Public WiFi Security Network Protocol Practices in Tourist Destination

Sime Lugovic[1], Leo Mrsic[2](✉), and Ljiljana Zekanovic Korona[1]

[1] University of Zadar, Mihovila Pavlinovica, Zadar, Croatia
sime.lugovic@gmail.com, ljkorona@unizd.hr
[2] Algebra University College, Ilica 242, Zagreb, Croatia
leo.mrsic@algebra.hr

Abstract. Paper addresses security issues with public access WiFi networks, with emphasis on networks deployed in touristic places, because of their popularity. Such networks are often poorly administered and guarded whereas tourist-services they support, are massively used by thousands of occasional users daily. With intention to put emphasis on the security awareness of the users, filed research was conducted to investigate current security preferences of wireless computer networks in tourist destination, in the City of Zadar, Croatia. The research was conducted during preparation and early in the tourist season, spring/summer 2018. Hardware research support include AP beacon used a TL-WN722N card with a data rate of 150 Mbps, a 5 db antenna, a chip Atheros AR9271, all powered by Linux operating. Small suite was a passive scan tool for the beacon area. The data set used include the default AP settings that transmits its current SSID every 100 ms. WLAN card was used in the vehicle that was set up in the monitor mode used to collect all the available beacon frames. In addition to field research, we conduct additional survey with aim to investigate the general habits of users of wireless computer networks, from personal perspective. Overall goal was to put attention on WiFi security awareness and to expose security behaviour at router level.

Keywords: Mobile security · Mobile applications security · Domestic appliances security · Identity theft and illicit diffusion of personal data · Law enforcement practices and uses of digital forensics tools · Online frauds

1 Introduction

Public WiFi is a common way for internet access, especially when there is no other easy way of internet access. Paper addresses security issues with public access WiFi networks, with particular emphasis on networks deployed in touristic places, because of their popularity. Such networks are often poorly administered and guarded whereas tourist-services they support, are massively used by thousands of occasional users daily. Being easy to access, users are often not aware that this is not the safest way of internet access. Main challenge, when connecting to public WiFi, is that all information transmitted from your computer is usually available to other devices on that network. That is why such connections can be are extremely dangerous because cyber-attackers can extract usernames, passwords and other information/data from communication stream [1].

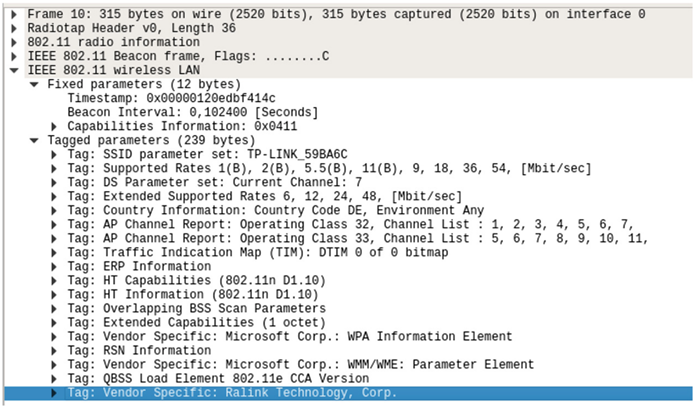
C. Esposito et al. (Eds.): I-SPAN 2019, CCIS 1080, pp. 321–332, 2019.
https://doi.org/10.1007/978-3-030-30143-9_27

Considering that, three most common forms of attack are: Man-in-the-Middle Attacks, Malware/ Evil Twins and Fake WiFi Access Points/WiFi Sniffing. In the first form, the attacker is looking to place attack between user and the computer to which one access by creating network through which user will access. The other form is much more dangerous, because the attacker is physically on your computer. The third form is used very often, because it is based on the attacker taking over enormous amounts of data you send and receive and use that data to extract something useful. WiFi Sniffing is not forbidden, user can even use it on its own, because the attacker takes over everything on the network so it's hard to prove that he just attacked someone. Since no great technological knowledge is required for these methods to take place, the best cure is prevention [3–6].

Sensitive information such as bank accounts and passwords are not to be provided or used on public networks. Using a public network should be reduced to entertainment and surfing the web rather than using tools of importance that sometimes sends your passwords to authorization. It's recommended to limit the quantity of background information on your device because apps in the background often send and receive some data without your permission.

2 WiFi Network Setup and Security Basics

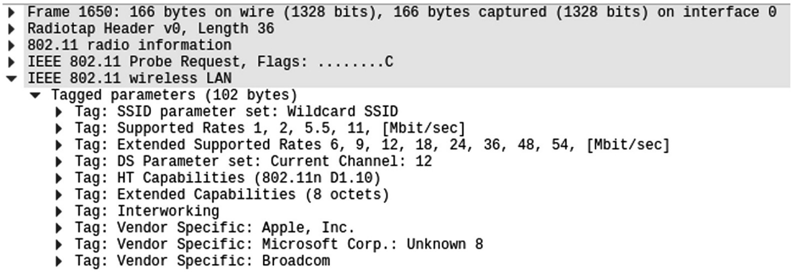
The world today cannot be imagined without wireless networks. WiFi is used to connect mobile devices and computers to the Internet and virtually enable permanent connectivity having instant access to the global network. The trend is that cities or local communities, build their wireless networks to provide Internet access to visitors and citizens. All those networks are common and often use the IEEE 802.11 protocol for air communication (radio waves). However, there are serious security risks when using such networks. For end users, it means connecting to the insecure a network or network that is controlled by malicious tools, can provide their confidential information to unwanted persons. In that case, someone can intercept and spy internet user's traffic and extract information like passwords for accessing the web services and other relevant data. Also, most households have a router with a wireless module that lets you connect wired handsets with your wireless waves cell phones, smartphones and other devices on the Internet. All traffic is being served by commercial Internet service provider (ISP). One of the obvious benefits of wireless connectivity is that it is not cable connected neither limited to one location. On the other hand, challenges include fact that waves, by which data is transmitted, are spreading in all directions and cover the wider area. Everyone can try to connect to "user's" connection point within the range of wireless network, and in case it goes hand in hand, it can execute various malicious actions. Routers are required to be adjusted to today's security standards to prevent malicious users from using it. This internet access threatens the security of other internet users, including those who are connected to the same device. Every device connected to the network passes through a set of procedures that either securely use the network traffic or prohibit it [2].



```
▶ Frame 10: 315 bytes on wire (2520 bits), 315 bytes captured (2520 bits) on interface 0
▶ Radiotap Header v0, Length 36
▶ 802.11 radio information
▶ IEEE 802.11 Beacon frame, Flags: ........C
▼ IEEE 802.11 wireless LAN
  ▼ Fixed parameters (12 bytes)
      Timestamp: 0x00000120edbf414c
      Beacon Interval: 0,102400 [Seconds]
    ▶ Capabilities Information: 0x0411
  ▼ Tagged parameters (239 bytes)
    ▶ Tag: SSID parameter set: TP-LINK_59BA6C
    ▶ Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 9, 18, 36, 54, [Mbit/sec]
    ▶ Tag: DS Parameter set: Current Channel: 7
    ▶ Tag: Extended Supported Rates 6, 12, 24, 48, [Mbit/sec]
    ▶ Tag: Country Information: Country Code DE, Environment Any
    ▶ Tag: AP Channel Report: Operating Class 32, Channel List : 1, 2, 3, 4, 5, 6, 7,
    ▶ Tag: AP Channel Report: Operating Class 33, Channel List : 5, 6, 7, 8, 9, 10, 11,
    ▶ Tag: Traffic Indication Map (TIM): DTIM 0 of 0 bitmap
    ▶ Tag: ERP Information
    ▶ Tag: HT Capabilities (802.11n D1.10)
    ▶ Tag: HT Information (802.11n D1.10)
    ▶ Tag: Overlapping BSS Scan Parameters
    ▶ Tag: Extended Capabilities (1 octet)
    ▶ Tag: Vendor Specific: Microsoft Corp.: WPA Information Element
    ▶ Tag: RSN Information
    ▶ Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Parameter Element
    ▶ Tag: QBSS Load Element 802.11e CCA Version
    ▶ Tag: Vendor Specific: Ralink Technology, Corp.
```

Fig. 1. Beacon frame

Figure 1 shows an example of a beacon packet that each Access Point emits approximately every 100 ms (default) during active time, or while SSID broadcasting is enabled. The beacon packet can read different field values. The SSID parameter field detects the network name (if SSID broadcasting is configured), supported rates, and extended support rates, detects supported speeds or data rates that can be used to detect which 802.11 protocol is working. The AP also advertises its current channel where communication takes place (ranging from channel 1 to 14), while optionally we can determine which chipset the AP uses (in our sample case, it is Railink Technology).



```
▶ Frame 1650: 166 bytes on wire (1328 bits), 166 bytes captured (1328 bits) on interface 0
▶ Radiotap Header v0, Length 36
▶ 802.11 radio information
▶ IEEE 802.11 Probe Request, Flags: ........C
▼ IEEE 802.11 wireless LAN
  ▼ Tagged parameters (102 bytes)
    ▶ Tag: SSID parameter set: Wildcard SSID
    ▶ Tag: Supported Rates 1, 2, 5.5, 11, [Mbit/sec]
    ▶ Tag: Extended Supported Rates 6, 9, 12, 18, 24, 36, 48, 54, [Mbit/sec]
    ▶ Tag: DS Parameter set: Current Channel: 12
    ▶ Tag: HT Capabilities (802.11n D1.10)
    ▶ Tag: Extended Capabilities (8 octets)
    ▶ Tag: Interworking
    ▶ Tag: Vendor Specific: Apple, Inc.
    ▶ Tag: Vendor Specific: Microsoft Corp.: Unknown 8
    ▶ Tag: Vendor Specific: Broadcom
```

Fig. 2. Probe request

Beacon frames from AP allow devices (supplicants) to detect when they are within communication reach, and automatically log in to the network if the fields match. User devices that have WiFi enabled send test request packets that are in the service of detecting currently available networks or detecting whether the pre-available networks are still available. Figure 2 shows an example of a device request package that has a wildcard parameter set for the SSID field. The wildcard parameter is actually a parameter that searches for all available networks, or checks which networks are all within the range of the device (because each letter can be a wildcard *). Also, the device announces its available transmission speeds that detect the current 802.1

protocol that it uses. It should be noted that devices that are not connected to any network and have WiFi enabled at time intervals, send test requests to refresh a list of available networks. This is a way of testing requests for all the available channels from 1 to 14 that all APs are listening in range and then AP * and responds with a frame containing SSID and other fields [7]. The schematic view of the probes for the specific SSID and for the null (wildcard) variance is shown in Fig. 3.

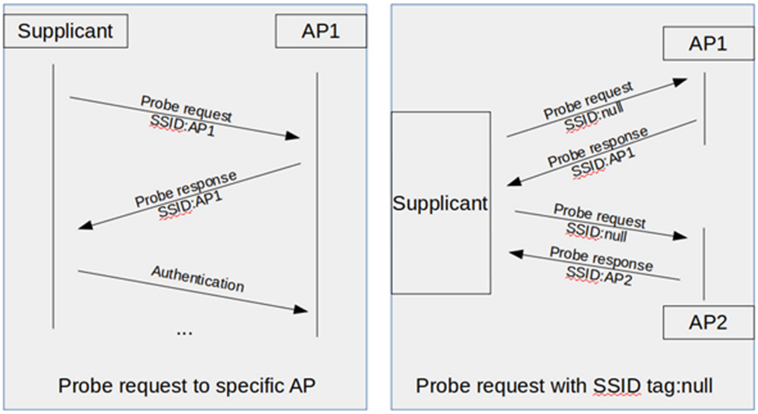


Fig. 3. Probes for the specific SSID/wildcard

3 WEP Security Protocol and Its Vulnerabilities

The WEP security protocol can be simple protection choice, because it is the easiest to implement when it comes to the needs for backward compatibility solutions. WEP disadvantages include usage of RC4 which is a symmetric stream chiper. RC4 uses the OR operator which encodes the message and deliver chipertext [8].

Security protocols for wireless networks can be listed as: WEP, WPA, WPA2. Protocols differ in the level of security they provide. The security level is defined as three different security points known as the “CIA”: Confidentiality, Integrity, Authentication. Data privacy is achieved by encryption that ensures that an attacker cannot read packets when he or she analyse network traffic using sniffers. The integrity check verify that the message has not been changed in the transmission by monitoring the integrity check value (ICV) at the end of the packet. Authentication ensures that the recipient accepts messages only from trusted senders [12] (Fig. 4).

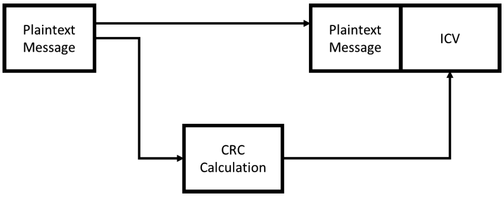


Fig. 4. CRC calculation

WEP, abbreviation for Wired Equivalent Privacy, is a protocol that has copied the level of security on wireless networks to the level that computers have in the network connected to the cable. The implementation of this protocol has opened the door to attackers in the network because of its vulnerability in its application. WEP does not offer any authentication when using the network, which means that there is no identity check or packet source within the network making the network vulnerable to MITM attacks [9] (Fig. 5).

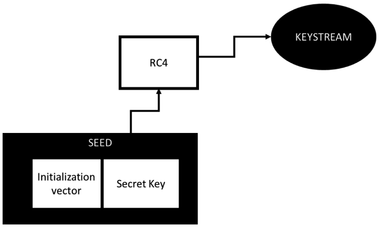


Fig. 5. RC4

Privacy with WEP protocol is achieved by implementing the RC4 encryption algorithm. The RC4 algorithm encrypts the message in a way that uses an initialization vector (IV) as input, which must be 1 higher for each new packet and the key. The output is a stream chipper that encrypts the message so that each bit is inversed using the OR logic. Vulnerability points from the situation where the 802.11 standard for WEP does not prescribe, come from scenario where each packet must have a new IV, meaning that the attacker may, by listening to the traffic, intercept packets that have the same IV (IV are not encrypted but have been added as a plaintext number at the end of the packet). Once the attacker has a duplicate IV, it can easily detect plaintext, since the protocols have a clearly defined structure, and the messages that require, for example, login often look unified.[1] WEP weaknesses can be described as: initialization vector number sent as plaintext in packet, limited rage of diverse IV and no shared key recheck process after initial authentication [14].

The WEP Wireless Encryption Protocol (WEP) is a protocol intended for wireless network security, part of the IEEE 802.11 standard. The WEP protocol encrypts data that travel between a user and an access point with a shared key. The user must have the appropriate WEP key to communicate with the access point. The WEP Encryption Protocol uses a 64-bit or 128-bit RC4 algorithm, and the CRC-32 algorithm is used to provide data integrity. It has been shown that such a security mechanism can be exploited by publicly available tools and is not recommended as an adequate safeguard measure. WPA and WPA2 Wi-Fi Protected Access (WPA) is a security mechanism designed to correct shortcomings in WEP protocol. WPA uses dynamically changing TKIP keys and the “Michael” algorithm for integrity checking. WPA2 as an enhancement instead of RC4 uses a variant of the AES encryption algorithm but is not

[1] http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html.

supported on older network interfaces. For authentication, WPA supports 802.1x, but a less secure shared-key system can also be used - users must know a common key to connect to the network [10].

4 WiFi Networks Vulnerabilities: Attack and Protection Tactics and Practices

Using various malicious software, the attacker is able to attack the system, expel users from the network, and hinder the normal operation and attack. After they've been excluded from the network, users are trying to sign back on to the network. The cellular phones are again running the process of association and authentication with AP and are sending packets that contain a shared secret key. After attacking the packets, saving them to the local system and no longer having to risk exposure at the location of the attack, brute-force techniques can break through the password and, if not changed in the meantime, return to the range of the network and sign up as a legitimate user. In addition to the security protocols WPA and WPA2, there are also alternative network protection methods that are not really, but they are important because they are often present in networks. The SSID cloaking technique is used to stop the broadcasting of the network and thus prevent malicious users from entering the network, ie, users can access the network only if they know in advance its name (SSID) and password, and they manually enter and request access [13]. This technique is not particularly effective due to the fact that when a legitimate user reaches the reach of the hidden network, the device sends a request packet while the AP sends a trial response packet, both containing the network name, and if WEP is used together with the cloaking method, the network is extremely vulnerable and exposed to attacks. The network protection technology of MAC protection or router protection so that only devices with a particular MAC address can access the network is also a false security. Deciphering an address is an extremely simple and trivial undertaking, so the question of whether the MAC filtering technique can be placed in network protection techniques [11]. Windows Vista even has the option to send probe request (null) automatically and revert to two categories of networks, those that have both non-configured broadcasts[2].

5 Public Access WiFi Networks Security Protocols Practices in Tourist Destination

With intention to put emphasis on the security awareness of the users, filed research was conducted to investigate current security preferences of wireless computer networks in tourist destination, in the City of Zadar, Croatia. The research was conducted during preparation and early in the tourist season, spring/summer 2018. Hardware research support include AP beacon used a TL-WN722N card with a data rate of

[2] https://support.microsoft.com/en-us/help/929661/connecting-to-non-broadcast-wireless-networks-in-windows-vista.

150 Mbps, a 5 db antenna, a chip Atheros AR9271, all powered by Linux operating. Small suite was a passive scan tool for the beacon area. The data set used include the default AP settings that transmits its current SSID every 100 ms. WLAN card was used in the vehicle that was set up in the monitor mode used to collect all the available beacon frames. In addition to field research, we conduct additional survey with aim to investigate the general habits of users of wireless computer networks, from personal perspective. Overall goal was to put attention on WiFi security awareness and to expose security behaviour at router level. The survey had nine questions, of which only one was of an open type, while the rest were closed type. The poll was filled by 64 people and all the polls were taken into account. The first question in the survey was the classification of dependent respondents to which neighbourhood in City of Zadar belonged (Fig. 6).

The second question related to physical access to the router, more than 80% of the respondents answered this question more accurately (Table 1).

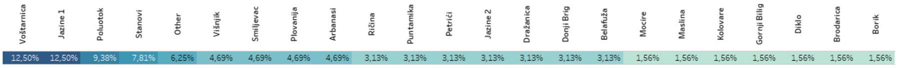


Fig. 6. City of Zadar areas/respondents

The third question was: “If you have access to the router, can you” access “the router? (Logged in as admin/user in router settings …)”. 49% of respondents answered positively while 43% answered negatively. Some less than 8% of respondents did not answer this question (Table 2).

Table 1. Router availability

Q1: Do you have physical access to router?	Number of answers
Yes	51
No	13

Table 2. Router access

Q2: If you have physical access to router, do you have skills to log-on? (admin log-in or similar access to router settings)	Number of answers
Yes	31
No	28

The fourth question was to examine whether network users have changed their settings so far. 39% of respondents answered positively while 59% answered negatively. Some less than 2% of respondents did not answer this question (Table 3).

Table 3. Router settings

Q3: Did you ever changed default router settings?	Number of answers
Yes	25
No	38

The next question was the question of multiple choice through which the habits of changing the default settings were examined. Majority of respondents, 44% of the total number, respond they changed the default settings (25), changed the name of the network and the PSK (Table 4).

Table 4. Router administration

Q4: If you changed router default settings, which one did you change (multiple answers)?	Number of answers
No answer	38
EssID (network name), Password (PSK)	11
EssID (network name), Password (PSK), Security level (WEP, WPA, WPA2)	1
EssID (network name), Password (PSK), Security level (WEP, WPA, WPA2), WiFi Channel	4
EssID (network name), Password (PSK), Security level (WEP, WPA, WPA2), WiFi Channel, MAC filtering, port forwarding	1
Password (PSK)	5
Password (PSK), WiFi Channel	1
Password (PSK), Security level (WEP, WPA, WPA2)	2
Password (PSK), Security level (WEP, WPA, WPA2), WiFi Channel	1

6 Field Research Results

Total number of records collected was 16.982, while only 2.81% networks were without any protection protocol set. Less than 10% of all records indicate cloaked parameter set. WEP protection protocol was set only on 3.07% records (counting 522 records), 33 being cloaked (Fig. 7).

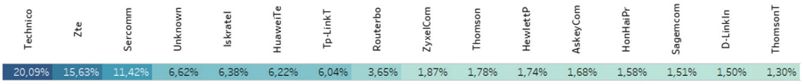


Fig. 7. Router ratio by manufacturer (top rated)

It is noticed that most popular router manufacturers are using default settings which include various kinds of encryption protocols, however most likely not WEP (Figs. 8 and 9).

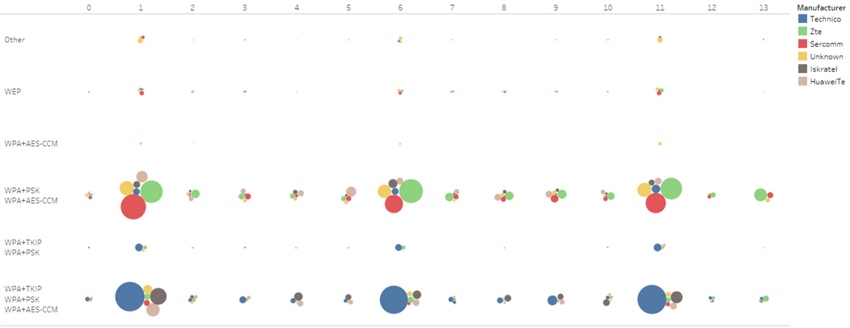


Fig. 8. Channel/router manufacturer/encryption ratio (top manufacturers)

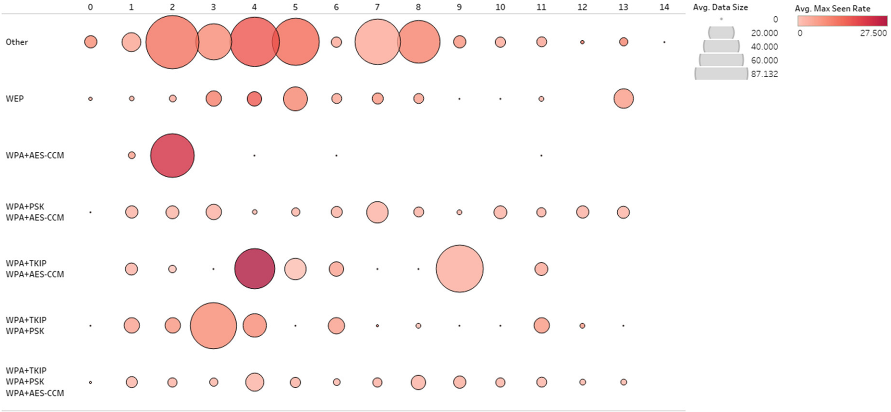


Fig. 9. Channel/encryption/data size/max seen rate ratio (all)

Significant data volumes are related to non-encrypted connection points while most used channels are 1, 6 and 11. In order to put attention on WiFi security awareness and to expose security behaviour at router level, city map was generated showing behaviour patterns and locations covered by WiFi signal (Fig. 10).

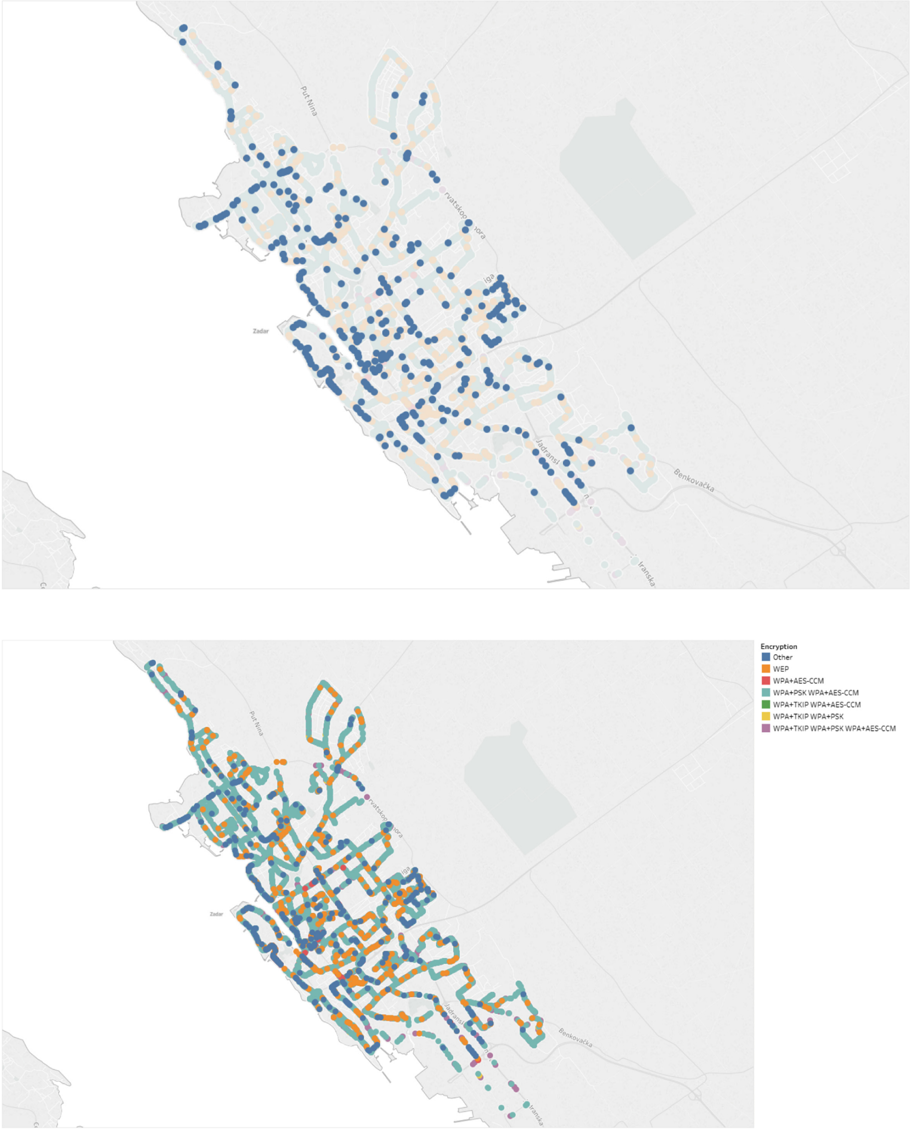


Fig. 10. City of Zadar WiFi/encryption city map (right), access points without encryption (left)

7 Conclusion

Paper addresses security issues with public access WiFi networks, with emphasis on networks deployed in touristic places, because of their popularity. Such networks are often poorly administered and guarded whereas tourist-services they support, are massively used by thousands of occasional users daily. With intention to put emphasis on the security awareness of the users, filed research was conducted to investigate current security preferences of wireless computer networks in tourist destination, in the City of Zadar, Croatia. Overall goal was to put attention on WiFi security awareness and to expose security behaviour at router level.

WiFi security protocols practices in tourist destination based on City of Zadar case, must be monitored carefully and used to engage and motivate access point owners to pay more attention on user behaviour to increase overall access point protection for all users. Large number of owners are relying on default setup for router and management while majority of users are using non encrypted access points.

Wireless networks provide great mobility, while they open new areas of connectivity but are open to various and new security vulnerabilities. The safety of wireless networks due to the properties of wireless media is more sensible and needs to be put in perspective and treated with caution. The speed of wireless network implementation needs to analyse security issues, the level of protection required, and the financial costs needed to achieve that level of protection. Because of the characteristics of wireless networks, they will probably represent the most effective and most vulnerable network segment suitable for cyber-attack. This paper is putting emphasis on the security awareness of the users, showing the most common vulnerability points and ways of reducing risk. Decision on level of protection that will be applied on specific location, primarily depends on the needs and the technical knowledge/possibilities. It is important to emphasize that the security system is dynamic, and that the only way to minimize risk is to keep track of the development of technology, to patch application and upgrade regularly, to apply precise defensive security policies and procedures, and to continuously invest in staff training and administrator recommendations.

References

1. Aime, M.D., Calandriello, G., Lioy, A.: Dependability in wireless networks: can we rely on WiFi? IEEE Secur. Priv. **5**(1), 23–29 (2007)
2. Bachman, R., Saltzman, L.E., Thompson, M.P., Carmody, D.C.: Disentangling the effects of selfprotective behaviors on the risk of injury in assaults against women. J. Quant. Criminol. **18**(2), 135–157 (2002)
3. BT Wi-fi (n.d.a) Find a Hotspot. https://www.btwifi.co.uk/find/
4. BT Wi-fi (n.d.b) Security when Using BT's Wi-fi Hotspots. https://www.btwifi.co.uk/help/security/index.jsp
5. BT Wi-fi (n.d.c) BT Wi-fi Protect. http://www.btwifi.com/Media/pdf/WIFI_PROTECT_250313_wifi.pdf
6. BT Wi-fi (n.d.d) Terms and Conditions. BT Wi-fi Acceptable Use Policy (including BT Openzone). http://www.btwifi.com/terms-and-conditions/acceptable-use-policy.jsp
7. Cheng, N., Xinlei, W., Wei, C., Prasant, M., Aruna, S.: Characterizing privacy leakage of public wifi networks for users on travel. In: Proceeding of INFOCOM 2013. IEEE (2013)
8. Guerette, R.T., Santana, S.A.: Explaining victim self-protective behavior effects on crime incident outcomes: a test of opportunity theory. Crime Delinq. **56**(2), 198–226 (2010)
9. Holt, T.J., Bossler, A.M.: An assessment of the current state of cybercrime scholarship. Deviant Behav. **35**(1), 20–40 (2014)

10. Lalonde Lévesque, F., Nsiempba, J., Fernandez, J.M., Chiasson, S., Somayaji, A.: A clinical study of risk factors related to malware infections. In: Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security, pp. 97–108. ACM (2013)
11. Spacey, R., Cooke, L., Muir, A.: Regulating use of the Internet in public libraries: a review. J. Doc. **70**(3), 478–497 (2014)
12. Castiglione, et al.: Virtual lab: a concrete experience in building multi-purpose virtualized labs for Computer Science Education. In: Proceedings of: SoftCOM 2012, 20th International Conference on Software, Telecommunications and Computer Networks, Split (HR), 11–13 September 2012. IEEE (2012)
13. Catuogno, L., Turchi, S.: The Dark Side of the Interconnection: security and Privacy in the Web of Things (2015). https://doi.org/10.1109/imis.2015.86
14. Gast, M.S.: 802.11 Wireless Networks: The Definitive Guide: The Definitive Guide, O'Reilly Media, Sebastopol (2005)
15. Lalonde Lévesque, F.L., Fernandez, J.M., Somayaji, A.: Risk prediction of malware victimization based on user behavior. In: Malicious and Unwanted Software: The Americas (MALWARE) (2014)