SECURITY ANALYSIS OF PUBLIC WI-FI NETWORKS ON THE STREETS OF FERGHANA

Juraev Jakhongir Nurmaxamadovich,

Assistant of the Department of Software Engineering of the Fergana branch of Tashkent University of Information Technologies named after Muhammad al-Khwarizmi

Abstract: *Based on the increasing popularity of the use of Wi-Fi networks, the article discusses the problems of vulnerability of Wi-Fi networks, problems related to the security of the use of wireless networks and access to them. It also provides statistics on the use of Wi-Fi networks in the central district of Fergana, the degree of their security and accessibility.*

Keywords: *Wireless networks; Wi-Fi; Internet; encryption protocol; authentication method; security; vulnerability; information security; interception of information.*

Currently, the Internet occupies a leading position in obtaining information. With its help, humanity can receive education, exchange thoughts and opinions with other users of the network, and send various information. There are two ways to transmit data: wired and wireless. The advantage of the wired method is the high speed of operation and increased physical security of the data transmission channel.

The wireless method is more mobile. But at the same time, stable data transmission and simultaneous operation of multiple wireless points in one place causes collisions, namely, the overlapping of several transmitters on top of each other, as a result of which the total signal becomes distorted. This problem prevents the correct transmission of data over the network [1].

Wi-Fi networks have become very widespread over the past few years. More and more of the world's leading organizations are actively using the developing Wi-Fi technology and providing Wi-Fi services to their customers. A lot of different devices have recently been manufactured with built-in Wi-Fi support, whether it's mobile phones, tablets, laptops or any other device from a variety of different gadgets. To connect to a wireless network, you only need to be within its radius of action. Actions to identify Wi-Fi networks and configure the necessary parameters occur automatically. A device located within the range of several Wi-Fi networks can connect to one or another access point either at the user's choice, or automatically to the network that has the most powerful signal strength. There is also a periodic check of the availability of an access point with the best signal strength.

A wireless Wi-Fi network has the following advantages, the main of which are:

* Organization, use and expansion of the network without the use of a cable;
* The ability to dynamically change the network topology;
* The ability to use one access point by several users;
* Easy to design and implement.

At the same time, the wireless network has some disadvantages, one of which is the dependence of the connection speed on the presence of various obstacles and the number of connected devices, as well as the vulnerability of the network in terms of security due to facilitated physical access to the signal.

Every day the number of users who use devices with wireless Internet access is continuously growing. Similarly, the number of attackers is growing, trying in every possible way to gain access to other users' data and use them for personal purposes. So, connecting to a Wi-Fi network with

ISSN2277-3630 (online),PublishedbyInternational journal of Social Sciences & Interdisciplinary Research.,January-2022 https://www.gejournal.net/index.php/IJSSIR

weak security settings is risky: the transmitted data may be accessible to unauthorized persons, as a result of which all confidential information may become open to intruders. To intercept all the necessary data, it is enough to be in the range of the Wi-Fi network in which the electronic device is located directly. The attackers' goal may be to violate each of the components of the data: confidentiality, availability, integrity, and interception of information for further use for personal purposes.

In order to identify vulnerabilities, it is necessary to understand the parameters of wireless networks. New ways of combating unauthorized data acquisition are constantly growing; new means of protection are emerging. Thus, it is necessary to analyze the basic principles of operation and organization of wireless networks in order to understand their vulnerabilities, to investigate the scale of the problem in order to further determine the volume of unprotected or using insecure Wi-Fi encryption protocols of access points.

A secure system by definition must have three properties: confidentiality, availability and integrity. The privacy property guarantees the user that his secret data will be available only to him or to a group of persons who are allowed access to them. The availability property indicates that authorized users have the right to access data at any time. The integrity property implies the immutability of the parameters and characteristics specified during the configuration of the device. This property is necessary because the privacy protection of the Wi-Fi network depends on it. Due to this property, an attacker cannot change the device settings, which could lead to a change in the order of work and even to the device's failure. In order to provide devices connected to a wireless network with security, it is necessary first of all to understand what parameters ensure confidentiality, integrity and availability of data.

First of all, an important parameter of any wireless network is the type of encryption. One of the important aspects of data transmission over the network is traffic encryption, since to intercept information transmitted over a wireless network, you do not need physical influence, but simply "listen" to the channel and intercept the information of interest.

Now several types of encryptions are most common:

* NONE – an open type of encryption, data is transmitted without any key, anyone can access this wireless network ("insecure network"). In most cases it is used for guest access;

* WEP is an RC4-based cipher with different static or dynamic key lengths (64 or 128 bits). Its algorithms are laid out in the public domain, which allows attackers to collect statistics until an encryption key is obtained. A network based on this encryption method is not secure. WEP is an insecure and functionally obsolete standard;

* TKIP - This encryption method is an advanced WEP method. Additional security checks and protection have been added to it. Encryption keys are 128 bits long and are generated by a complex algorithm, and the total number of possible key variants reaches hundreds of billions, and they change very often. But TKIP is outdated, it has a lower level of security than the AES standard, which replaces it;

* CCMP is the most advanced algorithm with additional checks and protection. This is a new method of protection for wireless data transmission. Provides a more reliable encryption method compared to TKIP. CCMP is chosen as an encryption method when enhanced data security is needed.

Also, to identify networks with insecure access, it is necessary to consider the interaction of

ISSN2277-3630 (online),PublishedbyInternational journal of Social Sciences & Interdisciplinary Research.,January-2022 https://www.gejournal.net/index.php/IJSSIR

the access point and the wireless client, otherwise called authentication methods•

* OPEN - an open network. All connected devices are authorized automatically;

* WPA - Personal - This mode is suitable for most home networks. When a password is set for a wireless access point, it must be entered by user's every time they connect to a Wi-Fi network;

* WPA - Enterprise - This mode provides the necessary protection of the wireless network in the work environment. This mode is more difficult to configure and offers individual and centralized access control to your Wi-Fi network. When users try to connect to the network, they will need to provide their authentication credentials.

WPA2 is the second version of a set of algorithms and protocols that provide data protection in wireless Wi-Fi networks. It is assumed that WPA2 should significantly increase the security of Wi-Fi wireless networks compared to previous technologies. The new standard provides, in particular, the mandatory use of a more powerful AES encryption algorithm and 802.1X authentication.

WPA2 protocols work in two authentication modes: personal and Enterprise:

* WPA2 - Personal is currently the most reliable form of protection, offered by Wi-Fi devices, and it is recommended to use it for all purposes. In WPA2-Personal mode, a 256-bit PSK (preshared Key) key is generated from the plaintext passphrase entered. The PSK key together with the SSID (Service Set Identifier) are used to generate temporary session keys PTK (Pairwise Transient Key), for the interaction of wireless devices. Like the static WEP protocol, the WPA2-Personal protocol has certain problems associated with the need to distribute and support keys on wireless network devices, which makes it more suitable for use in small networks of a dozen devices, while WPA2-Enterprise is optimal for corporate networks;

* WPA2 - Enterprise - WPA2-Enterprise mode solves problems related to the distribution and management of static keys, and its integration with most corporate authentication services provides account-based access control. To work in this mode, registration data such as the user's name and password, a security certificate or a one-time password are required, and authentication is carried out between the workstation and the central authentication server [2].

Using the example of the center of Fergana, as the area most saturated with Wi-Fi networks, it is of interest to analyze the vulnerabilities of wireless networks and assess the current distribution of networks by type of encryption and authentication methods.

To analyze the vulnerabilities of wireless networks in the central part of Fergana, information was collected. In the formulated approach, it consists in the following. With the help of the necessary equipment, namely, a GPS device (GlobalSat BU – 353s4), which allows you to accurately estimate the location of a wireless access point, the coordinates of Wi-Fi networks in the center of Fergana were obtained, according to a pre-set route.

It included central streets, alleys, embankments, driveways and squares with a wide variety of public places, which made it possible to further analyze the public Wi-Fi networks of the city of Fergana. The IV generation GPS receiver is a device with a USB interface on the SiRF STAR IV chipset, providing high quality and speed of coordinate determination. In one case there is a receiver and an active antenna. The magnetic base is used to mount the GPS receiver in any convenient place that provides high-quality reception of the satellite navigation system signal.

ISSN2277-3630 (online),PublishedbyInternational journal of Social Sciences & Interdisciplinary Research.,January-2022 https://www.gejournal.net/index.php/IJSSIR

Figure 1 - Equipment for finding vulnerable Wi-Fi points

After carrying out the analytical part of the work, 2,357 networks related to 29 streets, alleys, embankments, squares and driveways in the central part of Moscow, in the Kremlin Ring area, were analyzed. For a more visual location of the points, the Google Earth program was used, on the map of which all caught Wi-Fi networks are indicated.

Conclusions. The problem of wireless network security is becoming one of the main problems of IT technologies today. One of the key factors in the development and design of any system is security. Various algorithms of mathematical models of authentication, data encryption and integrity control of their transmission are used to protect Wi-Fi networks, but, nevertheless, the problem of network vulnerability remains very significant. If proper attention is not paid to the network setup, then an attacker will be able to access the resources of Wi-Fi network users.

References

1. Таненбаум Э. Архитектура компьютеров. / Э. Таненбаум - СПб.: Питер, 2007. - 848 с.
2. Олифер, В. Г. Компьютерные сети. Принципы, технологии, протоколы / В. Г. Олифер, Н. А. Олифер. – СПб.: Питер, 2006. – 958с.

ISSN2277-3630 (online),PublishedbyInternational journal of Social Sciences & Interdisciplinary Research.,January-2022 https://www.gejournal.net/index.php/IJSSIR