UDC 004.7.056.5

S.I. Lopatin,
Candidate of Juridicial Sciences,
Senior Researcher

CLASSIFICATION OF THE THREATS TO INFORMATIONAL SECURITY AND TECHNOLOGIES OF SECURITY, REALIZED IN OVER-THE-AIR NETWORKS OF THE STANDARDIEEE 802.11 (WI-FI)

Paper classifies the information security threats of wireless networks of IEEE 802.11 standard.

Keywords: *information security threats of wireless networks, standard IEEE 802.11, Wi-Fi.*

У статті класифіковано загрози інформаційній безпеки безпроводових мереж стандарту IEEE 802.11.

Ключові слова: *загрози інформаційній безпеці, безпроводові мережі, стандарт IEEE 802.11, Wi-Fi.*

В статье класифицированы угрозы информационной безопасности беспроводных сетей стандарта IEEE 802.11.

Ключевые слова: *угрозы информационной безопасности, беспроводные сети, стандарт IEEE 802.11, Wi-Fi.*

The threat of information security means the totality of conditions and factors that create the potential dangers associated with information leakage and / or unauthorized and / or unintentional actions [5]. Risk can be defined as a condition where the facility due to the appearance of security threats.

The difference between them is that the threat is the quality of property security and the threat – property of the object of an interaction and is in object security, which acts as a source of security threats [2]. One of the most fundamental features of information security problems are absolute requirements set of the completeness of information security threats.

Each undiagnosed or missed destabilizing factor can greatly reduce or even negate the effectiveness of the protection.

However, the problem of forming a complete set of threats related to the informal distinct problems.

Features of technology of the deployment of wireless networks related to data transmission over the air, is a source of information security threats, inappropriate with wired technologies.

Therefore, the deployment of wireless networks protecting traditional methods used in wired networks, should be supplemented by the measures to neutralize specific wireless threats.

In the documents of international organizations of the standardization several ways of classifying of security threats of communications systems separated by types, kinds and categories are allocated . Threats to security are the subject of an analysis in the design phase of the security of an architecture specific wireless network, set a great number with many elements, which causes difficulty in selecting measures to protect against threats. To facilitate this task, it is appropriate to classify according to the document ETSI (European Telecommunications Standards Institute) ETR (ETSI Technical Report) № 332 to group security threats according to the categories [1].

According to these recommendations threats can be classified as follows [6].

1. Threats to privacy violation

• violation of privacy by intercepting wireless traffic;

• unauthorized access to information and services of wired network segments , which operates a customer using a wireless access;

• disclosure of the parametres of wireless network or wired network segments, users access using wireless access outside the controlled zone;

• disclosure of information about setting up wireless network security systems.

2. Threats of breach of integrity:

• distortion of an information circulating on the network;

• destruction of user information or an information stored in segments wired network, which operates a customer using a wireless access;

• sending packets to the wrong address, packet loss, wrong assembling packets of substitution;

• interference in the access points;

• destruction of its own software access points.

3. Threats violation availability:

• intervention in the exchange of messages in the network;

• lock of adopted or sent messages on the user level or access points;

• introduction of unauthorized wireless traffic;

• disabling access point along with all attached users;

• slowdown, inadequate response to operator commands.

4. Specific threats:

• unauthorized, anonymous Internet traffic usage;

• illegal actions on behalf of anonymous user wireless network;

• theft of client devices or access points to obtain information about setting up wireless network security systems;

• installation of unauthorized access points and client network cards;

• unauthorized configuration change remedies wireless networks;

• unauthorized connection to a wireless network;

• human error;

• refusal wireless equipment.

Now we consider a wireless network standard IEEE 802.11 as an object of threats to information security and conduct classification on the configuration of used remedies.

For wireless networks 802.11 all means and methods of protection can be divided into three types [2,3,4]:

1. Means and methods of authentication;

2. Means of cryptographic protection of data transferred;

3. Additional remedies.

By means and methods of authentication are:

Basic authentication (open authentication, authentication with shared key authentication MAC address);

Authentication using the same PSK-keys;

IEEE 802.1x authentication protocol and EAP (Extensible Authentication Protocol) using RADIUS-server.

By means and methods of encryption are:

Encryption using static WEP (Wired Equivalent Privacy) keys;

Encryption technology with WPA, WPA2 (Wi-Fi Protected Access).

Additional remedies not provided by equipment manufacturers, include:

virtual private network (VPN);

the use of intrusion detection systems (IDS).

Open network.

At this time there are many completely open wireless networks that do not use cryptographic protection, MAC addresses, non-closed ESSID, there are no filtration protocols, it is possible to control access points directly from the network. The reason for the existence of networks of this type is caused by irresponsible users and system administrators are not configured by properly embedded parameters remedies. Because of the high vulnerability of this type of network attacks from offenders are most often exposed to.

Networks that use basic authentication.

Wireless networks of this type is more secure because they are sometimes called private. Applied remedies are not insurmountable for the offender. Disconnection of broadband transfer ESSID does not preclude its disclosure of the offender because actually no ID is removed from all administrative frames. For example, in frames requests for re-authentication and re-joining the wireless network identifier is present, which is essential vulnerability of networks of that class.

MAC address filtering is also vulnerable to a skilled intruder, which is sufficient to analyze network traffic and find out which MAC addresses are found. After disabling the user from the network intruder can assign your network adapter and its MAC address to join.

Networks that use an intrusion detection system as additional means of protection to be less vulnerable because in some cases, the system allows the network administrator to inform about the fact of attack.

Application protocol filtering in some specific cases where the wireless network users are limited in their actions, can be quite effective. But the market represented enough access points where properly implemented filtering protocols, and usually it's expensive high-end devices, which also leads to increased vulnerability of networks.

Wireless network with WEP-encryption.

Wireless networks of this class in addition to the basic means of authentication protocol using WEP encryption as means of cryptographic protection. WEP protocol allows the exchange of information between users is encrypted, which makes it harder to breach unauthorized user privacy.

However, the WEP protocol revealed a number of vulnerabilities that allow the offender to receive the encryption key.

Wireless networks that use protocol TKIP (Temporal Key Integrity Protocol) (WPA, WPA2) and authentication using common PSK (Pre-Shared Key) – keys.

TKIP protocol of the 802.11 protocol eliminates existing WEP vulnerabilities and is now considered an effective means of cryptographic protection. In networks that class along with TKIP protocol used means of authentication with pre-shared key PSK. Although each client may be a host PSK, but most implementations use one PSK per ESSID as well as the protocol WEP.

Unlike WEP, PSK is not used to encrypt data and to generate a pair of temporary keys (Transient Key RTC) for each TKIP protocol secure connection. Wireless networks do not use this class 802.1x protocol for key distribution and rotation TKIP. They are not obsolete network with an updated wireless equipment and software and hardware are not able to support the 802.1x standard, thus they can be vulnerable to attacks by exhaustive search or dictionary.

Wireless networks that use protocol TKIP (WPA) and authentication protocols IEEE 802.1x and EAP.

In networks of this class TKIP keys are generated, distributed via protocol 802.1x, or RADIUS. In that case, try to break the TKIP keys are ineffective, but it is possible unilateral attack 802.1x authentication system, which uses a protocol EAP MD5. However, such an attack limited use, since modern implementation of 802.1x support mutual (client server client and server) authentication protocol and the EAP MD5 resort only in extreme cases. If the implementation of the standard 802.1x protocols involved EAP-TLS, EAP-TTLS or EAP-Rear, then hacking the network is unlikely and the offender can only be DoS-attacks, social engineering methods, or attacks from the wired network to a server certificates.

Wireless networks that use AES encryption algorithm and authentication using common PSK-keys.

AES – improved encryption algorithm that is used as an alternative algorithms RC4 and TKIP protocol WEP. AES offers higher level of the encryption than TKIP and WEP. AES –- extremely secure cryptographic algorithm, wireless network, using this algorithm is the least vulnerable to hacking the encryption key. Along with encryption in networks of this class is a system of authentication with pre-shared key (pre-shared Key PSK).

Wireless networks that use a virtual private network VPN as a defense mechanism.

In this class wireless networks are performed when sending data encryption and decryption on the receiving device. Thanks to protocol configured tunnel, which can not penetrate that the data is not encrypted properly. For more safety encryption can provide not only the data but also the network addresses of the sender and recipient. Often used to build VPN protocol Point-to-Point Tunneling Protocol (RRTR) or implementing various protocol IPSec.VPN meets two conditions: confidentiality and integrity. However, VPN is not resistant to DDoS-attacks and can not guarantee availability at the physical level just because of its virtual nature, and depending on the protocols that are listed below.

Summing up, we must draw attention to the fact that at this time on the Internet there are more programs and algorithms, hardware specifications that enable the system to decipher all the encryption used in building wireless networks.

Thus, we can rightly conclude that to date there is no fully secure wireless networks, it contributes to the attention of specialists in the development of new technologies of information security.

LIST OF USED SOURCES

1. ETSI ETR 332: Security techniques advisory group (STAG) // Security requirements capture 1996.

2. *Герасименко В.А.* Основы защиты информации / В.А. Герасименко, А.А. Малюк. – М. : Триумф, 1997. – 368 с.

3. *Лукацкий А.В.* Мир атак многообразен / А.В. Лукацкий // Сетевой. – 2001. – № 11. – С. 45–49.

4. *Педжман Р.* Основы построения беспроводных локальных сетей стандарта 802.11 / Р. Педжман, Д. Лиери. – М. : Вильяме, 2004. – 294 с.

5. *Приходько А.Я.* Словарь-справочник по информационной безопасности / А.Я. Приходько. – М. : Синтег, 2001. – 124 с.

6. *Совлук Я.* Безопасность внутриофисных сетей Wi-Fi / Я. Совлук // Информационная безопасность: научный журнал. – 2002. – вып. 2. – С. 7–10.

Received 07.04.2015