SECURITY ISSUES IN WIRELESS NETWORKS

IOSEB KARTVELISHVILI
Professor, European University, Georgia

TEA TODUA
Professor, European University, Georgia

KEYWORDS: WIRELESS NETWORKS SECURITY, DOS ATTACK, UNAUTHORISED ACCESS POINT, MAN IN THE MIDDLE ATTACK

In the last period of time, the security in wireless networks and the quality of this service, became very important and it is a subject of active researches. Communication signals which is extended in some environment can be received by someone else also. Companies and individual users must recognize potentially existing problems and try to prevent it.

Every system which needs to secure has some deficiencies in it. These deficiencies or part of them can be used by attacker. Subsequently, for providing security of the system it is important to consider all possible threats and attacks which can be performed against the system. Security mechanisms must provide system security by considering of given threats, attacks and deficiencies.

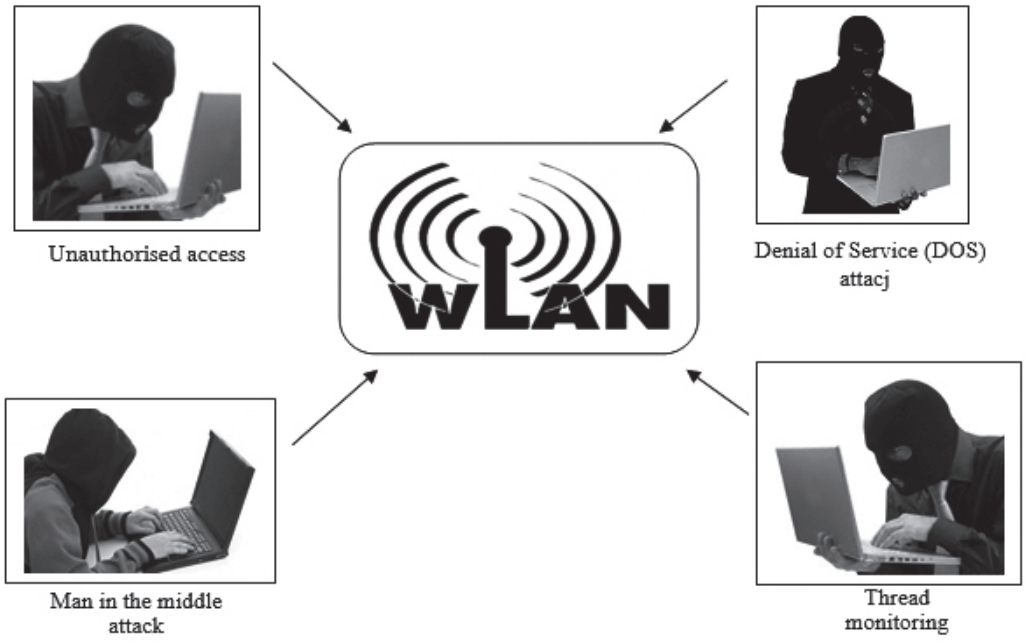
On the pic. 1 the most common forms of threats related to wireless networks are shown.

As a result of attack, hackers can perform unauthorized access inside the network system. They also can cause failures in a network systems working and catch the company's information. Attack is an attempt to ignore of computer security control mechanisms. After attack data can be changed, stolen and abolished. Examples of attack are data stealing from transferring environment and devices, gaining of unauthorized privileges, entering of false data, information modification, etc.

Experienced hacker or snooper easily can find unsecure packets of wireless network and open data inside it. For example, snoopers which are in the building, remote from wireless network several 100-th meters, can receive the information about all transactions performed in this network. The main threat is that as a result of an attack, someone can obtain such important information as user names and passwords, credit card numbers, etc.

To solve the problem it is necessary to encript the information which is transfering among wireless devices and base stations. During the encription process, bytes the data are exchanged by using of secret key. By using of effective mechanisms encryption can increase data security level.

Unfortunately, most of companies are using default configuration of base stations. This configuration can not ensure desired security. Windows operating system gives possibility to connect easily to the wireless network. When a notebook connects to the wireless local network, its owner can get access to any other notebook in this network. If the personal firewall is not used, everyone can get information from this notebook's hard disk.



Pic. 1. Different forms of threats which are related to using of wireless network

Very often when in the access points security mechanisms are activated, existence of unauthorized access point can be threat. Some personnel can obtain access point, not consider network security standards and set it in his/her office. Hacker can place access point in the building, intentionally connect access point to the corporative network.

In the unauthorized access point, as a rule, the encryption system is not activated. Proceeding from this, it is "open door" for everyone who has a desire to access to corporate network. Because of this, companies must always check existence of unauthorized access points.

In order to prevent unauthorized access in the wireless network, autentification is used. Autentification is performed among network devices and access points. In the wireless network must be used methods, by using which base station is informed about network device identity and viceversa. It is necessary in order to make connection among legitimate base stations and devices. Besides this, autentification procedure must be performed on the access points. By using this procedure existence of unauthorised access points in the network can be avoid.

By using of autentification and encription mechanisms, security of wireless network will be increased, though experienced hackers can always find the weak sides. Most dangerous is man-in-the-middle attack. The hacker places fake device among legitimate users and wireless network. When the standard man-in-the middle attack is performed the Address Resolution Protocol is used (ARP). The hacker who has necessary programming tools, can make control over wireless network by using the ARP. ARP allows to perform main procedure, for this it is sending request to network interface card in order to reveal physical adress of card. It is the same as MAC (Media Access Control) address. This address assigned to card from its producer and it is unique. Proceeding from this, transferring network interface card must know MAC address. This card recognizes and reacts only to MAC address.

Applied programs, which are necessary to transfer data must have receiver's IP (Internet Protocol) address. Network interface card uses ARP protocol for revealing proper physical address. Network interface card receives necessary address, sends ARP packets. From this packets it is possible to know the IP address of receiver's network interface card. Every station must return packet of answer by using of ARP protocol. It contains MAC and IP address. Sender-station will include MAC address in the transferring frame as a receiver's address. Corresponding MAC and IP address are saved during periods of time. Saving will performed till the period while station will receive another ARP answer from the station which has this IP address.

Some problems can be arisen because of the using of ARP protocol. In most cases it is spoofing. Hacker can send fictitious ARP-answer by using medium devices. This ARP-answer consists of IP address of legitimate network device and MAC address of medium device. By using this operation, hacker sends wrong information to the station. All stations of legitimate network automatically updates its ARP tables. In this tables wrong data will be entered. As a result stations begin sending packets to the medium devices, instead of to legitimated access point. This is so called Man-in-the-middle attack. Hacker can get passwords, important data and can interract to the corporate servers as an legitimate user.

In order to avoid attacks ARP providers offer secure ARP. Such improved ARP creates special protected tunnel among all users and access points. This tunnel ignores all the ARP-answers which are not related to the users on the other side of tunnel. Only legitimate ARP-answers will serve to ARP tables updating process. Stations which uses SARP protocols are not inclined to spoofing.

For application of SARP protocol it is necessary to install special software on all the user devices. Using the SARP gives possibility to avoid man-in-the-middle attack.

As a result of Denial of Service (DoS) attack, wireless network will be useless or its working will be blocked. It causes serious financial loss for companies.

One of the types of DoS attack is brute-force attack. All the recources of the network are activated during sending information packets. As a result network stops working.

Stopping work of the wireless network is possible by using the powerful radiosignals, which can mute other signals. Access points and radio boards will be useless.

Some security mechanisms can help to perform DoS attack. For example, Wi-Fi Protected Access (WPA) mechanism can cause Denial of Service (DoS) attack. User of WPA network uses mathematical algorithms for authentification. If some user is trying to gain access to this network and sends two packets of unauthorised data during one second, WPA assumes that it is an attack and stops working of a network.

To avoid the DoS attack it is necessary to develop strong security rules, for example, setting and updating of firewall system, permanent updating antivirus systems, using the passwords with many symbols, etc.

It is possible to protect wireless network from radiosignals. There are several recommendations for decreasing radiosignals flow in the building:

- if buiding's inside walls have metallic surface it is desired to ground it.
- it is preferable to set up thermoisolation windows and cover them by metallic surface.
- building walls must be covered with metallic mixture paint outside and inside
- transmitter power must be regulated in such way that signal leakage can be excluded, or its level must be decreased to that value, which is necessary to easily reveal a hacker.

REFERENCES:

1. O. Shonia, G. Nareshelashvili, I. Kartvelishvili. Security of Wireless Networks. Georgian Technical University. Tbilisi, 2009.
2. M. Merritt, D. Pollino. Security of Wireless Networks. Moscow, 2004.

SECURITY ISSUES IN WIRELESS NETWORKS

IOSEB KARTVELISHVILI
Professor, European University, Georgia

TEA TODUA
Professor, European University, Georgia

KEYWORDS: WIRELESS NETWORKS SECURITY, DOS ATTACK, UNAUTHORISED ACCESS POINT, MAN IN THE MIDDLE ATTACK

SUMMARY

In the last period of time, security in wireless networks and quality of service, became very important and it is a subject of active researches. Communication signals which are extended in some environment can be received by someone else. Companies and individual users must recognize potentially existing problems and try to prevent them.

Every system which needs to secure has some deficiencies in it. These deficiencies or part of them can be used by attacker. Subsequently, for providing security of the system it is important to consider all possible threats and attacks which can be performed against the system. Security mechanisms must provide system security by considering the given threats, attacks and deficiencies.

In this article questions of security of wireless networks are discussed, it analyzes possible threats and the appropriate mechanisms of protection. The most common forms of threats of wireless networks (non-authorised access, Denial of service, DoS and man-in-the-middle attacks) are described by its own properties and are given recommendations for security issue.