ISSN: 2350-0328

International Journal of AdvancedResearch in Science, Engineering and Technology

Vol. 6, Issue 2, February 2019

Problems of Security of Info communication Systems

Kadirov Mirhusan Mirpulatovich, Yuldasheva Masuda Toxtasinovna, Akbarova Shohida Azatovna

Assistant professor, Department of Information Technologies, Tashkent State Technical University, Tashkent, Uzbekistan.

Senior Lecturer, Department of Information Technologies, Tashkent State Technical University, Tashkent, Uzbekistan.

Senior Lecturer Department of Information Technologies, Tashkent State Technical University, Tashkent, Uzbekistan.

ABSTRACT: The article is devoted to the problems of security of information and communication systems, features of the use of information protection methods, analysis of threats and information security risks as well as means of improving information security. Considered the main ways to protect information.

KEYWORDS: threat, unauthorized access, attacks, information leakage, information security methods, access control, disguise.

I. INTRODUCTION

In connection with the “multi-user” mode of operation in a computer network, a whole set of interrelated questions arise regarding the protection of information stored in computers or servers of a computer network. It should be noted that the network operating systems themselves also provide powerful means of protection against unauthorized access to network resources. However, there are cases when even such protection does not work. Practice shows that an unauthorized user who has sufficient experience in the field of system and network programming, who has set himself the goal of connecting to the network, even with limited access to individual resources, sooner or later can still gain access to some protected network resources.

II. INFORMATION PROTECTION METHODS

The main type of information threats, against which a whole technology is created at every enterprise, is unauthorized access of intruders to the data. Malefactors plan in advance criminal actions which can be carried out by direct access to devices or by remote attack with use of the programs which are specially developed for theft of information [1].

Information leakage is considered as uncontrolled and unlawful exit of confidential information outside the organization or a circle of persons to whom this information was entrusted.

There are three types of threats.

1. The threat of breach of confidentiality is that information becomes known to someone who does not have access to it.

2. The threat of violation of integrity includes any intentional change of information stored in a computer system or transmitted from one system to another. When the attackers intentionally change the information, then the integrity of the information will be violated. Integrity will also be compromised if an unauthorized change is caused by a random software or hardware error. Authorized changes are those that are made by authorized persons for a reasonable purpose (for example, the authorized change is the periodic scheduled correction of a certain database).

3. The threat of service failure occurs every time when, as a result of deliberate actions taken by another user or an attacker, access to a certain computing system resource is blocked. In reality, blocking can be permanent - the requested resource will never be received, or it can only cause a delay in the requested resource, long enough for it to become useless.

Data protection technologies are based on the use of modern methods that prevent information leakage and its loss. Fig.1.1 shows six basic ways to protect information.

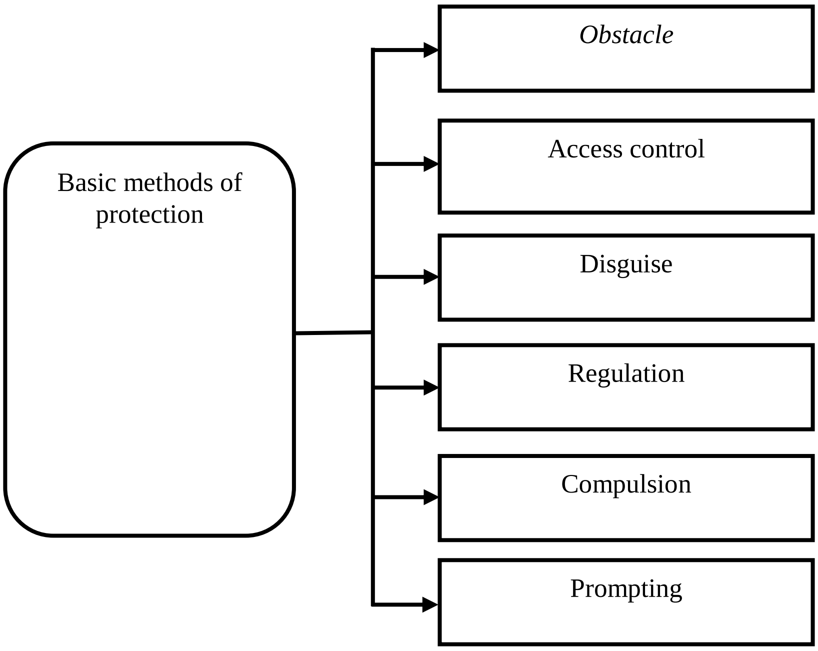

Fig. 1.1 Basic methods of protecting information

Obstacle - a method of physically blocking the path of an attacker to protected information.

Access control - ways to protect information under which control is exercised over all components of an information system.

Disguise - information security methods that involve the conversion of data into a form that is not suitable for perception by unauthorized persons. Decryption requires knowledge of the principle.

Regulation is the most important method of protecting information systems, which implies the introduction of special instructions, according to which all manipulations with protected data should be carried out.

Compulsion- methods of protecting information that are closely related to the regulations, implying the introduction of a set of measures in which employees are forced to follow established rules.

Promptingis a method of protecting information that encourages users and system personnel not to violate established rules by complying with established moral and ethical standards.

Ways to protect information involve the use of a specific set of tools. To prevent the loss and leakage of sensitive information, the following means are used:

- physical;
- software and hardware;
- organizational;
- legislative;
- psychological.

Physical protection means are intended for external protection of the territory of objects, protection of components of an automated information system of an enterprise and are implemented in the form of autonomous devices and systems.

Software and hardware - an indispensable component for ensuring the security of information systems. Hardware is represented by devices that are embedded in the equipment for information processing. Software - programs that reflect hacker attacks. Also to the software can include software systems that perform the recovery of lost information.

Organizational means provide measures that make it impossible or difficult to disclose, leak, unauthorized access to information on a regulatory basis.

Legislative means - a set of legal acts regulating the activities of people who have access to protected information and determine the extent of responsibility for the loss or theft of classified information.

Psychological means - a set of measures to create the personal interest of employees in the preservation and authenticity of information.

The question of protecting information from external influences is now in first place in terms of urgency. The cases of theft of intellectual property, industrial espionage, unauthorized access to personal data and strategically important information resources of organizations are becoming more frequent and more and more serious and threatening.

III. ANALYSIS OF MEANS OF INCREASING INFORMATION SECURITY

In fig. 1.2 shows the scheme of information security tools that can be used to collect statistical information about what is happening in computer networks. They are presented according to the degree of increase in the prevalence of the hardware component over the software component [2].

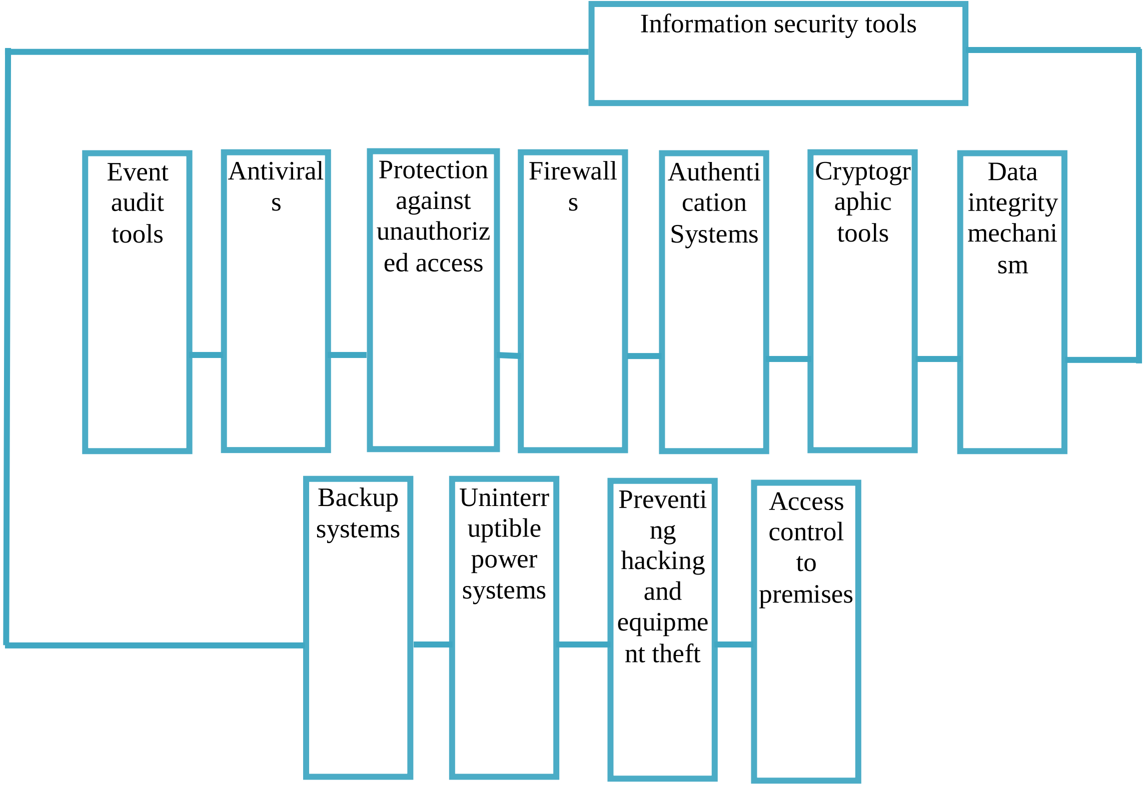
Information security tools
Event audit tools
Antivirals
Protection against unauthorized access
Firewalls
Authentication Systems
Cryptographic tools
Data integrity mechanism
Backup systems
Uninterruptible power systems
Preventing hacking and equipment theft
Access control to premises

Fig. 1.2. The scheme of information security tools used for the statistics of emergency situations in computer networks

Protection of confidential and valuable information processed in computer networks from unauthorized access is one of the most important tasks of information protection [3].

Consider the functioning of security monitoring systems:

1) The probability of a correct intrusion detection by a security monitoring system

$$P = 1 - \max\{1 - P_I, P_{II}\}, \qquad (1)$$

where P_I and P_{II} the probabilities of errors of the first and second kind, respectively.

2) Redundant configuration of the information security system:

$$K_1 = \frac{m_1 - n_1}{n_1} \quad u \quad K_2 = \frac{m_2}{n_2} \qquad (2)$$

where K_1, K_2 - redundancy coefficients; m_1 - number of protection mechanisms; m_2 - number of security monitoring system agents; n_1 - minimum required number of protectors to ensure a given level of security, while $m_1 > n_1$; n_2 – amount of information resources.

3) Estimates of costs required for the implementation of safety monitoring systems.

Table 1. Performance indicators of security monitoring systems.

№	Name	Probability of correct detection*	Configuration redundancy**	Cost estimates ***
1	RealSecure	0.89	0,71	130
2	Open View	0.90	0,56	140
3	Tivoli	0.88	0,62	140
4	Enterprise Security	0.90	0,59	150

* - according to information from manufacturers websites and independent tests

** κ_1 - according to information from manufacturers websites

*** - c.u./mon for protection of one resource (including cost of support and payment of the security administrator)

Based on a comparison of safety monitoring tools, the following common weaknesses are highlighted:

- a high level of errors of the first and second kind, because forming an assessment of the likelihood of intruders in the CN does not take into account the prediction of their behavior;
- priorities of reaction to security events are set statically, which does not allow adaptive control of the security system of the CN.

IV. CURRENTINFORMATION SECURITY THREATS

Actual threats to information security are considered, based on the results of numerous investigations, as well as data from authoritative sources.

According to the company Positive Technologies, in the second quarter of 2018, the share of attacks aimed at obtaining data continued to grow [4]. In 40% of cyber incidents, attackers were aimed at obtaining information, and in 39% - for financial gain. The credentials may be sold, so after the attack, in which the information was received, a new one may soon follow - on the owners of this data or on the company, the credentials of whose employees were compromised. Figure 1.3 shows a diagram of the intruders motives.

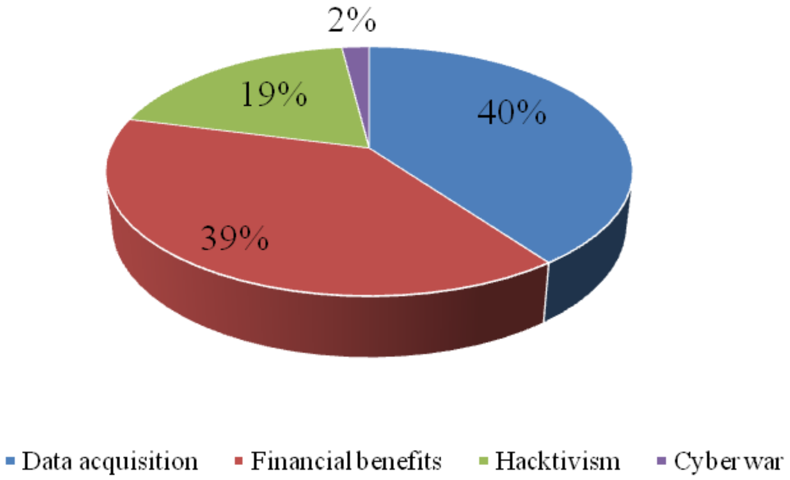

Fig.1.3. The motives of intruders

Considered what information most attracted criminals in the second quarter of 2018. In half of the cases, it was personal data (30%) or user accounts and password information for access to various services and systems (22%), including private online banks. In 15% of cases, the data of payment cards were stolen, their attackers were most often obtained through spyware malware or from compromised sites.

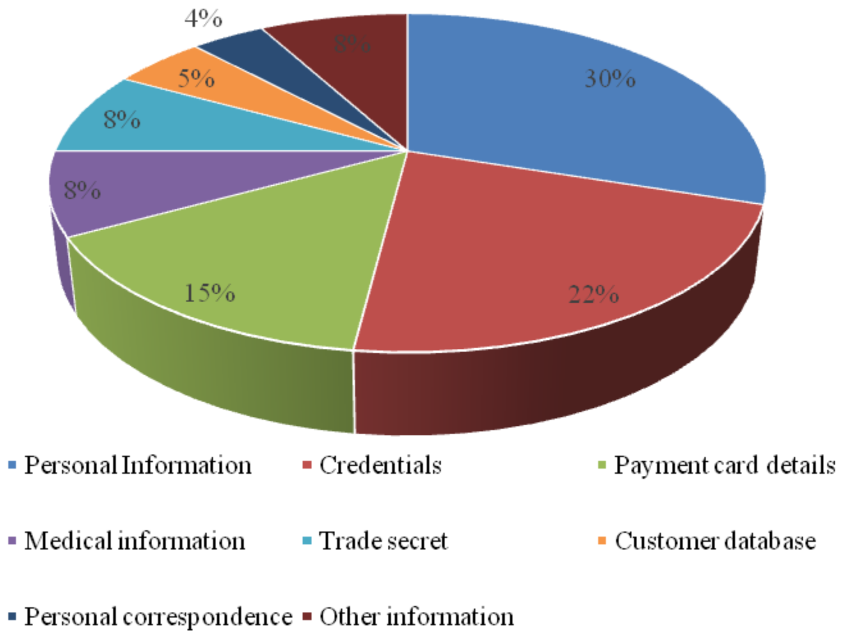

Fig.1.4. Types of stolen data

A large number of targeted attacks on various organizations, and the proportion of targeted attacks exceeded the mass share and amounted to 54%.

Large-scale cyber attacks, mainly harmful epidemics, which are not limited to the impact on any one industry. The share of attacks aimed at infrastructure in the II quarter of 2018 was 44%, the share of attacks on web resources increased compared to the same period last year and amounted to 32% against 23%. In addition, compared to Q1, the share of attacks on IoT devices has increased: this is mainly due to the emergence of new botnets, such as PyRoMineIoT, Muhstik, Wicked Mirai.

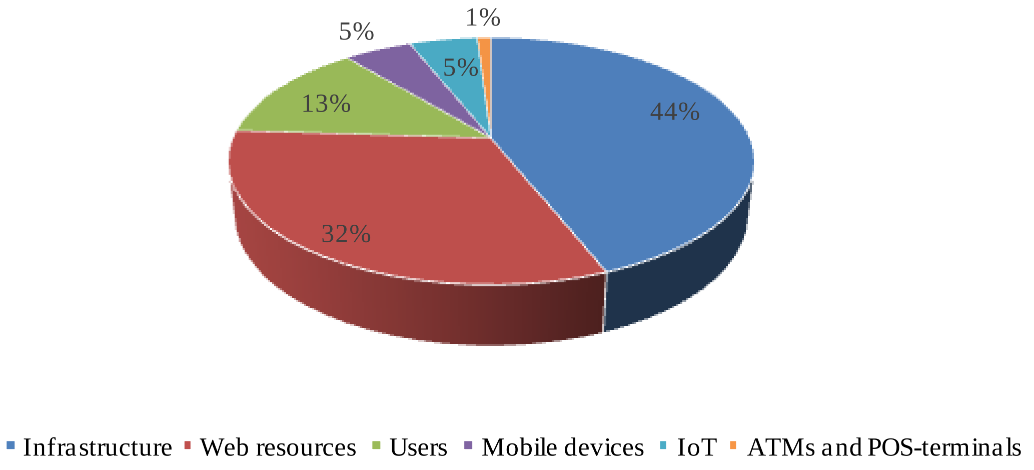

Fig. 1.5 Attack Objects

In the second quarter of 2018, the proportion of attacks in which attackers used malware decreased (49% instead of 63% in the first quarter). The share of attacks in which credentials were picked up increased by 12% compared with the first quarter of this year.

V. CONCLUSION AND FUTURE WORK

Principles of creating secure systems. Based on the analysis performed, it can be concluded that the creation of secure systems should include the following principles:

1. The principle of integration - means of protection should be built into the system so that all the interaction mechanisms without exception are under their control.

2. The principle of invariance - means of protection should not depend on the characteristics of the implementation of applications and should not take into account the logic of their functioning, on the contrary, they should be universal for all types of interactions and display them on the relationship between subjects and objects.

3. The principle of unification - there must be an unambiguous correspondence between controlled interactions of subjects and objects and access operations, the management of which is described by security models. This allows us to give versatility to protection tools and use them without modification, both for the implementation of various security models and for controlling access to objects of different nature.

4. The principle of adequacy - to ensure the real ability to resist attacks, it is necessary to eliminate the sources of vulnerabilities, on the use of which all mechanisms for the implementation of attacks are based.

5. The principle of correctness - the means of protection must implement access control in accordance with formal models. The presence of a consistent security model allows you to formally justify the security of the system, provides an objective criterion for the correctness of its operation, and can also serve as the basis for building exhaustive tests that verify the correctness of the operation of protective equipment for all situations.

Based on the analysis of the methods and technology of information protection, it was found that the construction of effective means of protection against unauthorized access requires the development and improvement of methods and models of access control in computer networks.

This work on the subject of the grant ЁОТ-Атех-2018-168“Improving methods and means of detecting attacks in computer networks”.

REFERENCES

[1] Домарев В.В. Безопасность информационных технологий. Методология создания систем защиты. -К.: «ДС», 2001. - 688 с.

[2] Mukhin V.E., Volokita A.N. Integrated security monitoring system based on the analysis of the objectives of the actions of subjects of computer systems and networks. // Control systems and machines. №5, 2006, -p.85-94.

[3] Kadirov M.M., Tojikhujaeva N. Z., Kasimova G. I.Classification of Modern Security Monitoring Systems in Computer Systems and Networks. International Journal of Advanced Research in Science, Engineering and Technology, Vol. 5, Issue 9, India 2018, P. 6764-6769.

[4] https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2018-q2.