Advanced Research on Information Systems Security

ISSN: 2795-4609 | ISSN: 2795-4560
Print & Online

(In)Security in Wi-Fi networks: a systematic review

Diogo Faíscas*

ISLA – Polytechnic Institute of Management and Technology, Vila Nova de Gaia, Portugal
Email: diogo.faiscas@sapo.pt

Abstract

Everyone wants to be connected to the internet at every second of their lives. Due to the ease and speed of access, Wi-Fi networks are the main internet connection point of users. The amount and coverage of Wi-Fi networks multiplies each passing day, as all the countries are now trying to give free Wi-Fi at public places. If we search for available networks anywhere with our phone, there will be very few places where there are not at least one or two networks available. In this paper we will do a systematic review of papers and literature indexed in Google Scholar; Research Gate or IEEE and on reliable webpages like Cisco, that analyze the risk to which Wi-Fi networks are exposed and why these networks are insecure. We will specially investigate the most used wireless security protocols like WEP; WPA; WPA2 or WPA3.

Keywords: wireless security; threats; wep; wpa

* Corresponding author. Email address: diogo.faiscas@sapo.pt

1. Introduction

Most of the devices that are used by people to access the internet are portable (mobile phones, tablets, and laptops) and this makes it not functional to connect a cable each time they want to connect to the Internet. On mobile phones and tablets that is not even possible because it does not have an interface for that, and most modern laptops also do not have an RJ45 port. Due to the ease and speed of access, Wi-Fi networks are increasingly the main internet connection point for users (it is easier and faster to connect a Wi-Fi network than connecting a cable).

More than 75% of the last-mile Internet traffic of today's mobile system is delivered via Wi-Fi, which thereby has also become an enticing target for various security threats [1]. Criminals exploit security vulnerabilities of Wi-Fi access points (APs) to eavesdrop on wireless traffic, to launch phishing attacks through DNS hijacking. Furthermore, adversaries not only compromise existing Wi-Fi APs, but also deploy malicious Wi-Fi-based edge devices. Currently, Wi-Fi-based attacks have become worldwide security threats, affecting hundreds of millions of end users [1]. And people are not aware of the risks they take when they connect to an unknown network, like is demonstrated on [2].

In companies, for reasons of security and internet speed, there is still preference for cable. Although Wi-Fi networks are increasingly evolved and there are already access points in the market that allow extremely fast internet speeds, there is always a wall or a barrier that prevents the signal reach the destination with the necessary strength and for this reason the preference continues to fall for a stable connection through cable.

On the other hand, in their homes people give preference to wireless networks. In houses with more than 10/15 years we do not have network ports in all divisions. In new homes there might be RJ45 ports in all divisions, but if we decide to change the location of our desk? If in the context of work, it is even tolerated that there is a cable tray to pass network cables to each workstation, at home this would be unthinkable. It would ruin any home decoration. In addition, it would be necessary to have a mini rack, with all the cables inserted in a ruler, to later connect to a switch, which would need to have at least 24 ports to be possible the cable reach all divisions and equipment of the house. And yet it wouldn't be easy to connect.

This exponential increase of people connected by Wi-Fi, especially in the last 10 years, increases the risk to which we are all subject. It does not matter how good the network intrusion policies are and how good the firewall is, from the moment a user can access the Wi-Fi network, it's like physically connecting a network cable to that network.

In this work we will address the growing risks with Wi-Fi networks, especially with the four most used security protocols (WEP; WPA; WPA2 or WPA3) and ways to mitigate them.

1.1. Why this is critical?

Preventing unauthorized access to a Wi-Fi network is essential for several reasons. Let's imagine some scenarios that can happen, in context of residential or enterprise networks:

- Let's imagine a citizen who lives in a building with several apartments. A neighbor who is within range of his Wi-Fi network and can access it, can commit several crimes with his network and incriminate him. This citizen may obviously be able to prove his innocence, but he certainly won't get rid of a house search and have his life searched by the authorities.
- Let's imagine a company that has high-value items or even cash in its facilities. A criminal can daily have coffee in a coffee shop contiguous to the company and attack the Wi-Fi network. Once he has accessed and had that main barrier broken, he can exploit various equipment, including video surveillance cameras. As CCTV usually are not accessed very often, a lot of organizations have outdated and vulnerable firmware. With access to

the organization's CCTV system, the criminal can see the times when there is no one in the company, know the place and type of items that are stored and the type of doors or safes. Which means a person with bad intentions can do an in-depth study of what he may up against if he wants to carry out a robbery.

- Let's imagine a third scenario: a law firm or an insurance agent, who has sensitive personal data stored in their computer systems. And they even have a good firewall, with undue access from abroad virtually impossible. However, they have a low-quality AP. A criminal manages to overcome the Wi-Fi barrier with some ease and after being inside the network, accesses several folders and files that are shared unprotected on the network and copy files with personal data.

What is intended to demonstrate with these examples is that it does not matter if an organization has an excellent firewall or an effective access control policy if the Wi-Fi access point is not equally secure. Security of data in Wi-Fi networks is as important as having access to the Internet.

2. WLAN Protocols

The rapid deployment of wireless networks, combined with an increasing demand for performance and security, has resulted in significant evolution of the IEEE 802.11 standards. Today, Wi-Fi 6 (IEEE 802.11ax) is the most advanced standard and can achieve data rates over 10 Gbps. Similarly, the security of Wi-Fi networks have come a long way since the introduction of WEP. Nevertheless, the adoption of new standards and prompt deprecation of older and vulnerable protocols remains the main key to securing Wi-Fi networks. In this part Internet Service Providers (ISPs) have a big role to play, in phasing out deprecated protocols and adopting new and more secure standards on the routers of their customers [3].

IEEE 802.11 standard defines communication among networks at the MAC layer by exchanging three frames: viz, control frames, data frames, and management frames. A robust security requirement at the MAC layer is to provide confidentiality, authentication, and Integrity of the frames to be exchanged. IEEE 802.11 defines models, namely pre-Robust and robust security networks, to secure the information Exchange in wireless networks. The Pre-RSN (Robust Security Networks) includes Wired Equivalent Privacy (WEP), and Wi-Fi protected Access (WPA), while as RSN model uses a four-way handshake to provide authentication [4].

There are four main wireless-security protocols. These protocols were developed by the Wi-Fi Alliance, an organization that promotes wireless technologies and interoperability. The group introduced three of the protocols, described below, in the late 1990s. Since then, the protocols have been improved with stronger encryption [5]. The fourth protocol (WPA3) was released in 2018, as a replacement to WPA2, which offers forward secrecy and mitigates security vulnerabilities caused due to poor choice of passwords [3].

2.1. WEP

The first wireless security protocol was WEP (Wired Equivalent Privacy). It was the standard method of providing wireless network security from the late 1990s until 2004. WEP was hard to configure, and it used only basic (64-/128-bit) encryption [5]. Wired Equivalent Privacy uses the RC4 cipher algorithm to encrypt data with a pre-shared key length of 64 to 128 bits. As a first-generation security solution, WEP was vulnerable due to limitations

in key size (initially 40 bits, later extended to 104 bits) and its lack of replay detection. As a result, users had to complement WEP with Virtual Private Networks (VPNs), IEEE 802.1X, or proprietary solutions to meet their security needs [4]. WEP is no longer considered secure and should be replaced by a newer protocol such as WPA2 [5]. Article [6] describes an easy way to crack WEP authentication.

2.2. WPA

WPA (Wi-Fi Protected Access) was developed in 2003. It delivers stronger (128-/256-bit) encryption than WEP by using a security protocol known as Temporal Key Integrity Protocol (TKIP). Along with WPA2, WPA is the most common protocol in use today. But unlike WPA2, it is compatible with older software [5]. It is used for home or organizational network.

Commercial WPA uses 802.1x +EAP for authentication and replaces WEP with TKIP in this mode; no pre-shared key (PSK) is used but instead RADIUS server is required [4]. Using a PSK of less than 20 characters is very unsafe. Article [7] demonstrates that although the method to crack the WPA-PSK is not trivial, it also is not beyond the reach of an average Linux user. Home users can lessen their security risks by using a passphrase significantly greater than 20 characters or, alternatively, by using WPA-Enterprise and incorporating an authentication server, like RADIUS. Corporate users should implement an authentication server, use per-user keying and refrain from implementing WPA in PSK mode.

2.3. WPA2

WPA2, a later version of WPA, was developed in 2004. It's easier to configure and provides even greater network security than WPA by using a security protocol known as the Advanced Encryption Standard (AES). Versions of the WPA2 protocol are available for individual users and enterprises [5]. This protocol is probably the most widely used worldwide today.

Article [6] describes WPA2 as a protocol that uses a key size of 128 bits for the encryption of data. The AES Encryption process in WPA2 is done either by AES or by using TKIP. WPA2 creates secure communication in four phases. The first phase being authentication and pre-authentication method. In this phase AP and the client will agree on security policy. In the second phase a master key will be generated. In the third phase temporal keys will be created in a regular manner. In phase four, all keys generated in phase three will be used by CCMP protocol to provide data integrity and data confidentiality. [6].

However, on article [8] it's provided a survey to almost 400 people, that shows most of the population that uses this protocol is vulnerable. In this paper we can see that about 60% of the examined users, have a password with 12 characters or less on their Wi-Fi, and 61% never change it. As we can imagine, this is a can bring several security issues.

2.4. WPA3

A new generation of WPA, known as WPA3, is designed to deliver simpler configuration and even stronger (192-

/256-/384-bit) encryption and security than any of its predecessors. It is also meant to work across the latest Wi-Fi 6 networks [5]. All devices powered by WPA3 use the latest security measures, do not allow expired asset policies, and require the use of protected frames (PMF). However, article [9] shows that multiple stations are still able to be downgraded on WPA3-TM networks. In their work downgrades were all achieved using ten-year-old consumer hardware with no special or proprietary software and low inherent difficulty to perform. Both the Apple iOS and macOS stations would auto-connect to a WPA2 only SSID, even when they initially connected using SAE on a WPA3-TM enabled AP, and thereby exposing the necessary information to crack the PSK. Because Windows and Network Manager only establish a connection using the stored AKM, they are not affected if the previous connection was made using WPA3 [11], [12].

According to article [10], WPA3 contains very strong security mechanisms which fix many of the issues found in older standards. However, it's full adoption will likely take several years. It's common sense that most of the users have a low level of security knowledge and skills, so it is very unlikely they suddenly become more capable of knowing that they need to upgrade to WPA3 [12]. Besides that, there's also a long road to go on to upgrade all IoT devices to WPA3. And this applies not only to final users, but also to cybersecurity workers and manufacturers as well, because in nowadays not all devices are ready for WPA3 [13], [14].

3. Conclusion

All the four protocols have vulnerabilities. The older protocols are more vulnerable than the recent ones. There's not a 100% method, but obviously we can take some procedures to improve security and mitigate the problem. WEP and WPA are deprecated solutions with a lot of known vulnerabilities and should not be used even in domestic environment.

3.1. On enterprise context

- Having 2 Wi-Fi networks and segregate the main services of the organization from the general internet access.
- In the main network, the connection should never be established with a pre-shared key, but with server authentication, like RADIUS or AD.
- Every time an employee leaves the organization, his access should be immediately revoked.
- On the segregated network (e.g., guest), should be impossible to reach devices on the main network.
- Use only WPA2 or WPA3 protocols and, again, never use a PSK.
- If using WPA2, define a timeline to upgrade to WPA3 as soon as possible. WPA3 is not 100% secure but is harder to crack than WPA2.
- On workstations that are always in the same place, consider connect those devices by cable if possible.

3.2. On residential context

- Almost all residential consumers will not invest in expensive solutions, so having a domain controller server or an expensive router or firewall with RADIUS built in, normally is not an option.
- But there are a few access points in the market not very expensive that allow creation of segregated networks.

This way, it's possible to use a main network for all the resident devices and give a limited and separated network to a guest.

- Using WPA3 is naturally the best option, but not all devices are ready to that.
- If WPA3 is not an option, use WPA2 with RADIUS server or a pre-shared key (PSK), with, at least, 20 characters long and with numbers, symbols, lower- and upper-case letters and replace it every 6 months.

4. References

[1] D. Gao, H. Lin, Z. Li, F. Qian, Q. A. Chen, Z. Qian, W. Liu, L. Gong and Y. Liu, "A Nationwide Census on WiFi Security Threats: Prevalence, Riskiness, and the Economics," MobiCom '21: Proceedings of the 27th Annual International Conference on Mobile Computing and Networking, pp. 242-255, October 2021.

[2] P. F. Wilbur, "HACKERNOON. A hacker intercepted your WiFi traffic, stole your contacts, passwords, & financial data.," 2 february 2019. [Online]. Available: https://hackernoon.com/a-hacker-intercepted-your-wifi-traffic-stole-your-contacts-passwords-financial-data-heres-how-4fc0df9ff152. [Accessed 2022 december 3].

[3] D. Schepers, A. Ranganathan and M. Vanhoef, "Let Numbers Tell the Tale: Measuring Security Trends in Wi-Fi Networks and Best Practices," in WiSec '21, Abu Dhabi, United Arab Emirates, 2021.

[4] Z. A. Najar and R. N. Mir, "Wi-Fi: WPA2 Security Vulnerability and Solutions," Wireless Engineering and Technology, vol. 22, pp. 15-22, 18 April 2021.

[5] Cisco, "What Is Wi-Fi Security?," [Online]. Available: https://www.cisco.com/c/en/us/products/wireless/what-is-wi-fi-security.html#~q-a. [Accessed 4 december 2022].

[6] A. Sharma, T. Bhatia, A. Katyar and S. E. U, "Wireless Security – An Introduction to Wireless Security Protocols and their Security Flaws," Annals of R.S.C.B., vol. 25, no. 6, pp. 11805-11812, 2021.

[7] J. L. MacMichael, "Auditing Wi-Fi Protected Access (WPA) Pre-Shared Key Mode," Linux Journal, 28 july 2005.

[8] D. J. Fehér and B. Sándor, "Effects of the WPA2 KRACK Attack in Real Environment," in IEEE 16th International Symposium on Intelligent Systems and Informatics, Subotica, Serbia, 2018.

[9] E. Lamers and R. Dijksman, "Securing home Wi-Fi with WPA3 personal," in 2021 IEEE 18th Annual Consumer Communications & Networking Conference (CCNC), 2021.

[10] G. Sagers, "WPA3: The Greatest Security Protocol That May Never Be," in 2021 International Conference on Computational Science and Computational Intelligence (CSCI), 2021.

[11] Duarte, N., Coelho, N., Guarda, T. (2021). Social Engineering: The Art of Attacks. In: Guarda, T., Portela, F., Santos, M.F. (eds) Advanced Research in Technologies, Information, Innovation and Sustainability. ARTIIS 2021. Communications in Computer and Information Science, vol 1485. Springer, Cham. https://doi.org/10.1007/978-3-030-90241-4_36

[12] F. Alves, N. Mateus-Coelho and M. Cruz-Cunha, "ChevroCrypto – Security & Cryptography Broker," 2022 10th International Symposium on Digital Forensics and Security (ISDFS), Istanbul, Turkey, 2022, pp. 1-5, doi: 10.1109/ISDFS55398.2022.9800797.

[13] N. Mateus-Coelho and M. Cruz-Cunha, "Serverless Service Architectures and Security Minimals," 2022 10th International Symposium on Digital Forensics and Security (ISDFS), Istanbul, Turkey, 2022, pp. 1-6, doi: 10.1109/ISDFS55398.2022.9800779.

[14] Nuno Mateus-Coelho, A New Methodology for the Development of Secure and Paranoid Operating Systems, Procedia Computer Science, Volume 181, 2021, Pages 1207-1215, ISSN 1877-0509, https://doi.org/10.1016/j.procs.2021.01.318.