УДК 621.37/39

Gabidyen Ainur – master, student (Almaty, Kazakh Academy of Transport and Communications named after M. Tynyshpaev)

METHOD OF INFORMATION PROTECTION IN THE WIRELESS NETWORK

The rapid increase in the growth in the number of laptops and electronic organizers, which has been happening lately, leads to an expansion of the scope of their possible use. At the same time, the network is an integral part of normal operation. As a result, wireless networks, in any form, are gaining popularity. But along with convenience, there are also problems, one of which is improving the level of security. When the transmission of information is carried out by radio waves, then anyone can take them, there would be a receiver. Accordingly, an additional security mechanism is required.

Open System Authentication is the default authentication protocol for the 802.11 standard. It consists of a simple authentication request containing the station ID and an authentication response containing success or failure data. Upon successful authentication, both stations are considered mutually authenticated. It can be used with WEP (Wired Equivalent Privacy) protocol to provide better communication security, however it is important to note that the authentication management frames are still sent in clear text during authentication process. WEP is used only for encrypting data once the client is authenticated and associated. Any client can send its station ID in an attempt to associate with the AP. In effect, no authentication is actually done

And in the 802.11 standard it was implemented as a WEP protocol. Its main task is to protect information from listening. WEP is part of the international standard; It is used in all devices using the 802.11 protocol.

Unfortunately, WEP did not cope with the task. Despite the use of a proven RC4 encryption method, WEP contains several important drawbacks. These shortcomings make it possible to conduct a number of attacks, both active and passive, the ability to listen and falsify network traffic.

For wireless networks, the issue of security is much more important than for conventional wired networks, since all traffic exchange in the network is performed in a radio channel and for its interception, quite inexpensive standard equipment. Developers of Wi-Fi standards understood this and did their best to provide a level of security, at least not lower than in wired networks.

Encryption of information is the transformation of open information into encrypted information (which is often called a cipher text or cryptogram), and vice versa. The first part of this process is called encryption, the second part is decryption.

In symmetric encryption algorithms, decryption usually uses the same key as for encryption, or a key associated with it by some simple relationship. The latter is much less common, especially in modern encryption algorithms. Such a key (common for encryption and decryption) is usually called simply an encryption key.

You can imagine encryption in the form of the following formula:

$$\text{Where } C = Ek1 (M) \qquad (1)$$

M (message) - open information;
C (cipher text) - is the cipher text obtained as a result of encryption;
E (encryption) - is an encryption function that performs cryptographic transformation over M;
k1 (key) - parameter of the function E, called the encryption key.

In the standard GOST 28147-89 (the standard defines the domestic algorithm of symmetric encryption) the concept key is defined as follows: "The specific secret state of some parameters of the cryptographic transformation algorithm, which ensures the selection of one transformation from the set of all possible transformations for the given algorithm".

The key can belong to a specific user or group of users and be unique for them. Encrypted using a specific key information can be decrypted only using only the same key or key associated with it by a certain relationship.

Similarly, we can imagine and decryption:

$$\text{Where} \quad M' = Dk2\,(C) \tag{2}$$

M 'is the message received as a result of decryption,
D (decryption) - the decryption function; as well as the encryption function,
performs cryptographic transformations over the cipher text,
k2 is the decryption key.
To get the correct plaintext (that is, the one that was previously encrypted:
(M'= M) as a result of decryption, simultaneous fulfillment of the following conditions is necessary:

1. The decryption function must correspond to the encryption function.
2. The decryption key must match the encryption key

If there is no valid key k2, it is impossible to get the original message(M '= M) using the correct D function. The word "impossible" in this case usually means the impossibility of computing in real time with the existing computing resources.

The WEP algorithm is based on using four 40-bit private keys (user passwords) common for one network The pseudo-random sequence generator is initialized with a 64-bit number (keys) consisting of a 24-bit initialization vector (IV) and a 40-bit secret key. It is significant that if the secret key is known to network devices and is unchanged, then the vector IV can vary from packet to packet. To protect against unauthorized changes to the transmitted information, each encrypted packet is protected with a 32-bit CRC-32 checksum, its value being transmitted in the ICV (integrity check value) parameter. Thus, when encrypting, 8 bytes are added to the transmitted data 4 for ICV, 3 for IV, and more 1 byte contains information about the number of the secret key used (one of four) (Figure 1.2). Note that the key can be not only 64, but also 128 bits. In the latter case, the password is not reserved for 40, but for 104 bits.

This protocol should ensure the protection of data at the time of transmission over the network. It is based on encryption of transmitted packets with the help of a special key k. Consider the process of encryption Checksum: the first stage. The checksum c (M) of the message (M) is calculated. Then the checksum is added to the message P = (M, c (M)), which is the initial data for the second stage. Note that neither c (M) nor P is independent of the key k. Encryption: the second stage. Text P is encrypted using the RC4 algorithm. Let the starting vector be (IV). Algorithm RC4 generates keystream - i.e. a sequence of random bytes depending on IV v and key k. Denote this keystream as RC4 (v, k). Then the XOR message is superimposed on the keys team, and we get the encrypted message:

$$C = P \text{ xor } RC4(v,k) \tag{3}$$

Transmission: the last stage. There is a transfer of IV and encrypted messages over the network all this can be represented these:

$$A - B: v, (P \text{ XOR } RC4 (v, k)), \text{ where } P = (M, c (M)) \tag{4}$$

We introduce the following abbreviations for future use: message (M) - the initial data for encryption; text (P) - the amount of the message and its checksum; package (C) - encrypted text transmitted over the network. To decode the received data, the recipient conducts reverse actions. Firstly: the keystream RC4 (v, k) is generated and by means of the XOR operation it turns the packet into text.

$$P' = C \text{ xor } RC4(v,k) = (P \text{ xor } RC4(v,k)) \text{ xor } RC4(v,k) = P \quad (5)$$

Then the receiver checks the checksum of the decoded text P ', starting from (M', c '), recounts it c (M'), and checks if it matches the received C '. This implies that the user only receives packets with the correct checksum

The WPA (Wi-Fi Protected Access) standard is a subset of the specifications from the 2004 IEEE 802.11i standard. The whole set of specifications of the standard IEEE 802.11i. The Wi-Fi Alliance is called WPA2. The WPA specifications were designed to give users an alternative to WEP and became a transition between it and the new IEEE 802.11i standard, the development of which was heavily delayed. The structure of WPA can be represented in the form of the formula WPA = IEEE 802.1X + EAP + TKIP + MIC, I e WPA is the sum of several elements considered below.

Protocols IEEE 802.1X and EAP (Extensible Authentication Protocol) provide a mechanism for authenticating users who must produce a credential or certificate for accessing the network. In large corporate networks, RADIUS server is often used for authentication. In the network hierarchy, it is located above the access point and contains a database with a list of users who are allowed access to the network. Such a network security system is called Enterprise (corporate). For small businesses and home users, its use is not justified, they have a mode with a pre-shared key PSK (Preshared Key). In this mode, the same password is entered on each wireless network device, and authentication takes place by means of the access point without using the RADIUS server.

The TKIP (Temporal Key Integrity Protocol) protocol performs data confidentiality and integrity functions. Functionally, . Like WEP, it uses the RC-4 encryption algorithm, but a more efficient key management mechanism. The TKIP protocol generates a new private key for each transmitted data packet, and one static WEP key is replaced with approximately 500 billion possible keys that can be used to encryption this data packet. The mechanism of key generation has also been changed. It is obtained from three components: a 128-bit key base (TC), a packet transmission number (TSC), and a MAC address of the transmitter device (TA). Also, TKIP uses a 48-bit initialization vector to avoid reusing IV, on which the above-described FMS attack is based. The TKIP algorithm uses a through packet counter (TSC) of 48 bits in length. It is constantly increasing, dropping into 1 only when generating a new key. The lower 16 bits of the TSC are included in the new Thus, a mechanism is created that prevents so-called playback attacks The TKIP attack uses a mechanism similar to the WEP attack that trying to decode one byte at a time by using multiple replays and observing the response over the air. Using this mechanism, an attacker can decode small packets like ARP frames in about 15 minutes. If Quality of Service (QoS) is enabled in the network, attacker can further inject up to 15 arbitrary frames for every decrypted packet. Potential attacks include ARP poisoning, DNS manipulation and denial of services. Although this is not a key recovery attack and it does not lead to compromise of TKIP keys or decryption of all subsequent frames, it is still a serious attack and poses risks to all TKIP implementations on both WPA and WPA2 network.

802.11i supersedes the previous security specification, WEP, which was shown to have security vulnerabilities. WPA had previously been introduced by the Wi-Fi Alliance as an intermediate solution to WEP insecurities. WPA implemented a subset of a draft of 802.11i. The Wi-Fi Alliance refers to their approved, interoperable implementation of the full 802.11i as WPA2, also called RSN (Robust Security Network)..

The standards of WPA and 802.11i are sufficiently reliable and provide a high level of security for wireless networks. Nevertheless, one security protocol is not enough - you should also pay attention to the proper construction and configuration of the network.Physical protection. When deploying a Wi-Fi network, you need to physically restrict access to wireless points.

Correct setting. The paradox of modern wireless networks is that users do not always include and use built-in authentication and encryption mechanisms. In the detection phase, the STA finds an AP with which it can establish a connection and obtain from it the security parameters used in the network. Thus, the STA recognizes the network identifier (SSID) and authentication methods. The STA then selects an authentication method and establishes a connection between the STA and the AP. The standard provides for two-way authentication (unlike WEP, where only the workstation is authenticated, but not the access point). At the same time, the places of decision-making on access are STA and AS, and the places of execution of this decision are STA and AP. For the IEEE 802.11i standard, a key hierarchy is created that includes the Master Key, Pairwise Master Key (PMK), Pairwise Transient Key (PTK), and the group keys (GTK) used to protect the broadcast network traffic

Conclusion

Protection of user devices. Do not fully rely on built-in network protection mechanisms. The most optimal is the method of echeloned defense, the first line of which is the means of protection installed on a stationary PC, laptop or PDA.

Traditional measures. Effective computer operation on the network is unthinkable without classical protection measures - timely installation of updates, use of security mechanisms built into the OS and applications, as well as antiviruses. However, these measures are not enough for today, as they are focused on protection against already known threats.

Network monitoring. The weak link in the corporate network is the unauthorized access points. Actual is the problem of localizing unauthorized access points. Special means of localizing access points allow you to graphically display the location of the "foreign" terminal on the map of the floor or building. If classical methods do not save from invasion, attack detection systems should be used.

VPN-agents. Many access points operate in an open mode, so you need to use methods to protect the transmitted data. A VPN client must be installed on the protected computer, which will take care of this task. Almost all modern operating systems (for example, Windows XP) contain in their composition such software components.

REFERENCES

1. Proletarskiy A.V., Baskakov I.V., Fedotov R.A. Wireless networks
2. Wi-Fi (2nd edition).-2016
3. Merrit M. Protection of wireless networks.-2015 Shubin V.I. Besprovodnye
4. Chandra P., Dobkin D.M., Bensky A., Olexa R., Lide D.A., Dowla F., 2008.
5. Networking Know it all, 47-95 Roshan P., Leary J., 2003. 802.11 Wireless LAN Fundamentals