AMERICAN Journal of Science on Integration and Human Development
Volume 01, Issue 03, 2023 ISSN (E): XXX-XXX

Information Security Problems of Computer Networks

Abdullaev Sharof Abdugafforovich
Termez State University, Teacher of the Department of Information Technology

Abstract:

The article deals with the problems of information security of computer networks and the main functions of the information security system.

Keywords: problems of information, computer networks.

In connection with the “multi-user” mode of operation in a computer network, a whole set of interrelated issues arises regarding the protection of information stored in computers or servers in a computer network [1, 2].

It should be noted that the network operating systems themselves also provide powerful protection against unauthorized access to network resources. However, there are cases when even such protection does not work. Practice shows that an unauthorized user with sufficient experience in the field of system and network programming, who set out to connect to the network, even with limited access to certain resources, sooner or later can still gain access to some protected network resources. Therefore, there is a need to create additional hardware and software to protect network resources.

Hardware protection tools include various firewalls, filters, protocol encryption devices, etc. Software protection tools include: data encryption programs; network connection tracking programs (network monitoring); authentication and identification programs, etc. When developing large-scale computer networks, the problem arises of ensuring the interaction of a large number of computers and servers, i.e., the problem of finding optimal topologies. The most important component of local and corporate networks is their system topology, which is determined by the architecture of intercomputer connections [3–4].

It is known that critical information must be processed in computer networks to ensure security.

The term "critical information" refers to information:

with various secrecy stamps; information for official use;

information constituting a trade secret or company secret;

information that is the property of some organization or individual.

Let us give some basic definitions. Exposure is a form of possible loss or damage to a computer network. For example, exposures are considered to be unauthorized access to data or counteracting the authorized use of a computer network. A vulnerability is a security weakness that can cause damage to a computer network.

An attack is an action of some subject of a computer network that uses a vulnerability of a computer network to achieve goals that go beyond the authorization of this subject in a computer

network. A threat to a computer network is a condition that has the potential to cause damage to a computer network.

Management in security terminology is a protective mechanism (action, device, procedure, technology, etc.) that reduces the vulnerability of a computer network.

Each network node is an independent computer system with all its inherent problems, and there are also problems associated with communication lines and the procedure for transmitting information. From the point of view of security, computer networks have the following disadvantages: - sharing of resources. Because resources and load are shared across different nodes on the network, many users have the potential to access the network as a single computer system. In other words, having gained access to one of the systems included in the network, the user (or invader) has a real opportunity to attack other network systems; - the complexity of the system. Every computer system has an operating system, which is a complex set of interacting programs.

Because of this circumstance, it is difficult to formulate clear security requirements, especially for general-purpose networks that were developed without security in mind; – undefined periphery.

The vulnerability of the network is strongly affected by the inability to determine, in most cases, the exact limits of the network. One and the same node can simultaneously work in several networks, and, therefore, the resources of one network may well be used from nodes that are part of another network. Such a wide-ranging sharing of resources is undoubtedly an advantage.

However, an indefinite number of potentially unprepared users and potential invaders greatly complicates the security of both the network as a whole and most of its individual nodes; - multiple points of attack. On a single computer system, it is possible to control access to the system by users as that access is provided from the terminals of the computer system.

The situation on the network is completely different: the same file can be requested by the so-called remote access from different network nodes. Therefore, if the administrator of a particular system can pursue a clear security policy in relation to his system, then the network host administrator is deprived of such an opportunity;

- unknown access trajectory. A user or invader can request access to the resources of some network node with which this node is not directly connected.

In such cases, access is through some intermediate node connected to both nodes, or even through several intermediate nodes. In a network environment, it's not easy to pinpoint exactly where the access request came from, especially if the invader goes to great lengths to hide it;

- weak security of the communication line. The network differs from a separate system in that it certainly includes communication lines through which data is transmitted between nodes.

It can be an elementary wire, or it can be a radio communication line, including a satellite channel. Under certain conditions (and appropriate equipment), you can imperceptibly (or almost imperceptibly) connect to the wire, you can successfully listen to the radio link - that is, nothing prevents you from “pumping out” the transmitted messages from the communication lines and then isolating the required.

Based on the analysis of computer network security threats, conclusions can be drawn about the properties and functions that a corporate network (CN) security system should have.

Identification of protected resources, i.e. assignment of identifiers to protected resources - unique features, by which the system subsequently performs authentication. Authentication of protected resources, i.e., their identification based on comparison with reference identifiers. Apply password protection of resources. Differentiation of user access to the CS. Differentiation of user access by operations (reading, writing, modification, etc.) over resources (programs, files, directories, disks, servers, etc.) using software administration tools.

Registration of events: a user entering the network, leaving the network, violation of access rights to protected resources, etc. Reaction to the facts of violation of access rights to protected network resources, unauthorized connection to the CS. Ensuring the protection of information during maintenance and repair work.

Literature:

1. Широчин В. П., Мухин В. Е., Кулик А. В. Вопросы проектирования средств защиты информации в компьютерных системах и сетях. Киев; «ВЕК+». 2000. — 111 с.
2. Ганиев С. К., Каримов М. М. «Вопросы оптимального сегментирования топологии локальных компьютерных сетей».-Ташкент, Проблемы информатики и энергетики, 2001,№ 2.-С.20–25.
3. В. Г. Олифер, Н. А. Олифер.Компьютерные сети. Принципы, технологии, протоколы 4 издание — Питер-2010. 944с.
4. Платонов В. В. Программно-аппаратные средства защиты информации: учебник для студ. Учреждений выс. Образования/ — М.: Издательский центр «Академия», 2014.