УДК 61:004.651 (075.8)
І.Є.Андрущак, І.В.Андрощук
Луцький національний технічний університет

CONCEPT AND SECURITY TECHNOLOGY COMPUTER NETWORKS

I.Ye.Andrushchak, I.V.Androshchuk. Concept and security technology computer networks. In this paper, a review of the history of the formation of the issue of technology and the concept of security of computer networks, current state and prospects of development of methods and tools for security in networks. Highlight key aspects of building planes and the use of technology in modern security systems of computer networks. Highlighted key issues, normative and technical security of computer networks.
Keywords: Computer network, content filtering, information security, integrated content filtering system, model receiving content.

І.Є.Андрущак, І.В.Андрощук. Концепція та технологія безпеки компютерної мережі. В роботі проведено огляд історії становлення питання про технологію та концепцію безпеки компютерних мереж, сучасного стану та перспектив розвитку методів та засобів безпеки в мережах. Виділено ключові площини аспектів розбудови та застосування технологій систем безпеки в сучасних компютерних мережах. Підкреслено основні проблемні питання, нормативно- правового та технічного характеру безпеки компютерних мереж.
Ключові слова: компютерна мережа, фільтрація контенту, інформаційна безпека, комплексні системи фільтрації контенту.

И.Е.Андрущак, И.В.Андрощук. Концепция и технология безопасности компьютерной сети. В работе проведен обзор истории становления вопрос о технологии и концепции безопасности компьютерных сетей, современного состояния и перспектив развития методов и средств безопасности в сетях. Выделены ключевые плоскости аспектов развития и применения технологий систем безопасности в современных компьютерных сетях. Подчеркнуто основные проблемные вопросы, нормативно- правового и технического характера безопасности компьютерных сетей.
Ключевые слова: компьютерная сеть, фильтрация контента, информационная безопасность, комплексные системы фильтрации контента, модель получения контента.

Security Information Network Protection includes hardware, software, data and personnel. Network security consists of the provisions and policies adopted by the network administrator to prevent and monitor unauthorized access, misuse, modification or denial of the computer network and available resources. Network security includes permission to access the data network that is provided by the network administrator. Users choose or are assigned their ID and password or other authentication information, allowing them to access the information and applications within their authority.

Network security includes a variety of computer networks, both public and private, which are used in the daily workplace for transactions and relationships between enterprises, government agencies and individuals. Networks can be private, such as inside a company or open to the public. Network security is involved in organizations, enterprises and other types of institutions. The most common and easy way to protect network resources is to give them a unique name and corresponding password [1].

At a time when computer systems are the foundation of security of entire countries and databases - the main capital of many companies, virus protection stands next to general issues of economic security as the country as a whole and individual institutions and organizations. Especially this problem for institutions and businesses that deal with sensitive data about customers. Theft, destruction, distortion of information, failure and rejection computer systems - the problems that carry the viruses and virus programs.

Threats to information security can be divided into two types: threats that are random (their source may be unintentional errors in software, failure of hardware, incorrect user actions) and threats intended that, unlike random, pursuing the goal causing intentional damage information system, data theft, damage to natural or legal persons.

Network security starts with authentication usually involves a username and password. If you need only one piece of authentication (username), it is called single-factor authentication. With two-factor authentication, the user still has to use a security token or 'key' credit card or mobile phone at contol authentication, the user must use a fingerprint scan or take retina.

After authentication, firewall provides access to network users. For detection and suppression action malware using antivirus software or intrusion prevention systems (IPS).

The connection between two computers using network can be encrypted to preserve

confidentiality.

Data protection is one of the main problems of computer networks as an advantage network access to shared data and devices, and this leads to the possibility of unauthorized access to data.

Data security is to protect network resources from destruction and protect data from accidental or intentional disclosure, as well as the unlawful changes.

Designed to ensure the security of the network administrator. In large networks this purpose there are special positions (security officers). To ensure data security developed multilevel system of protection:

- built-in protection - software and system (passwords, permissions);
- physical protection - locks, door security, alarm;
- administrative control - arrangements, orders administration;
- legislation and social environment - the laws of copyright and property rights, intolerance of software piracy.

US Department of Defense in the book "Computer Security Evaluation Criteria" (Orange Book), has identified seven levels of security and computer network systems. This development became common in the world to classify the security of the system. , The following levels of protection [3]:

- D – the level of minimum protection (Minimal Protection). Restricted systems at other levels do not guarantee the required level of security;
- C1 – level of protection selective (Discretionary Protection). Allows users to apply access restrictions to protect private information;
- C2 – controlled level of access (Controlled Access Protection). Includes requirements Level C1, and the protection of the registration process in the system records events protection, resource isolation different processes;
- B1 – protection by category (Labeled Protection). By requirements of C2 added ability to protect individual files, records in the files, and other objects of special security tags stored together with these objects. It is believed that such protection can overcome well-trained hacker as a normal user - no;
- B2 – Structured protection level (Structured Protection). By B1 level requirements attached full protection of all system resources directly or indirectly available to the user. It is believed that hackers can not penetrate the system with such protection;
- B3 – Domain level security (Security Domains). For the demands of B2 is added to a clear specification of users who are prohibited access to certain resources, fuller sign of potentially dangerous events. It is believed that even experienced programmers unable to overcome the system with this level of security;
- A1 – verified level of development (Verified Design). Full protection. Specified and verifiable mechanisms for protection. It is believed that in the system with this level of protection without permission can not penetrate no.

Some systems (like banking or tax) need not user identification and individual. Distinguishes several ways such identification.

For personal physical characteristics (biometrics). Remove fingerprint or hand geometry, retina, pupil, facial features, and then analyzed. Alternatively, the system offers again a number of randomly selected words and analyzes the features of voice.

For a subject that person-to-user to carry. This can be the subject of a special badge, magnetic card code. This method is cheap but unreliable, the subject can be faked, steal, etc. [5].

For that person must know or remember. We must remember the password or correctly answer a series of questions. This method is the cheapest and most common, but unreliable (password can be selected answers guess).

Safety is ensured by the use of a network the right to access, authentication and registration of connections.

The identification process is called user authentication. Standard authentication method - using a user name and password as the previous pair of identifiers is intended that the user must enter at the request system for obtaining access to network resources. In this, the most simple form of authentication user ID and password are transmitted over the network in clear text (ie not encrypted). The process of authentication - comparing pairs identifiers transmitted with the records of the table located on the server - is performed according to the protocol for authentication password (Password Authentication Protocol,

PAP). Recordings are stored encrypted, unlike couples identifiers transmitted and this is a weakness of this method of authentication.

A more advanced challenge-response system operates according to the authentication protocol for establishing communication with the (Challenge Handshake Authentication Protocol, CHAP). Under this protocol, agent authentication (software located on the server) sends the user to a key by which that encrypts your username and password and sends this information back to the server. Authorization - the process of providing the user the right access to the system in which a user name and password assigned to him are recorded in a special table systems [7].

Widespread system that provides a high level of protection for authentication, challenge-response system, which uses a smart card.

Control attempts to access the network, you can easily determine whether an unauthorized user was trying to sneak in, and see if you forgot your password anyone of staff.

Blocking access. In many organizations as user IDs cited their initials and surname. Attackers try to sneak in, it was enough to know the following. Software developers have created a program block access to the system. Often software that performs blocking access allows you to specify another threshold, this threshold is determined by the time during which the system will be locked.

An important concept of data protection issues in the networks is recognition.

Recognition - a guarantee that information (package) came from a legitimate source rightful recipient.

Indeed, one of the most common practices malicious networks are packet sniffing and substitute their own or directing them to another destination. Therefore, all modern network protocols are usually equipped with means of recognition. One of the mechanisms of recognition packages are hotel and destination of the same pseudorandom number generator. Each package indicate random number which is compared with the same number of the recipient.

A similar task performs electronic signature - a sequence of bytes that form special algorithms and whose authenticity can be verified.

To recognize use separate servers that issue electronic certificates. Servers used in the certification of sufficiently powerful operating systems.

One of the most prominent solutions is the system of centralized recognition Kerberos (it is implemented by programming and is compatible with all types of systems. System works in client-server paradigm. It consists of client software, deployed on workstations, users, and server applications. There are three types of server programs: recognition server, the server permits and server administration. In the process of recognition of the client involved in the first two of these servers. Each server has a scope defined by the content of its database of users).

To measure recognition accuracy using two indicators: the percentage of false identification (False Acceptance Rate (FAR)) and the percentage of false recognition (False Rejection Rate (FRR)).

The original meaning of the firewall (firewall) - a wall in a building made of fire-resistant and non-flammable material that can prevent the spread of fire. In computer network firewall - a computer with a software system which is installed on the network edge and allow that only authorized packets in a certain way. [6]

Most firewalls to protect internal corporate network from attacks from external networks. However, they can be used to filter the output information, limiting user access internal network outside.

Sometimes firewall functions in complex systems distributed among their own firewalls and servers intermediaries. The firewall protects the network from external influence. It filters link layer frames, recognizes the session that opens external user. Intermediary server controls and limits the output of internal user outside, and often his representative.

Features intermediary server, hiding internal addresses of stations, handing out the entire network as a computer server address; caching popular web-pages, files, so users do not have to turn to the external network. Popular information server updates automatically defined intervals.

Firewalls use different filtering algorithms, they have different degrees of protection and cost. To classify firewalls describe their work using a reference model OSI.

There are:

- Firewalls filtering packets (packet filtering firewall; operate at the data link, network levels);
- Locks the session level (circuit level gateway; working on session level, recognize the session);

- Application level gateways (application level gateway; filtered information for applications);
- Expert-level firewalls (stateful inspection farewall; perform the functions of firewalls all lower levels).

Typically, the higher the level of the firewall, the more protection it provides.

Firewall packet filtering work with hardware or software router. They analyze the content of IP-packet header and based on the information they have and their rules table and decide about the passage of the package or its rejection. Often the information for which decide to pass the package is its complete address information, information about protocol and application port numbers recipient and sender. If the package does not meet any of the rules, the rule "default". It often rejects the package. The specific configuration depends on the rules of politics. Firewalls generate small delay transmitting messages. Often filtering packets in routers integrate. However, the level of protection in such firewalls insignificant - the attacker may substitute the IP address [9].

Gateways of the session participants recognize the session. Verification procedures performed only at the beginning of the session. After the client and server authenticity is confirmed, a gateway simply copies packets without performing filtering. Gateways of the session supported operating table sessions and when the session ends, destroying an entry. Copying packages carry out a special program, called channel-mediators (pipe proxies). Gateways of the session can perform the function of an intermediary server which displays the internal LAN addresses into one (actually for firewall). For packets coming in the opposite direction, reverse operation is performed. Consequently, network address space reserved - external user sees internal addresses. However, such gateways do not provide sufficient protection and is usually not a separate product, supplying them with gateways of applications.

Penetration testing (penetration testing, pentest - tests to overcome the defense) - a detailed analysis of networks and systems in terms of a potential attacker. The essence of the test is sanctioned attempt to circumvent existing remedies complex information system. During testing plays the role of attacker specialist who must determine the level of protection, identify vulnerabilities, identify the most likely way of hacking and determine how well the detection and protection of information systems against attacks on the company. Penetration test allows you to get an objective assessment of how easily access corporate network resources and the company's website, how and through which vulnerability. Penetration test is to simulate the actions of the attacker on the entry into the information system and allows you to identify most vulnerabilities on the network. Penetration test is carried out to obtain an independent assessment of the security of their corporate networks.

The goal of penetration testing is to identify weaknesses in the protection of IP and, if possible, and corresponds to the wishes of the customer, to make a show evil.

The main objective of penetration testing, simulating the action completely attacker to carry out an attack on the Web server, application server, or database, personnel, corporate network. Penetration testing can be performed as a part of auditing for compliance, as well as independent work.

Penetration test - a method of evaluating the security of a computer system or network by partial simulation for external intruders from penetration into it (which means no authorized access to the system) and internal attackers (who have a certain level of authorized access). This process involves an active analysis of the system to identify any potential vulnerability that may result from improper system configuration, known and unknown defects of hardware and software or operational lag in procedural or technical countermeasures. This test is done from a position of a potential attacker and can involve active use of vulnerabilities.

Security problems that have been identified during the penetration test, presented to the owner of the system. Effective Penetration Test combine this information with accurate assessment of the potential impact on the organization and outline the boundaries of technical and procedural countermeasures to reduce risks.

Testing is about a variation of things in the software and its surroundings, which can be changed by varying them, and seeing how the software responds. The aim is to ensure that the software performs safely and securely at reasonable or even unreasonable production scenarios. Thus, the most fundamental is planning a test that can be done to understand what can be changed and how that change should be organized to test. In terms of safety, the environment, user input, and internal data and logic are the main places where such changes might reveal safety problems, which consist of files, applications, system resources, and other local or network resources. Any of them can be the starting point of attack. User

input that comes from outside (usually unreliable) persons analyzed and used software. Internal data and logic stored internally as well as variables and logical ways that a number of potential transfers.

Penetration test is useful for several reasons:

- determine the possibility of a particular set of attacks;
- identify vulnerabilities of highest risk resulting from the combination of lower risk vulnerabilities used in sequence.

By applying special programs correspond intermediary. They can perform filtering level applications. Each application can have its mediator. In contrast agents in the session-level gateways, intermediaries of applications analyze packets at applications. For example, the mediator can use FTP to ban the use of teams put to prohibit transfer of information to your server [7].

Firewalls expert level combine features of all previous systems. They perform packet filtering link-level gateways recognize the session as the session level and are able to analyze and filter packets on the basis of applications. Unlike firewalls of applications that actually transmit information between two transmission links dissolved client-gateway and gateway external computer and cause a significant delay in transmitting information, expert level firewalls establishing a direct link between the identified client and server. For flow filtration using custom templates, heuristic rules relative to standards other methods from the arsenal of expert systems. Firewalls expert level provide the highest level of protection and higher performance options.

Protecting the network using firewalls. The firewall is usually set between the router and the network that protects, and a computer with two network adapters. One adapter is connected to the hub so-called demilitarized network (DMZ), the other - to the hub network, which is protected. A firewall typically connect to through it passed all traffic "Internet - a network that protects". It is important to note that since access to DMZ-concentrator are just a router and firewall, all data exchange with the Internet is through the firewall [10].

The proxy service is a mediator between the host, the host service, and service and most used protocols such as FTP, Telnet. The firewall processes connection requests, meaning that it functions as a proxy service. Many proxy service allow you to use FTP or disable specific FTP-command.

Firewall software is made, check the contents of the package, perform proxy services, encryption, authentication and generate alerts. To check suspicious traffic (such as repeated attempts to connect to the network) analyzes the contents of packets with the same IP-address of the destination. Further action depends on the firewall configuration, or deny any further suspicious packages or situation reported firewall administrator.

1. Simmonds. A; Sandilands. P; van Ekert. L (2004). An Ontology for Network Security Attacks. Lecture Notes in Computer Science. Lecture Notes in Computer Science 3285. с. 317–323. doi:10.1007/978-3-540-30176-9_41. ISBN 978-3-540-23659-7.
2. Role-Based Trusted Network Provides Pervasive Security and Compliance - interview with Jayshree Ullal, senior VP of Cisco.
3. Dave Dittrich, Network monitoring/Intrusion Detection Systems (IDS), University of Washington.
4. Гайкович В. Ю. Необхідна умова їх успішного застосування / В.Ю.Гайкович, Д.В. Єршов // "Системи безпеки, зв'язку та телекомунікацій", №3, – 2007.
5. Єршов Д.В., Попова З.В. Навчання комп'ютерної безпеки / Д.В. Єршов, З.В. Попова // «КомЛог», №2, – 2007.
6. Кадыров М.М. Информационная безопасность компьютерных сетей / М.М. Кадыров, Н.О. Каримова // Молодой ученый. – 2016. – №8. – С. 124-126.
7. Лукацький А.В. Нові підходи до забезпечення інформаційної безпеки мережі / А.В. Лукацький // Комп'ютер-Прес. – № 7. – 2007.
8. Лукацький А.В . Адаптивна безпеку. Данина моді чи усвідомлена необхідність / А.В. Лукацький // PCWeek, – №37. – 2009.
9. Лукацький А.В. Сімейство засобів адаптивного управління безпекою / А.В. Лукацький // «Мережі», – № 10. – 2008.
10. Новіков С.М. Захист інформації в мережах зв'язку з гарантованою якістю обслуговування. / С.М.Новіков // Новосибірськ. – 2003. – С.18-31.