International Journal of Academic Pedagogical Research (IJAPR)
ISSN: 2643-9123
Vol. 5 Issue 1, January - 2021, Pages: 61-64

Information Protection in Wireless Communication Systems

Usmonov Makhsud

Tashkent University of Information Technologies, Karshi branch 3rd year student
+99891 947 13 40
maqsudusmonov22@gmail.com

Abstract: *Wireless networks allow people to connect without a wired connection. This gives you the freedom to navigate and access apps at home, in urban areas, or in remote corners of the world. Wireless networks allow people to receive emails or browse Web pages wherever they want. There are many types of wireless networks, but the most important feature is that the connection is made between computer devices. Computers include personal digital assistants (PDAs), laptops, personal computers, servers, and printers.*

Keywords: power, global networks, transmitter, license, telecommunications, data transmission, asynchronous transmission.

INTRODUCTION

1. Wireless network concept and structure

2. Threats to the security of wireless networks

3. Wireless Network Security Protocols

Wireless network concept

Wireless networks allow people to connect without a wired connection. This gives you the freedom to navigate and access apps at home, in urban areas, or in remote corners of the world. Wireless networks allow people to receive emails or browse Web pages wherever they want. There are many types of wireless networks, but the most important feature is that the connection is made between computer devices. Computers include personal digital assistants (PDAs), laptops, personal computers, servers, and printers. Cell phones are not usually included in the list of computer devices, but the latest phones and even headsets have certain computing capabilities and network adapters. In the near future, most electronic devices will be able to connect to wireless networks.

METHODS

The following categories of wireless networks differ depending on the size of the physical area to which the connection is provided:

- Wireless personal-area network (PAN);

- Wireless local-area network (LAN);

- Wireless metropolitan-area network (MAN):

- Wireless Wide-area network (WAN).

Wireless private networks are characterized by a small transmission distance (up to 17 meters) and are used in a small building. The characteristics of such networks are average, and the transfer rate usually does not exceed 2Mb / s.

Such a network, for example, can provide wireless data synchronization on a user's PDA and on his or her PC or laptop. Similarly, a wireless connection with the printer is provided. Loss of clutter in the wiring that connects the computer to external devices is a significant advantage, as it makes it much easier to initially install external devices and then, if necessary, relocate them.

Wireless LANs provide high transmission characteristics inside and outside offices and workplaces. Users of such networks typically use PDAs with processors and large screens capable of running laptops, personal computers, and applications that require large resources. The employee can use the network services in the conference hall or in other rooms of the building. This allows the employee to perform their duties effectively. Wireless LANs can meet the requirements of all office or home applications at

speeds up to 54Mbit / s. In terms of characteristics, components, cost, and performance, such networks are similar to traditional Ethernet-type wired LANs.

Wireless regional networks serve a city-wide area. In most cases, applications require a dedicated connection, and sometimes mobility is required. For example, in a hospital, such a network provides data transmission between the main building and remote clinics. Or an energy company can use such a network on a city-wide basis to provide access to work from different districts. As a result, wireless regional networks aggregate existing network infrastructures or allow mobile users to connect to existing network infrastructures.

Wireless Internet Service Providers (WISP) provide wireless regional networks in cities and rural areas to provide regular wireless connections for home users and companies. Such networks are often more efficient than ordinary wired connections, which have limitations associated with laying wired connections.

Wireless regional network arn characteristics vary. The use of infrared technology in communications ensures data transfer speeds of 100 Gbps and above.

Wireless global networks enable mobile applications to be used across countries or even continents. Based on economic considerations, telecommunications companies are creating a relatively expensive infrastructure for a wireless global network that provides long-distance connectivity for many users. The cost of such a solution is shared among all users, so the subscription fee is not very high.

Users. Because the wireless network serves the user, the user can be seen as an important part of the wireless network. The user starts the process of using the wireless network and completes it himself. Therefore, it is permissible to call it "end user". Typically, a user interacts with a computer device that performs other tasks related to specific applications, in addition to interacting with the wireless network.

Threats to the security of wireless networks

There are many benefits to using wireless technology. While this technology gives users the feeling of being able to move around without losing touch, it provides a great opportunity for network developers to build connections. It also allows you to create many new devices to use the network. But wireless technology poses more threats than conventional wired networks. To create a secure wireless application, you need to identify all the routes through which wireless "attacks" can be transmitted. Unfortunately, apps are never completely secure, but a careful study of the risks of wireless technology can help increase the level of protection in any case. This means analyzing potential threats and building the network in such a way that it is able to prevent attacks and be prepared to defend against non-standard "attacks".

Uncontrolled territory

The main difference between wired and wireless networks is the completely uncontrolled zone between the network endpoints. In a sufficiently wide area of cellular networks, the wireless environment is never controlled. Modern wireless technologies offer a limited set of network space management tools. This allows attackers near wireless structures to carry out attacks that are not possible in a wired world.

Hearing in secret. The most common problem in an open and unmanaged environment, such as wireless networks, is the possibility of anonymous attacks.

Choking. Network failures occur when intentional or unintentional interference exceeds the sender's and receiver's capabilities in the communication channel. As a result, this channel is disabled. An attacker can use a variety of methods.

Refusal to provide services. An attack like DoS (Denial of Service) can completely shut down the network. Throughout the network, including base stations and client terminals, there is such a strong interference that stations cannot communicate with each other. This attack will block all communications within a certain range. It is difficult to prevent or stop a DoS attack on a wireless network. Most wireless networking technologies use unlicensed frequencies, which means there can be interference from multiple electronic devices.

Customer suffocation

Blocking the client station allows the fraudster to place himself in the position of the strangled client (Figure 24.3). It is also used to deny service to a customer in order to prevent them from making the connection. The intent of the very skillful attacks extends the existing connection in order to connect the corrupt human station to the base station.

Block the client station

WLTS protocol. The SSL / TLS-based WLTS protocol is used in WAP (Wireless Application Protocol) devices, such as mobile phones and PDAs. SSL and WLTS differ from each other in traffic levels. SSL relies on TCP to redirect lost packets or transmit non-standard packets. WLTS users using WLTS cannot use TCP to perform their functions because they only use UDP (user Datagram Protocol). The UDP protocol is not intended for connection, so these features should be included in the WLTS.

802.1x protocol. The main function of this protocol is authentication; in some cases, the protocol can be used to set encryption keys. Once connected, only 802.1x. DHCP (Dynamic Host Configuration Protocol) configuration protocol), IP, and h. such protocols are not allowed. Extensible Authentication Protocol (EAP) (RFC 2284) is used for user authentication.

RESULTS

There are many benefits to using wireless technology. While this technology gives users the feeling of being able to move around without losing touch, it provides a great opportunity for network developers to build connections. It also allows you to create many new devices to use the network. But wireless technology poses more threats than conventional wired networks. To create a secure wireless application, you need to identify all the routes through which wireless "attacks" can be transmitted. Unfortunately, apps are never completely secure, but a careful study of the risks of wireless technology can help increase the level of protection in any case. This means analyzing potential threats and building the network in such a way that it is able to prevent attacks and be prepared to defend against non-standard "attacks".

Uncontrolled territory

The main difference between wired and wireless networks is the completely uncontrolled zone between the network endpoints. In a sufficiently wide area of cellular networks, the wireless environment is never controlled. Modern wireless technologies offer a limited set of network space management tools. This allows attackers near wireless structures to carry out attacks that are not possible in a wired world.

Hearing in secret. The most common problem in an open and unmanaged environment, such as wireless networks, is the possibility of anonymous attacks.

Choking. Network failures occur when intentional or unintentional interference exceeds the sender's and receiver's capabilities in the communication channel. As a result, this channel is disabled. An attacker can use a variety of methods.

Refusal to provide services. An attack like DoS (Denial of Service) can completely shut down the network. Throughout the network, including base stations and client terminals, there is such a strong interference that stations cannot communicate with each other. This attack will block all communications within a certain range. It is difficult to prevent or stop a DoS attack on a wireless network. Most wireless networking technologies use unlicensed frequencies, which means there can be interference from multiple electronic devices.

DISCUSSION

Wireless private networks are characterized by a small transmission distance (up to 17 meters) and are used in a small building. The characteristics of such networks are average, and the transfer rate usually does not exceed 2Mb / s.

Such a network, for example, can provide wireless data synchronization on a user's PDA and on his or her PC or laptop. Similarly, a wireless connection with the printer is provided. Loss of clutter in the wiring that connects the computer to external devices is a significant advantage, as it makes it much easier to initially install external devices and then, if necessary, relocate them.

Wireless LANs provide high transmission characteristics inside and outside offices and workplaces. Users of such networks typically use PDAs with processors and large screens capable of running laptops, personal computers, and applications that require large resources. The employee can use the network services in the conference hall or in other rooms of the building. This allows the employee to perform their duties effectively. Wireless LANs can meet the requirements of all office or home applications at speeds up to 54Mbit / s. In terms of characteristics, components, cost, and performance, such networks are similar to traditional Ethernet-type wired LANs.

Wireless regional networks serve a city-wide area. In most cases, applications require a dedicated connection, and sometimes mobility is required. For example, in a hospital, such a network provides data transmission between the main building and remote clinics. Or an energy company can use such a network on a city-wide basis to provide access to work from different districts. As a result, wireless regional networks aggregate existing network infrastructures or allow mobile users to connect to existing network infrastructures.

CONCLUSION

802.1x protocol. The main function of this protocol is authentication; in some cases, the protocol can be used to set encryption keys. Once connected, only 802.1x. DHCP (Dynamic Host Configuration Protocol) configuration protocol), IP, and h. such protocols are not allowed. Extensible Authentication Protocol (EAP) (RFC 2284) is used for user authentication.

Wireless networks allow people to connect without a wired connection. This gives you the freedom to navigate and access apps at home, in urban areas, or in remote corners of the world. Wireless networks allow people to receive emails or browse Web pages wherever they want. There are many types of wireless networks, but the most important feature is that the connection is made between computer devices. Computers include personal digital assistants (PDAs), laptops, personal computers, servers, and printers. Cell phones are not usually included in the list of computer devices, but the latest phones and even headsets have certain computing capabilities and network adapters. In the near future, most electronic devices will be able to connect to wireless networks.

REFERENCES

1 Seymour Bosworth, Michel E. Kabay, Eric Whyne. Computer security handbook. Wiley.2014.

2Bulletin of the Oliy Majlis of the Republic of Uzbekistan. - T., 2003. - №1. - 2-m.

3Information security in the field of communication and information: Terms and definitions. Network standard: TSt 45-010: 2010.

4 Bulletin of the Supreme Council of the Republic of Uzbekistan. - T., 1993. - №5. - 232-m.

6 Sean Harris. ALL IN ONE CISSP. McGraw-Hill. 2013.

5Explanatory dictionary of information and communication technologies (second edition). - T., 2010.

6 See Tadjikhanov B.U. Ugolovno-pravovye mery borby s terrorizmom / Otv. ed. Ph.D. jurid. nauk A.S. Yakubov. - T .:, 2003. - S.4–20; Naumov A.V. Rossiyskoe ugolovnoe pravo. Obshchaya chast. - M., 1999. –162–163.

7 See Krylov V. Informatsionnye prestupleniya - novyy kriminologicheskiy object // Rossiyskaya yustitsiya. - 1997. - № 7 - S.22 - 23.

8 See Chichko L.. Kompyuternye xishcheniya // Rossiyskaya yustitsiya. - 1996. - №5. - S.45.

9 See Vexov V.B. Computer prestupleniya: sposoby sovershеniya i raskrytiya. - M., 1996. –S.163.

10 See Sorokin A.V. Computer prestupleniya: ugolovno-pravovaya characteristics, metodika i praktika raskrytiya i rassledovaniya. Internet resource: //http://kurgan.unets.ru/~procur/my_page.htm, 1999.

11 See Ugolovnoe pravo. Special time. - M., 1998. - S.546.

12 See Ugolovnoe pravo. Obshchaya chast / A.S.Yakubov, R. Kabulov et al. - T., 2005. - p. 112-119.

13 See Krylov V.V. Informatsionnye kompyuternye prestupleniya: Uchebnoe i prakticheskoe posobie. - M., 1997. - p. 40-44; Bogomolov M.V. Ugolovnaya otvetstvennost za nepravomernыy dostup k oxranyaemoy zakonom kompyuternoy informatsii. - Krasnoyarsk, 202. - S, 8 - 14; 62-64.

14 See Sottiev I.A. Legal means of combating organized crime: Textbook - T, 2005. - pp. 30-43.