International Journal of Academic Engineering Research (IJAER)
ISSN: 2643-9085
Vol. 5 Issue 1, January - 2021, Pages: 14-21

Establish Network Protection

Usmonov Makhsud

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

Abstract: *In order to process confidential information, it is necessary to use computers that have passed the necessary verification. It is important that the protective equipment is fully functional. In this case, the work of the system administrator and the control carried out are of great importance. For example, users change passwords frequently and the length of passwords makes it difficult to identify them. Therefore, it is important to limit the registration of a new user (for example, only during working hours or only at the company where he works). It is necessary to make a feedback (for example, using a modem) to verify the authenticity of the user. It is possible to use the mechanism of restriction of access to information resources and its effect on LAN objects.*

Keywords: LAN, WAN, Network protection, computer telephony.

INTRODUCTION

1. Weak parts of computer networks.

2. Basics of network protection.

3. Methods of protection in computer telephony.

4. Ways to provide protection in computer networks.

5. Technical means of computer protection.

6. The main directions of data protection in computer networks

1. Weak parts of computer networks.

Currently, the differences between local area network (LAN) and global computing networks (WAN) are disappearing. For example, Netware 4x or Vines 4.11. operating systems are taking LAN operations to the regional level. This, in turn, increases the capacity of the LAN, which requires further improvement of data protection methods.

METHODS

The following should be considered when designing a safeguard:

• large number of entities connected to the system, and in many cases, some users are out of control;

• availability of necessary information for the user in the network:

• use of personal computers manufactured by different companies in the network;

• the ability to use different programs in the network system;

• Due to the fact that the network elements are located in different countries, the length of communication cables laid in these countries and their complete, almost impossible to control;

• use of information resources by several users at the same time;

• connection of several systems to the network;

• slight expansion of the network, ie the uncertainty of the boundaries of the system and the uncertainty of who works in it;

• multiplicity of attack points;

• Difficulty controlling access.

The need to protect the network arises in the following cases:

• read arrays of other users; • Read data stored in computer memory

bypassing security measures and harassing media;

• work anonymously as a user;

• use of software holders;

• exploiting the shortcomings of programming languages; • Deliberate dismissal of protective equipment

• Input and use of computer viruses.

The following should be taken into account when organizing the protection of the network: • control of the security system;

• file access control;

• control of data transmission in the network; • control over access to information resources; • control the flow of data to another network-connected tapmoklap

Fundamentals of network protection

In order to process confidential information, it is necessary to use computers that have passed the necessary checks. It is important that the protective equipment is fully functional. In this case, the work of the system administrator and the control carried out are of great importance. For example, users change passwords frequently and the length of passwords makes it difficult to identify them. Therefore, it is important to limit the registration of a new user (for example, only during working hours or only at the company where he works). It is necessary to make a feedback (for example, using a modem) to verify the authenticity of the user. It is possible to use the mechanism of restriction of access to information resources and its effect can be fully transferred to LAN objects.

The following measures should be taken to protect the data transmitted between the elements of the network:

• do not allow data to be identified;

• not to allow the analysis of information exchange;

• do not allow messages to be changed;

• Prevent covert connections and detect them quickly.

Cryptographic protection during data transmission over the network

methods should be used, and information about unauthorized entries should be recorded in the logbook. Restriction of access to this log should also be done through safeguards.

The main reason for the complexity of controlling a computer network is the complexity of controlling the software. In addition, many computer viruses are networked makes it difficult to control the flow.

Until now, even though security software was diverse, operating systems did not provide the required level of protection. Netware 4.1, Windows NT operating systems can provide adequate protection.

Methods of protection in computer telephony

Modern technologies of electronic communications have recently created many opportunities for businessmen to transmit various forms of information (eg, fax, video, computer, speech) through communication channels.

The modern office today is overcrowded with means of communication and office equipment, and includes telephones, fax machines, answering machines, modems, scanners, personal computers, and so on. enters. The development of information and communication technology - computer telephony for modern technology has given a great impetus. Only ten years ago, CANON launched the Navigator, a $ 6,000 product, and is one of the first systems to do so.

Computer telephony has grown rapidly over the past decade. The currently available PC Phone (Export Industries Ltd, Israel) costs only 1,000 German marks. Powertine-II (Talking Technology, USA) costs $ 800. Recently, 70% of computer telephony equipment is manufactured by Dialogue (USA).

Information security is very important in computer telephony. For example, the fact that phone hackers broke into the Scotland Yard ATS and caused $ 1.5 million in damage proves the need for security.

Speech recognition technology used in computer telephony is important for recognizing the caller's voice. Pretty Good Privacy Inc. is committed to providing adequate protection for computer telephony. The company has developed a PC Phone 1.0 software package. It digitizes information to protect it from being transmitted over computer telephony, and processes it with software and hardware during reception. The encryption speed of modern computer telephony tools is also very high, and the probability of error is very small (about 10-8 - 10-12).

Ways to protect your computer network

Information security in computer networks refers to technical, software and cryptographic methods and tools, as well as organizational measures to prevent users from owning unauthorized networks, elements and resources. The methods and means of ensuring information security in direct telecommunication channels can be classified as follows

Methods

Tuskin-lik

Ownership management

Nikob-lash

Sorting

Coercion

Unda - mok

It is accepted to describe the above methods as follows.

Depression is said to be a physical resistance to access to devices, data carriers, and so on.

Ownership management is a way of regulating the operation of system resources. This method consists of the following functions:

• identification of each object, element of the system, for example, users;

• Identify the object or subject of identification as authentic;

• verification of competencies, ie verification of the availability of the required number of days, daily hours, required reserves in accordance with the selected work schedule (regulations);

• creation of working conditions and permission to work in accordance with the adopted regulations;

• registration of appeals to protected reserves;

• Responding to unauthorized actions, such as signaling, refusing to complete a survey, etc.

Masking is the process of encrypting data to make it difficult to read.

Sorting - When working with data, conditions are created to reduce the likelihood of unauthorized access to the system.

Coercion is the processing of data according to accepted rules, otherwise users will be subject to material, administrative and criminal penalties.

Undamok is aimed at carrying out the procedures adopted in accordance with the rules of morality and ethics.

In the implementation of the above methods apply the tools classified as follows.

Formal tools are tools that perform the function of protecting information without the involvement of individuals

Informal means are regulations that directly determine the activities of individuals or their activities.

Technical means are electrical, electromechanical and electronic devices. Technical means can be physical and hardware, respectively.

Hardware means devices included in telecommunication devices or connected to it through an interface. For example, a pair of data control diagrams is a control used to detect misinterpretation of information on the road, and automatically checks the number of work pairs (along with the control discharge).

Physical hardware is devices and systems that operate autonomously. For example, simple door locks, metal bars installed on windows, electrical installation equipment are physical and technical means.

Software is specialized software designed to perform information security functions. The most widely used software tools in data protection in the first place are currently the second most common means of protection. An example of this is the password system.

Organizational protection means are organizational-technical and organizational-legal measures taken in the process of creation and use of telecommunication equipment. A direct example of this is the following processes: construction of buildings, system design, installation, inspection and commissioning of facilities.

Moral and ethical safeguards are the procedures and arrangements that arise as a result of the development of computer technology. While these procedures are not found at the level of the law, failure to recognize it can damage users 'reputations.

Legal remedies are legal documents developed by the state. They regulate the use, processing and transmission of indirect information and define the responsibilities of violators of these rules.

For example, the rules developed by the Central Bank of the Republic of Uzbekistan clearly define the organization of information protection groups, their powers, duties and responsibilities.

The development of methods and tools for security can be divided into three stages: 1) the development of software; 2) development in all directions; 3) At this stage, developments are observed in the following areas:

- hardware implementation of protection functions;

- creation of means covering several protection functions; - generalization and standardization of algorithms and technical means.

In order to protect the data transmitted directly over the network, the following measures should be taken:

- avoid disclosure of transmitted data;

- protection of the transmitted data from tampering;

- prevent the transfer of data and identify attempts to change it;

- prevent the detection of software interrupts used for data transmission;

- prevention of fraudulent connections.

Cryptographic methods are mainly used in the implementation of these measures.

Technical means of providing computer protection

As a result of computer-related crimes, the United States alone spends $ 100 billion a year. dollars in losses. On average, $ 430,000 is stolen in each crime, and the probability of finding the culprit is 0.004%.

According to experts, 80% of these crimes are committed directly by employees of the enterprise.

The analysis of the committed crimes gives the following conclusions:

In many computer networks, the user can connect to the network from any workstation. As a result, it is difficult to determine from which computer the offender did the work.

• As a result of the abduction, nothing is lost, so often no criminal proceedings are instituted; • Lack of ownership of the data;

• Errors made during data processing are not observed and corrected in a timely manner, and as a result, future errors cannot be prevented;

• Computer crimes are not reported in a timely manner, as this is to hide the shortcomings of computer networks from other employees.

In order to eliminate these shortcomings and reduce computer crime, the following measures should be taken:

• increase staff responsibility:

• inspection of recruits; • replacement of employees performing important functions;

• Setting passwords and user accounts in a good way; • Restrict access to information;

• data encryption.

As a result of the development of information and communication technologies, many information security tools have been developed. They are software, software and hardware.

Currently, hardware designed to ensure network security can be classified as follows:

Physical protection devices are devices that prevent access to information using special electronic devices.

Logical protection is used by software to prevent access to data.

Firewalls and gateways - the information that enters and leaves the system Checks and records with known attacks.

Security audit systems are systems used to detect vulnerabilities in the parameters set from the implemented operating system.

Real-time security system - provides continuous network security analysis and audit.

Stochastic testing tools are a tool used to check the quality and reliability of information systems.

Thematic directional tests are used to check the quality and reliability of information and communication technologies.

Imitation of threats - threats are created to information systems and the effectiveness of protection is determined.

Statistical analyzers are used to identify deficiencies in the structure of programs, to find undefined entry and exit points in the program code, to determine the correctness of the variables in the program, and to determine the part programs that do not fall.

Dynamic analyzers are used to track executable programs and detect changes in the system.

Network vulnerability detection is used to identify existing vulnerabilities by organizing artificial attacks on network resources.

Examples include the following tools:

• Dallas Lock for Administrator is a software and hardware tool based on existing electronic Proximity equipment that is used to control unauthorized access to direct data.

Security Administrator Tool for ANALYSING Networks (SATAN) is software that directly identifies network vulnerabilities and provides solutions. Several programs have been developed in this area, such as Internet Security Scanner, Net Scanner, Internet Scanner and others.

• NBS system - a software and hardware tool used to protect data on communication channels;

• Free Space Communication System - allows the exchange of data in the network through various beams, such as laser beams;

• SDS system - this software controls the system data and displays it in the account. Its main function is to control unauthorized access to data transmission media;

• Timekey is a software and hardware that is installed directly on the parallel port of the computer and prevents the widespread use of software in a timely manner;

• IDX is a software and hardware tool that "reads" and analyzes the user's fingerprints, provides high-quality information security. It takes up to 1 minute to read and memorize fingerprints, and up to 6 seconds to compare.

The main directions of data protection in computer networks Comparison of existing methods and means of data protection and the evolution of communication security technology in computer network channels show that in the first stage of technology development software was preferred and developed, in the second stage all protection characterized by the intensive development of methods and tools, and in the third stage the following trends are evident:

- technical implementation of the main functions of information protection;

- creation of joint means of protection performing several security functions:

- unification and standardization of algorithms and technical means.

It is always important to keep in mind that attacks on computer networks are carried out by highly qualified professionals. This requires the creation of models that are always superior to their motion models. In addition, personnel are one of the most influential parts of automated information systems. Therefore, it is important to take measures to prevent the malicious person from using the information system staff.

RESULTS

Network vulnerability detection is used to identify existing vulnerabilities by organizing artificial attacks on network resources.

Examples include the following tools:

• Dallas Lock for Administrator is a software and hardware tool based on existing electronic Proximity equipment that is used to control unauthorized access to direct data.

Security Administrator Tool for ANALYSING Networks (SATAN) is software that directly identifies network vulnerabilities and provides solutions. Several programs have been developed in this area, such as Internet Security Scanner, Net Scanner, Internet Scanner and others.

• NBS system - a software and hardware tool used to protect data on communication channels;

• Free Space Communication System - allows the exchange of data in the network through various beams, such as laser beams;

• SDS system - this software controls the system data and displays it in the account. Its main function is to control unauthorized access to data transmission media;

• Timekey is a software and hardware that is installed directly on the parallel port of the computer and prevents the widespread use of software in a timely manner;

• IDX is a software and hardware tool that "reads" and analyzes the user's fingerprints, provides high-quality information security. It takes up to 1 minute to read and memorize fingerprints, and up to 6 seconds to compare.

The main directions of data protection in computer networks Comparison of existing methods and means of data protection and the evolution of communication security technology in computer network channels show that in the first stage of technology development software was preferred and developed, in the second stage all protection characterized by the intensive development of methods and tools, and in the third stage the following trends are evident:

- technical implementation of the main functions of information protection;

- creation of joint means of protection performing several security functions:

- unification and standardization of algorithms and technical means.

DISCUSSION

Masking is the process of encrypting data to make it difficult to read.

Sorting - When working with data, conditions are created to reduce the likelihood of unauthorized access to the system.

Coercion is the processing of data according to accepted rules, otherwise users will be subject to material, administrative and criminal penalties.

Undamok is aimed at carrying out the procedures adopted in accordance with the rules of morality and ethics.

In the implementation of the above methods apply the tools classified as follows.

Formal tools are tools that perform the function of protecting information without the involvement of individuals

Informal means are regulations that directly determine the activities of individuals or their activities.

Technical means are electrical, electromechanical and electronic devices. Technical means can be physical and hardware, respectively.

Hardware means devices included in telecommunication devices or connected to it through an interface. For example, a pair of data control diagrams is a control used to detect misinterpretation of information on the road, and automatically checks the number of work pairs (along with the control discharge).

Physical hardware is devices and systems that operate autonomously. For example, simple door locks, metal bars installed on windows, electrical installation equipment are physical and technical means.

Software is specialized software designed to perform information security functions. The most widely used software tools in data protection in the first place are currently the second most common means of protection. An example of this is the password system.

Organizational protection means are organizational-technical and organizational-legal measures taken in the process of creation and use of telecommunication equipment. A direct example of this is the following processes: construction of buildings, system design, installation, inspection and commissioning of facilities.

Moral and ethical safeguards are the procedures and arrangements that arise as a result of the development of computer technology. While these procedures are not found at the level of the law, failure to recognize it can damage users 'reputations.

Legal remedies are legal documents developed by the state. They regulate the use, processing and transmission of indirect information and define the responsibilities of violators of these rules.

For example, the rules developed by the Central Bank of the Republic of Uzbekistan clearly define the organization of information protection groups, their powers, duties and responsibilities.

CONCLUSION

In order to process confidential information, it is necessary to use computers that have passed the necessary checks. It is important that the protective equipment is fully functional. In this case, the work of the system administrator and the control carried out are of great importance. For example, users change passwords frequently and the length of passwords makes it difficult to identify them. Therefore, it is important to limit the registration of a new user (for example, only during working hours or only at the company where he works). It is necessary to make a feedback (for example, using a modem) to verify the authenticity of the user. It is possible to use the mechanism of restriction of access to information resources and its effect can be fully transferred to LAN objects.

REFERENCES

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

2 Bulletin 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.

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

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

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