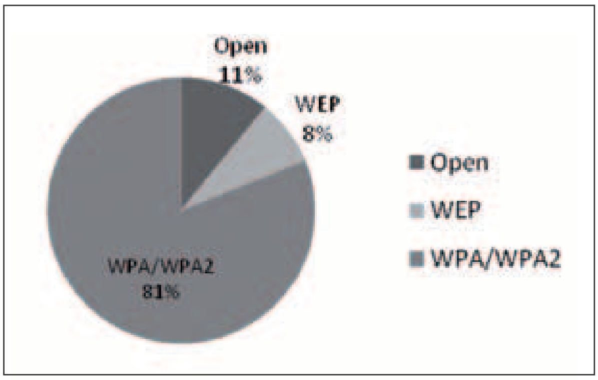


Figure 6 *The ratio of Open, WEP and WPA/WPA2 protection in World (November, 2013)* [9]

Slika 6 *Omjer otvorenih, WEP te WPA/WPA2 zaštita u svijetu (Studeni, 2013)* [9]

The analysis shows that the protection of the town of Sisak must improve. Croatian Criminal Code does not provide for identity theft as a crime. The term "identity theft" is used in the Republic of Croatia in the informal communication that may relate to several offenses which, in general, the ultimate goal of obtaining illegal gain or causing any damage to another [10]. This is why the citizens of the city of Sisak need to improve the protection of their devices that have wireless network and the ability to connect to them. If an unknown threat exploits security of your device, there can be great danger. While connected to the device, threats can download from your computer, and use the data traffic as you can and do illegal things while connected to a network and your IP address. This can lead to national problems if an attempted terrorism or to personal problems when it comes to downloading illegal content from the Internet. And that's only because the threat is connected to your IP address through your unprotected network. Identity theft can lead to big trouble anyone, and since some of it's braches are punishable by law, even if it were unaware of it, you can end up in jail because of their unprotected network.

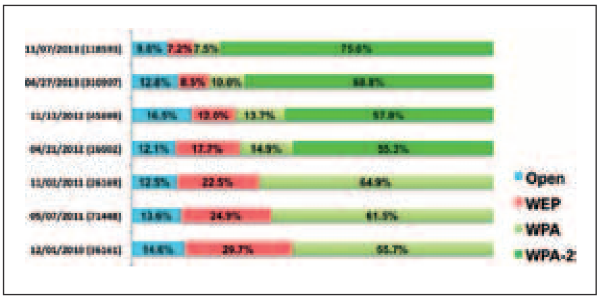


Figure *7 World results of wireless protection ratios for Open networks, WEP, WPA and WPA-2 (December, 2010 – November, 2013)* [9]

Slika *7 Svjetski rezultati omjera zaštite bežičnih mreža za otvorene mreže, WEP, WPA I WPA-2 (Prosinac, 2010 – Studeni, 2013)* [9]

4. Further prevention

4. Daljnja prevencija

People need to be aware of the dangers around them. Educating the people is an essential thing that would lead to improvement of situation that is currently in the town of Sisak. Checking their modem / router, users can configure the wireless security. They can change property protection protocols to one that is better and more secure such as WPA/WPA2 and setting their passwords strong. Thus greatly increasing security and protection from any identity theft or exploitation. Pointing the main points of danger to the society to understand that they have to devote more time for technologies and what it provides. When they realize that problems lurk, then the results of the measurements would greatly improve. Percentage of unprotected networks would have fallen and safety would increase to a better standard and that is the goal of this paper.

5. Conclusion

5. Zaključak

The rapid development of technology brings us a lot of good as well as bad things. Smartphone, laptops and devices are advancing, people live at a faster pace and often endanger themselves. Everyone must be aware of the technology and all that she offers. There are lots of free open-source tools that can be harmful to user privacy. Wireless networks are one of the biggest causes of danger. Exploiting the protection of the protective protocols such as WEP, the user may unknowingly be a victim of identity theft. This could endanger him with a fine or even imprisonment because some branches of identity theft are a criminal law.

Measurements in Sisak show that the percentage of unprotected networks is around 32%, which is slightly higher than the world average of about 19%. This research has proven that it needs to increase the awareness of people in Sisak, as well as people in other cities and regions in the world.

Awareness of the problem and proper training can save many people from potential identity theft over the Internet and thus increasing the safety of them and the people around them.

6. References

6. Reference

[1] National Library of Australia; “Information Technology”; available at: https://www.nla.gov.au/corporate-documents/annual-report/2012-2013/information-technology

[2] Webopedia; “wireless”; available at: http://www.webopedia.com/TERM/W/wireless.html

[3] Wi-Fi Alliance; “How does Wi-Fi Protected Setup work?”; available at: http://www.wi-fi.org/knowledge-center/faq/how-does-wi-fi-protected-setup-work

[4] Archangel Amael; Martin Bos; Emanuele Gentili; “BackTrack Linux”; available at: http://www.backtrack-linux.org/

[5] Gina Trapani; “How to Crack a Wi-Fi Network’s WEP Password with BackTrack “; available at: http://lifehacker.com/5305094/how-to-crack-a-wi+fi-networks-wep-password-with-backtrack

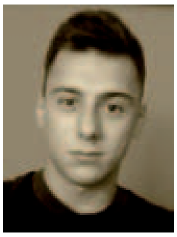
[6] Aircrack-ng; “Description”; available at: http://www.aircrack-ng.org/

[7] occupytheweb; “How to Hack Wi-Fi: Cracking WPA2-PSK Passwords Using Aircrack-Ng”; available at: http://null-byte.wonderhowto.com/how-to/hack-wi-fi-cracking-wpa2-psk-passwords-using-aircrack-ng-0148366/

[8] Webopedia; “dictionary attack”; available at: http://www.webopedia.com/TERM/D/dictionary_attack.html

[10] Ministarstvo unutarnjih poslova Republike Hrvatske; “Sigurnost na društvenim mrežama “; available at: http://www.mup.hr/83255.aspx

AUTHOR · AUTOR



Tomislav Marjanović, bacc.ing. techn.inf. rođen je u Sisku 1992. godine. Nakon završene srednje tehničke škole u Sisku školovanje nastavlja na stručnom studiju Informatike Tehničkog veleučilišta u Zagrebu. Zvanje stručnog prvostupnika stječe 2014. godine te iste godine upisuje specijalistički studij Informatike na istom veleučilištu; usmjerenje elektroničko poslovanje. Dobitnik državne stipendije za najuspješnije studente svoje interese usmjerava prema informacijskoj sigurnosti, uvođenju i implementiranju novih rješenja u informacijske sustave te grani Internet marketinga kojoj posvećuje svoju istraživačku temu završnog rada. Trenutno nezaposlen.

Korespondencija:
tmarjanovic92@gmail.com