TESTS AND EVALUATES THE EFFECTIVENESS OF NETWORK SECURITY (WIFI) AGAINST EXTERNAL THREATS

Yasir Khudheyer Abass Aloubade
Iraqi Ministry of Education , General Directorate of Education Baghdad Karkh3,
Planning Department , Information and Communication Division.
yasirkhuiraq@gmail.com
ORCID: 0000-0001-9976-5406

Abstract

The protection of the network (IEEE 802.11) means protection from possible external threats and attacks, which occur as a result of a weakness in network security protocols and lead to the penetration of users, so our study aims to search for potential threats to the Wi-Fi network based on the standard (IEEE 802.11) and evaluate these threats that are being violated By using programs and devices and revealing them to government institutions, companies and users in order to maintain the security of their information, personal data and digital transactions, Where solutions were given for each potential penetration, gaps were identified, and the level of risk was determined., as well as rationalizing the user for the optimal correct use of Wi-Fi networks and how to use the most secure networks, where the protection of users' data and their information is one of the important priorities for users to trust networks in all transactions.

Keywords: Wi-Fi wireless network, standard IEEE 802.11, Information Technology and communication, Iraqi Ministry of Education .

1. Introduction

The rapid development of wireless networks has led to the fact that the lack of support for Wi-Fi technology in modern manufactured devices is a serious drawback for a potential user. The ability to get rid of the placement of cables or wires and go to the network almost anywhere attracts more and more people who want to take advantage of this. Simplicity, mobility and convenience of placement of a new access point allow the use of wireless networks in many areas of life: from a small apartment to a huge factory.

Such widespread use attracts not only ordinary users, but also those who want

ResearchJet Journal of Analysis and Inventions
https://reserchjet.academiascience.org

to penetrate such networks and intercept information within it. In parallel with the development of wireless technologies, the means of intercepting wireless signals also developed. And already here difficulties arise due to the fact that the only physical boundary of the Wi-Fi network is the signal level itself, which is limited only by power, but not by premises or other physical obstacles. This allows attackers in close proximity to wireless structures to carry out a range of attacks that were not possible in the wired world.

It is worth noting that, according to the data bank of information security threats [1], some threats to the security of wireless connections can be carried out by an internal or external intruder with a low potential.

Recent regulations related to information security assessment include vulnerability analysis requirements and information system penetration testing.

Thus, the task of protecting a wireless network is a relevant and integral part of building such a connection.

1.1.Research problem

The problem lies in searching for potential threats to the Wi-Fi network based on the standard (IEEE 802.11) and assessing and detecting these threats to users, government institutions and companies to avoid security threats and keep their information and data away from intruders.

1.2. Research importance

The importance of the research lies in taking advantage of the threat methods of the Wi-Fi network and how to rationalize the user for the correct use of these networks, as well as how to use the most secure and reliable networks to ensure the safety of their data and information in digital transactions.

1.3. Research goals

- Eliminate potential threats to the Wi-Fi network.
- Support and development of the Wi-Fi network and increase the awareness of customers in the correct use of the network in order to enhance confidence in the exchange of information.
- Finding appropriate solutions to potential threats and problems.

1.4. Research hypothesis

The research hypothesis aims to support and develop the Wi-Fi network by conducting an assessment of potential threats and revealing them to the client to avoid penetration and threat and how to rationalize the user with the correct and safe use of the Wi-Fi network.

1.5. Research limits

The current research is determined for Iraqi Ministry of Education. within the year 2022.

2. Program research and related work

2.1. Program research

The research depends on the method of descriptive analysis to reach its goals and purpose to solve problems and address threats related to the Wi-Fi network. The research method is based on a combination of desk study and applied study.
The following aspects were worked out:

1. Theoretical aspect: In this aspect, work has been done to study some literature related to the topic of the Wi-Fi network and the potential threats, through the use of library books and specialized research in this field.

2. The practical aspect: a test was done using protocols and access points that threaten the security of Wi-Fi networks, and to determine the level of weakness and strength in the threatened networks and the method of protecting the network or addressing possible external attacks.

2.2.Related work

Study **(May Aye Chan Aung, Khin Phyo Thant,2019)** , which showed that (IEEE802.11) networks are one of the most widely used networks in the world and it is possible for hackers to take advantage of any loopholes in these networks and use them to harm the user or institutions and companies such as spying, theft, and damage to property and documents and data of users and customers [2].

Study **(Rashid Nazir , Asif Ali laghari , Kamlesh Kumar , Shibin David, Munwar,2020)**, which showed that (IEEE802.11) networks are exposed to continuous threats that are used to penetrate customer data or companies and government institutions and cause the theft of important information and data that makes the customer untrustworthy. The network The study discussed ways to develop Wi-Fi networks and eliminate obstacles and how to create safety systems for these networks [3].

3. Research Procedures

3.1. Classification of methods for implementing threats to the security of wireless Wi-Fi networks

An information security threat is understood as a set of conditions and factors that create a potential or real danger associated with information leakage and unauthorized or unintentional influences on it [4].

A threat with a certain probability can be implemented in a particular wireless network. Depending on the level of training of a potential intruder and the equipment he has, any attack on the network can be carried out. It is worth noting that, unlike wired networks, the intruder does not need to be in close proximity to his target, it is enough for him to be in the network signal reception area.

The classification of methods for implementing threats is shown in **Figure.1**.

3.2. Description and analysis of methods for implementing threats to the security of wireless Wi-Fi networks

Let us consider in more detail the methods for implementing security threats to wireless Wi-Fi networks. The following values are used as an assessment of the danger of each of the methods: high - an attacker can gain almost unlimited access to the system - the rights of an authorized user (administrator), both to manage and access information in it, medium - leakage of part of valuable information, low - leakage of non-critical information [5].

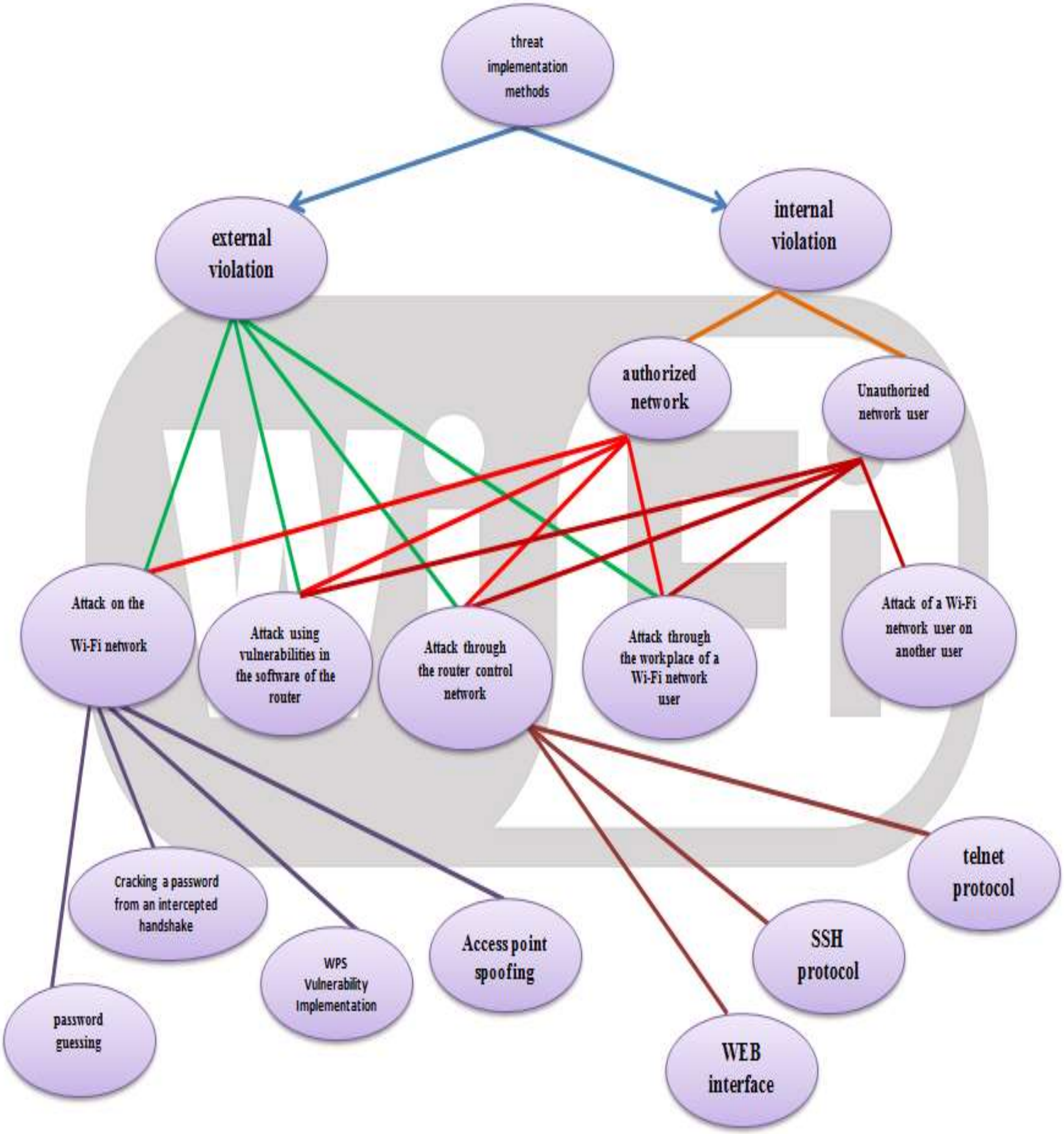

threat implementation methods
external violation
internal violation
authorized network
Unauthorized network user
Attack on the Wi-Fi network
Attack using vulnerabilities in the software of the router
Attack through the router control network
Attack through the workplace of a Wi-Fi network user
Attack of a Wi-Fi network user on another user
Cracking a password from an intercepted handshake
WPS Vulnerability Implementation
Access point spoofing
password guessing
telnet protocol
SSH protocol
WEB interface

Figure.1 Classification of methods for implementing threats in terms of typical situations .

ResearchJet Journal of Analysis and Inventions
https://reserchjet.academiascience.org

1. Attack on the Wi-Fi network

Includes password guessing, password cracking from an intercepted handshake (handshake), WPS vulnerability implementation and access point spoofing.
Hazard rating: medium.
Countermeasures: to exclude the possibility of guessing a password, or at least to complicate the brute force process itself, it is recommended to use a password of at least 10 characters in length, it should not contain meaningful words and phrases, as well as words and sets of numbers related to personal life user, disabling WPS technology, increased access control, hiding SSID, filtering by MAC addresses, using a minimum of open access points [6].

2. Attack through the router control network

This attack can be carried out in the three most famous ways: via HTTP (Web interface) , via Telnet and via SSH.
Each router has some kind of Web interface that allows you to configure a wireless network access point in many ways. The main problem is that many users neglect the correct configuration and leave everything by default. The settings window may not even be password protected and, therefore, anyone can get into it, you just need to know the IP address of the router. As a rule, all the necessary information for logging in is on the bottom panel of the router. Moreover, there are such cases that the login and password data are specified when you first enter the router configuration page. Once in these settings, an attacker gets an extremely wide range of options for working with Wi-Fi: from viewing service information to the ability to change network credentials or deny access to authorized clients. But even without knowing the model of the router, being not near it, an attacker can find standard combinations, which are not so many, and get into the control panel of the router using the selection method.
Telnet is a network protocol that implements a text-based interface through the command console with the ability to use additional commands to fine-tune the router.
SSH is an analogue of Telnet, but it has traffic encryption during authorization and networking.
The last two network protocols are usually not enabled on the router by default, and therefore some additional steps may be required to use them.
Hazard rating: high;
Countermeasures: using an administrator login and password other than the default ones, prohibiting or restricting network access to the router [7].

3. Attack using vulnerabilities in the software (software) of the router

As an example, consider the firmware vulnerability of the D-Link DSR-500 router [8], which allows an attacker to gain administrator rights. It lies in the fact that the (scgi-bin/platform.cgi) script of the router firmware does not properly filter the data entered by the user in the “Password” field, as a result of which an attacker can bypass the authentication procedure and gain access to the device with administrator privileges . Often, such equipment continues to operate without installing updates, despite the fact that the specified vulnerability has already been fixed by the manufacturer.

Hazard rating: depending on the type of vulnerability, the hazard can be low, medium or high.

Countermeasures: Installing up-to-date software updates will help you avoid attacks that target discovered vulnerabilities.

4. Attack through the workplace of a Wi-Fi network user

The software that users use cannot always guarantee safe operation and data transfer. Some applications offer to save or save user passwords by default in order to simplify the authorization task. Even users themselves can unknowingly put themselves at risk by using the same passwords on different systems. You also cannot be sure that no one or nothing is monitoring the actions or data that the user enters. For example, there is such a type of software as **key loggers** - software that registers various user actions, including keys pressed and applications opened by them. Such programs are freely available and can work in a mode invisible to the user.

Hazard rating: medium.

Countermeasures: constantly updating anti-virus programs, installing applications from trusted sources, using non-standard, complex and different passwords will allow the user to ensure the required security when working on any device [9].

5. Attack of a Wi-Fi network user on another user

An example of this attack is the process of intercepting information over wireless channels. Interception of information can be carried out by various means of monitoring network traffic. Of particular value to an attacker are the logins and passwords of users of various network services. So, for example, when trying to authenticate in any service, the user enters and sends his data. This information is inside network packets and, since it is not protected, can be intercepted.

Hazard rating: medium.

Countermeasures: Use strong data encryption, such as VPN technology.

3.3. Practical assessment of the possibilities of using programs and methods of penetration

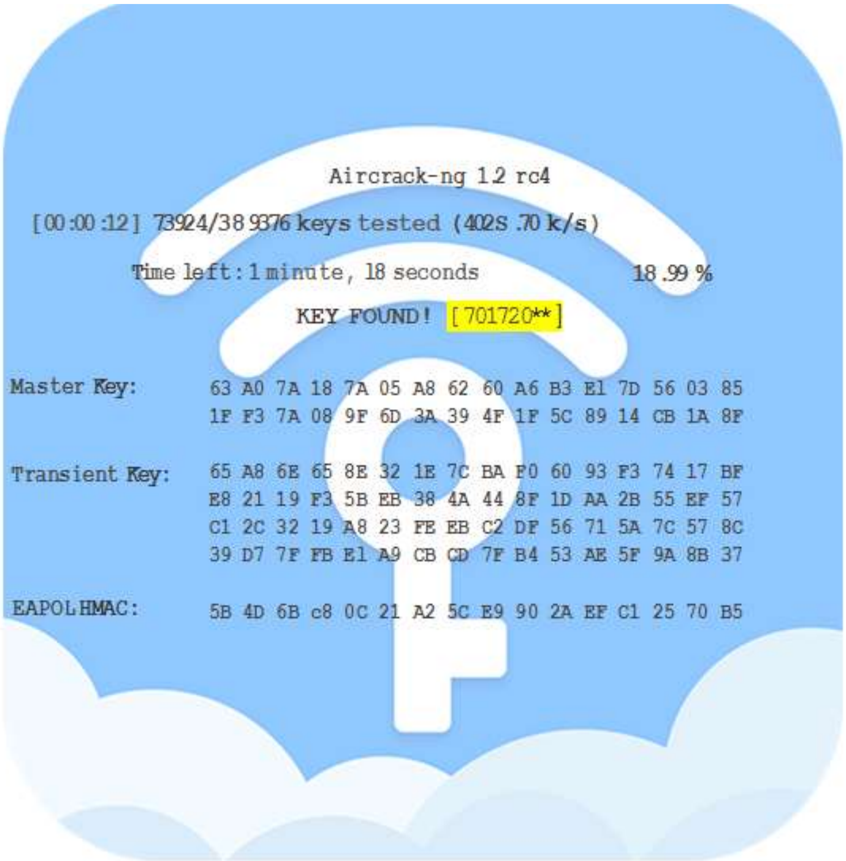
To assess the possibilities of unauthorized access to the Iraqi ministry of education Wi-Fi network, the Kali Linux operating system and its built-in tools were used. The wireless networks of department of Educational Planning , Division of Information and Communications were chosen as the object of testing: CS-Wireless and CS-Guest-WPA. The features of these networks are presented in **Table.1**.

The Aircrack-ng software package was used as a credential cracking tool. During the network monitoring process, the target access point CS-Guest-WPA with the largest amount of transmitted data was selected. As soon as it was possible to intercept the handshake, the process of its decryption was launched using a dictionary containing about 400,000 different combinations [10]. After 18 seconds, the program successfully completed password guessing **Figure.2**.

Table.1 Comparative characteristics of Wi-Fi connections.

Criteria	CS-Wireless	CS-Guest-WPA
Protocol encryption	WPA2	WPA2
Password uniqueness	Individual for each network client	General
Access	Registered employee	The possibility of authorization for everyone, who knows the network password

ResearchJet Journal of Analysis and Inventions
https://reserchjet.academiascience.org



```
                    Aircrack-ng 1.2 rc4

 [00:00:12] 73924/38 9376 keys tested (402S.70 k/s)

      Time left: 1 minute, 18 seconds              18.99 %

                KEY FOUND! [ 701720** ]

Master Key:        63 A0 7A 18 7A 05 A8 62 60 A6 B3 E1 7D 56 03 85
                   1F F3 7A 08 9F 6D 3A 39 4F 1F 5C 89 14 CB 1A 8F

Transient Key:     65 A8 6E 65 8E 32 1E 7C BA F0 60 93 F3 74 17 BF
                   E8 21 19 F3 5B EB 38 4A 44 8F 1D AA 2B 55 EF 57
                   C1 2C 32 19 A8 23 FE EB C2 DF 56 71 5A 7C 57 8C
                   39 D7 7F FB E1 A9 CB CD 7F B4 53 AE 5F 9A 8B 37

EAPOL HMAC:        5B 4D 6B c8 0C 21 A2 5C E9 90 2A EF C1 25 70 B5
```

Figure.2 Successful completion of handshake decoding.

A study of this method was also carried out for the CS-Wireless network. In the course of the work, it turned out that the interception of the handshake is quite feasible, but due to the peculiarities of the implementation of the connection to this network, it was not possible to open the login and password of the user of this network.

Implementation of the WPS vulnerability turned out to be impossible, since not a single access point in the coverage area of CS-Wireless or CS-Guest-WPA networks uses this technology.

To intercept information transmitted over a wireless connection, the Wire shark program was used. Since this program allows you to get information only when connected to the target network, it was tested on CS-Guest-WPA, the password for which was obtained as a result of a password attack from a handshake.

As a result of working with the Wire shark program, it was possible to obtain information about the sites visited by users, but due to the use of the secure HTTPS protocol on the sites found, all data was encrypted.

The results of the study are displayed in **Table. 2.**

Table.2 Wi-Fi Penetration Test Results.

Penetration testing method	WiFi connection	
	CS-Wireless	**CS-Guest-WPA**
Password cracking	–	+
Implementation of an attack on vulnerability(WPS)	–	–
Interception of information	–	+

4. Conclusions and Recommendations

4.1. Conclusions

As a result of the research, it was found that the CS-Wireless network is a network with a high level of protection against unauthorized access, while CS-Guest-WPA has vulnerabilities. Thus, the results of the analysis show the high vulnerability of the technologies that implement the Wi-Fi connection and require the adoption of additional protection measures related to the analysis and elimination of constantly detected vulnerabilities. To the extent possible, it is recommended to refuse to use such technologies in information systems that require a high class or level of security.

4.2. Recommendations

Recommendations for improving the efficiency of information protection
According to the results of a practical assessment of testing for penetration into wireless Wi-Fi networks, the following general recommendations can be made to improve the effectiveness of information protection:

- using complex passwords with a length of at least 10 characters and containing no meaningful words or phrases;
- periodic penetration testing to find new vulnerabilities and eliminate them;
- using MAC address filtering and hidden SSID mode to prevent rogue access point attacks;
- segmentation of the wireless network.

References

1.W. Kassab and K. A. Darabkh,"A–Z survey of Internet of Things: Architectures, protocols, applications, recent advances, future directions and recommendations," *Journal of Network and Computer Applications* ,163 , 102663, 2020.

2. May. A. Aung and Khin. Phyo. Thant," IEEE 802.11 Attacks and Defenses," *University of Computer Studies, Mandalay,* 186–191, 2019.
3. R. Nazir , Asif. Ali .laghari , K. Kumar, S. David, &Munwar, "Survey on Wireless Network Security, " © *CIMNE, Barcelona, Spain, springer 2021.*
4. G. Wang and Y. Qin , "Mac protocols for wireless mesh networks with multi-beam antennas: A survey, in: K. Arai,R. Bhatia (Eds.), " *Advances in Information and Communication, Springer International Publishing, Cham,* pp. 117–142,2020.

5. A. Seferagic, J. Famaey, E. De Poorter & J. Hoebeke, " Survey on wireless technology trade-offs for the industrial Internet of Things, " *Sensors 20 (2) 488,2020*.
6. W. Sun , M. Choi & S. Choi, " IEEE 802.11ah: A long range 802.11 WLAN at Sub-1GHz," *Journal of ICT Stan-dardization 2 (2)* , 83–108,2013.
7. M. Park, " IEEE 802.11ah: Sub-1GHz license-exempt operation for the Internet of Things, "*IEEE Communications Magazine 53 (9)* , 145–151,2015.
8. M . S. Meera and S. N. Rao, "A survey of the state of the art of 802.11ah, " *in: 2017 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC)*, pp. 1–4, 2017.
9. S. Khan and M. Zeeshan, "Performance and throughput analysis of IEEE 802.11ah for multiband multimode operation, " *in: 2018 21st International Symposium on Wireless Personal Multimedia Communications (WPMC),IEEE,* pp. 150–155,2018 .
10. S. Khan, M. Zeeshan & Y. Ayaz, "Implementation and analysis of multicode multicarrier code division multiple access (mc–mc cdma) in IEEE 802.11ah for uav swarm communication, " *Physical Communication 42* , 101159,2020.