International Journal for Social Studies

Available at https://edupediapublications.org/journals

ISSN: 2455-3220
Volume 03 Issue 07
June 2017

The Problems of Ensuring Network Security and Ways to Effectively Protect Against Network Attacks

Odil Olimovich Ishniyazov
(Tashkent University of Information Technologies named after Muhammad al-Khwarizmi assistant, Basic of Informatics)
Jahongir Bahtiyorovich Husainov
(Tashkent state university of law assistant, Department of Legal Informatics and Systems Analysis)

Computer and information technologies, telecommunications, information transfer networks, use of Internet services, chosen as one of the priority directions of our country's policy, are developing and modernizing more and more rapidly. Widespread introduction of modern information technologies in all sectors of our society serves to ensure the long-term goals of our state. The use of the Internet in each field of activity contributes to the effectiveness of its work.

It is the rapid exchange of information through the use of networks that can give the opportunity to gain time. In particular, the formation of the e-government system in our country, as well as the organization of the strengthening of the interconnection of the population and public administration on its basis, is carried out through the use of the network. Effective use of the network ensures the formation of a democratic information society. In such a society, the speed of information exchange increases, the efficiency of collecting, storing, processing and subsequent use of information.

At the same time, the problem of protecting information from illegal access to the network, use and modification, destruction of information remains urgent. At enterprises, organizations and government agencies, whose activities are connected to the network, before sharing communication for the exchange of information, serious attention should be paid to network security. Network security is implemented through the use of various tools and techniques, the implementation of measures and operations, the purpose of which is the system security of transmitted, stored and processed information. The tool used to ensure network security must quickly identify threats and take action against them. There are many types of threats to network security, they are divided into several categories:

- Listening or changing by means of an attack during the transfer of information (Eavesdropping);

ISSN: 2455-3220
Volume 03 Issue 07
June 2017

• denial of service; (Denial-of-service)

• Port scanning.

In the process of listening or changing by attack during the transfer of information, you can listen, change, block information transmitted through telephone lines, the Internet, videoconferences, sending by telefax without the knowledge of users of information. Such an attack can be done with the help of protocols analyzing several networks at once. Through the software that performs the attack, the digital sound of the CODEC standard (the system for changing the view or sound analog signal to a digital signal, or vice versa) is easily changed to high-quality but high-volume audio files (WAV). Usually, the attack process is not detected by the user. The system performs its tasks without any effort and noises. There is no suspicion of the theft of information. Only users who have preliminary information about a possible attack and who want to save the entire amount of information sent by using special security measures have the opportunity to exchange information over a secure network. In the process of information exchange over the network, there are several technologieseffective result against eavesdropping and changing the information sent:

• IPsec (Internet protocol security) protocol;

• Private virtual network VPN (Virtual Private Network);

• System for detecting illegal access to IDS (Intrusion Detection System).

Ipsec (Internet protocol security) provides the ability to securely exchange information over networks using security protocols and encryption algorithms. It by means of special standards provides mutual correspondence of programs and information, and also program devices at interaction of computers. With the help of the Ipsec protocol, the confidentiality of the information transmitted via the network is realized, that is, the clarity only for the sender and the recipient of information, the purity of information, and the authentication of packets. The use of modern information technologies becomes a necessary development tool for any organization, the Ipsec protocol provides effective protection for the following:

• when connecting the main office and branches through a global network;

• when the enterprise is remotely managed via the Internet;

• protecting the network associated with sponsors;

• Increase the security of e-commerce.

VPN (Virtual Private Network) is characterized as a virtual private network. This technology is aimed at providing reliable protection based on the exchange of all user information through the internal

International Journal for Social Studies

Available at https://edupediapublications.org/journals

ISSN: 2455-3220
Volume 03 Issue 07
June 2017

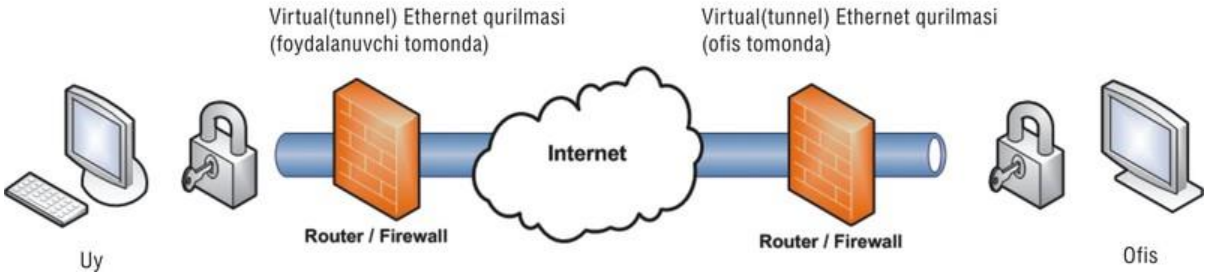
network. Nevertheless, the basis for the VPN is the Internet.

Advantages of VPN technology. By combining local networks into a common VPN network, a cheap and highly secure tunnel can be built. To create this network, you need on each computer that is part of a single network, a special VPN gateway, serving to exchange information between branches. Each department exchanges information in the usual way. If the information needs to be sent to another part of the VPN network, then all the information is sent to the gateway. In turn, the gateway processes the information, encrypts it based on a reliable algorithm, and then sends it to the gateway of another branch through the Internet. At this point, the information is again decrypted and transmitted to the desired computer in the usual way. All this is done completely unnoticed by the user and differs nothing from working on the local network. With the help of the Eavesdropping attack, the information obtained turns into a completely incomprehensible one.

Also, VPN is an excellent way to connect a separate computer to the organization's LAN. Imagine, you went on a business trip with your laptop, there is a need to join your network or obtain from it certain information. With the help of a special program you can contact the VPN gateway and carry out your activities as an ordinary employee in the office. It is not only easy, but also cheap.

The principle of the VPN. For the organization of the VPN network, in addition to new devices and software, two main parts are needed: the protocol for the transfer of information and the means to protect it.

Using the system for detecting illegal access (IDS), identifies techniques and tools that attempt to violate the security policy of the system or network. The system for detecting illegal access has almost a quarter century history. The first models and prototypes of the system for detecting illegal access were used to analyze information on the audit of computer systems. This system is divided into two main classes: the Network Intrusion Detection System and the system of detection of the illegal access to the computer (Host Intrusion Detection System).



The architecture of IDS systems consists of the following:

ISSN: 2455-3220
Volume 03 Issue 07
June 2017

• a system of a sensory part that collects and analyzes facts related to the security of secure systems;

• an analytical part system designed to detect suspicious actions and attacks on the basis of sensory information;

• a warehouse providing the collection of analysis results and information on preliminary positions;

• a management console that allows you to configure the IDS system, monitor the status of IDS and the protected system, conflicts detected by the analytic part system.

This system is divided into two main classes: the Network Intrusion Detection System and the system of detection of the illegal access to the computer (Host Intrusion Detection System). The principle of the system for detecting illegal access to the network (NIDS) is as follows:

1. checks traffic that has the right of access to the network;

2. Establishes a ban on harmful and unauthorized packages.

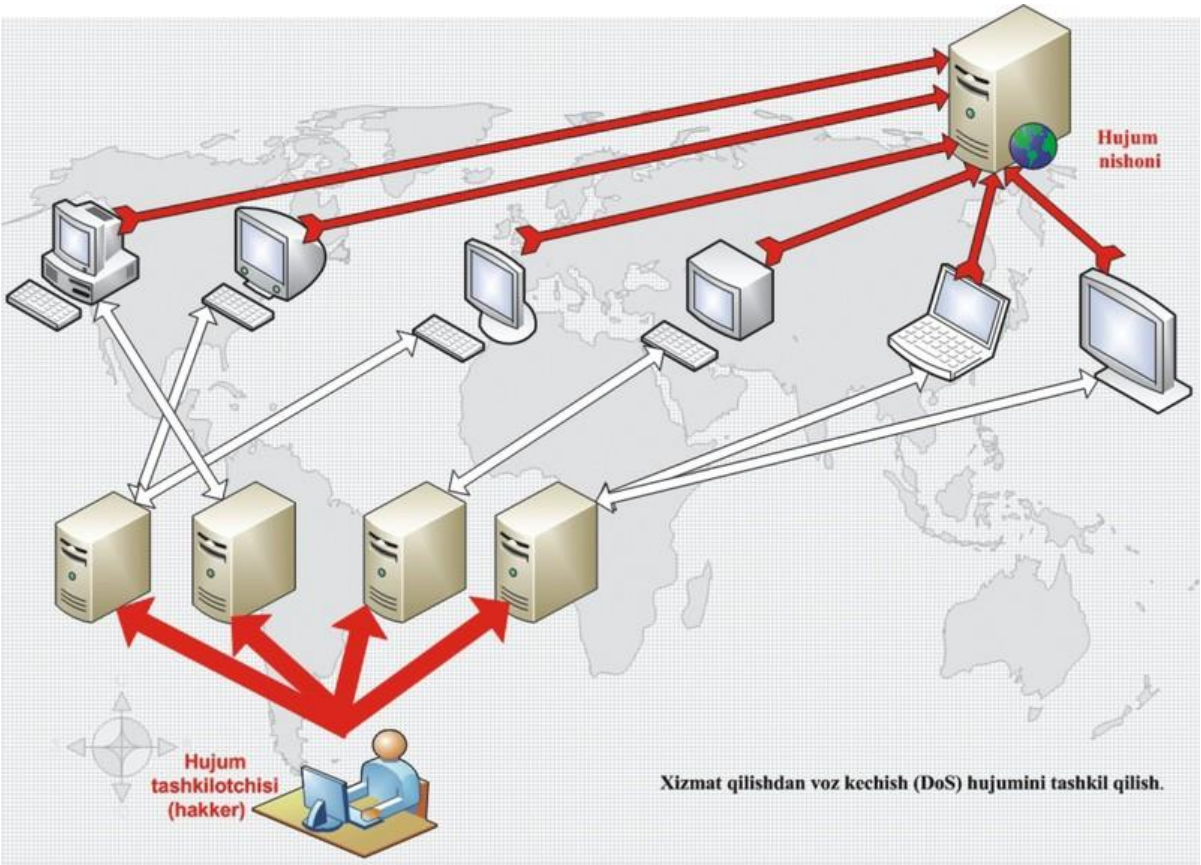
By using the listed security stages, you can effectively protect yourself from Eavesdropping threats.

DOS (Denial of service) - this type of network threat is called an attack in the form of a denial of service. In this case, the attacker tries to prevent the use of the network or the service by legitimate users. Often, such attacks are carried out in the form of overflow of permissions to infrastructure services. These attacks can be directed to both individual hosts and the entire system. Before the attack, the object is carefully studied, that is, the weaknesses and shortcomings of the protection against network attacks, which operating systems are installed, as well as the peak activity in the operation of the object. Based on the findings and results of the audit, a special program is being written. At the next stage, the created program is sent to authoritative servers. The servers send them to users registered on their databases. A legitimate user, knowing or not knowing that the program is directed by a reliable server, installs this program. A similar situation can happen in thousands, even millions of computers. At a certain time, the program is activated in all computers and starts to continuously send requests to the server of the object scheduled for the attack. The server, busy with a response to continuous requests, can not do its main job. Finally, in the server there is a refusal to work.

International Journal for Social Studies

Available at https://edupediapublications.org/journals

ISSN: 2455-3220
Volume 03 Issue 07
June 2017



The most effective ways to protect against attack type failure activity are as follows:

• Technology of firewalls (Firewall);

• IPsec protocol.

The firewall is the first protective device on the inner and outer perimeter. The firewall manages incoming and outgoing information in information and communication technologies (ACT) and, by filtering information, provides ACT protection by performing information checks based on certain criteria, making decisions about accessing packets to the system. The firewall scans all packets passing through the system, checking in accordance with certain rules all packets in two directions (input, output), decides whether to access them or deny access. Also, the firewall protects between two networks, that is, it protects a protected network from an open external network. The listed advantages of the protection, especially the packet filtering function, is an effective protection against DOS attacks. Packet filters control the following:

• the physical interface where the packet comes from;

• Source IP address;

• IP-address of the receiver;

• transport ports of the source and the receiver.

However, due to the following shortcomings, the firewall

ISSN: 2455-3220
Volume 03 Issue 07
June 2017

can not provide full protection against DOS attacks:

• design errors and shortcomings - different firewall technologies can not cover all ways of accessing a secure network;

• implementation flaws - each firewall, representing a complex software (hardware / software) complex, has its own mistakes. In addition, there is no unified methodology that will provide an opportunity to verify the quality of the implementation of the program, as well as testing to verify the reliability of implementation in the firewall of all its certified properties;

• Lacks of use (operation) - management of firewalls, configuration in accordance with the security policy is very complex, often there are cases of incorrect configuration of firewalls.

The listed shortcomings can be eliminated using the IPsec protocol. Summarizing the above, we can conclude that the proper use of firewalls and the IPsec protocol allows for sufficient protection against DOS attacks.

The type of Port scanning attack, usually is often applied to computers that provide network services. To ensure network security, we should pay more attention to virtual ports. Because ports are means of information delivery through channels. There are 65,536 standard ports on the computer. In a figurative sense, computer ports can be compared to doors or windows of a house. The attack in the form of scanning ports, it may be said, is similar to the preliminary check of thieves, whether the doors are open, whether there are holes in them. If the thief finds out that the windows are open, getting inside the house will make it easier. When attacking a hacker, to obtain information about the openness or non-use of ports, uses the Port scanning attack.

In this case, for the simultaneous analysis of all ports, a request is sent, as a result, in real-time it becomes clear which computer port the user is using, it is the weak point of the computer. It is through the number of the detected port that you can find out which service the user is using. For example, as a result of the analysis, the following port numbers were identified, this way it is possible to identify the services that are currently used:

• Port # 21: FTP (File Transfer Protocol) - the file exchange protocol;

• Port # 35: Private printer, server;

• Port # 80: HTTP traffic (Hypertext Transfer [Transport] Protocol) Hypertext exchange protocol;

• Port # 110: POP3 (Post Office Protocol 3) is the E-mail protocol.

ISSN: 2455-3220
Volume 03 Issue 07
June 2017

Hujum turlari	Himoya vositalari
Axborotni uzatish jarayonida hujum qilish orqali, eshitish va o'zgartirish (*Eavesdropping*)	IPSec (*Internet protocol security*) protokoli. VPN (*Virtual Private Network*) virtual xususiy tarmoq IDS (*Intrusion Detection System*) ruxsatsiz kirishlarni aniqlash tizimi
Xizmat ko'rsatishdan voz kechish (*Denial-of-service*)	Tarmoqlararo ekranlar texnologiyasi (*Firewall*) IPSec (*Internet protocol security*) protokoli.
Portlarni tekshirish (*Port scanning*)	Tarmoqlararo ekranlar texnologiyasi (*Firewall*)

As a means of protecting against the attack of Port scanning, the use of the firewall gives the expected effect. An attack in the form of simultaneous requests for port checking can be mirrored by implementing a special rule on the response in a given situation on the firewal

l.