Scientific and Practical Cyber Security Journal (SPCSJ) 3(1): 6-11 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)

DEVELOPMENT OF AN AUTOMATED SYSTEM INTRUDER MODEL

Mykola Brailovskyi Taras Shevchenko National University of Kiev, PhD in Engineering Science, Associate Professor. Kiev, Ukraine.
Volodymyr Khoroshko National Aviation University, Doctor of Engineering Science, Full Professor. Kiev, Ukraine

ABSTRACT. The model of the security penetrator of the automated system is developed, on the basis of the use of a 4-level gradation of access to information

KEYWORDS: penetrator, information security system, penetrator model, set of threats.

Any information is considered as the form of streams acting on sense bodies of an operator by the forms of image, communication and text, which leads to the generation of flows in corresponding forms. Modern information technologies sublimate the features of all forms, and various current forms can be transformed between themselves.

Thus, the main stage in the construction of the information security system is the analysis of information threats and the use of measures to reduce or eliminate them. However, not enough attention is paid to the development of the model and the analysis of penetrators, without which it is impossible to carry out a qualitative analysis of threats, because it describes the possibility of a penetrator concerning the violation of information security.

The need to classify threats to information security is due to the fact that the architecture of modern means of automated information processing, organizational, structural and functional construction of information and computing systems and networks, technology and processing conditions are such that information is a subject to excessive overflow of factors on which it is necessary to formalize the description task and threats as well as effective counteraction to them. The list of threats to information security [1,2] will be considered by the target sign of the classification and description of components of information flows critical to modification. The analysis of these threats should be carried out on the basis of their qualifications by a number of assessments. Each rating reflects one of the generalized requirements for the system of protection (confidentiality, integrity, availability): unauthorized copying of information carriers; careless actions leading to the disclosure of confidential information or make it publicly available; ignoring organizational constraints (setting rules) when determining the rank of the system.

According to information systems, we will consider the following types of threats:

- the threat of privacy breach is that the information becomes known to those who do not have the authority to access it;
- the threat of integrity breach includes the notion of any deliberate change in information stored in the system or when it is transmitted between systems;
- the threat of service failure occurs every time when access to some resources is blocked as a result of intentional actions;
- the threat of disclosure of the security of the information system.

When considering the protection of automated information systems, it is expedient to use a 4-level gradation of access to information stored, processed and transmitted by the system: the level of information carriers; level of interaction with carriers; level of information provision; level of information security.

In addition, additional requirements for the analysis of information threats need to be formulated: the list of existing threats should be as complete and detailed as possible. For each of the threats it is necessary to determine in violation of which properties of the information or information system it is directed (confidentiality, integrity, availability, as well as failure of the services of the system); Possible methods of realizing threats [3].

Proceeding from the technology of information processing and constructing a model of information threats, it is necessary to develop a penetrator model that should be adequate to the actual penetrator for the given information system.

Relative to the automated information system, penetrators can be external or internal. The penetrator model should determine: the possible purpose of the penetrator and its gradation according to the degree of danger for the system; categories of persons who may be the penetrator; prediction of the penetrator's qualification; prediction of the nature of his actions.

Therefore, the correct constructed model of the penetrator suggests that it reflects its practical and theoretical capabilities, a priori knowledge, time and place of action, etc. The model should be constantly adjusted in the light of obtaining new knowledge about the possibilities of the penetrator and changes in the system of protection of the system and the system on the basis of analysis of the causes of violations that have occurred, which will affect the exact reasons, as well as more precisely determine the requirements for the system of protection against this type of violation [3].

In order for the model of the penetrator to be of maximum benefit, it must be created for a specific object of protection and can not be universal, take into account the motives and socio-psychological aspects of the violation, the potential opportunities for access to information resources of various categories of external and internal penetrators to various spatial-temporal sections of the object of protection.

Determining the specific characteristics of probable penetrators is largely subjective, so the model of the penetrator, which is built on the specific features of a particular subject area and technology of information processing, can be represented by the listing of several variants of the penetrator's appearance.

A penetrator is a subject that mistakenly or deliberately attempts to perform prohibited operations and uses various opportunities, means and methods for doing so. Each penetrator for the realization of his intentions is guided by a certain motivation and intentions, possesses a set of knowledge, skills and methods of committing unlawful actions with the use of appropriate technical means. Only a set of knowledge about all characteristics of the penetrator will adequately respond to possible threats and choose the appropriate means of protection.

In addition, the actual capabilities of the penetrator are largely determined by the state of the object of protection, the availability of potential channels of information leakage, the quality of information security. The reliability of the information security system depends on the penetrator, because in order to achieve his goals the penetrator must make some effort, spend resources. As a penetrator, an entity that has access to an object with regular means of information and communication systems is considered. It is believed that in its field the penetrator is a specialist in higher qualification, knows everything about information and communication systems and means of their protection.

But skills and abilities can be realized subject to staying in certain premises of the facility, from which it is possible to realize the threat. Therefore, in addition to the level of knowledge of the penetrator, his qualifications, preparedness for the implementation of his plans, to form the most complete model of the penetrator, it is necessary to determine the category of persons to which the penetrator may belong.

When forming a penetrator model, it is necessary to differentiate all employees not only from their ability to access the system, but also for possible losses from the actions of the personnel, that is, for potential losses from each category of employees, from system administrators to ordinary users and even cleaners. Also, we cannot forget about such a category as external penetrators (competitors, customers, etc.).

Thus, each user according to his category, that is, level of professional knowledge and access to information resources of the system, can cause more or less damage to the object of

protection by accessing specific elements of the information processing system. Additionally, there might be some interesting information about what kind of threat an intruder may realize: stealing, copying, modifying, destroying, disclosing information, blocking access to it, etc.

Such a system of categorizing staff at risk should not be perceived as a dogma. In each individual case, a separate system of categorization and comparison with a variety of threats is created, which helps in the creation and simulation of the information security system.

The model of the penetrator must be specified and expanded to clarify the possible scenario of violations. To this end, each category of probable penetrators should be analyzed separately for the following parameters:

1) technical equipment and methods and means used for the violation:

- only staffing and shortcomings of the information security system to overcome it (unauthorized actions with the use of permissible means);
- passive means (means of interception without modification of components of the information system);
- methods and means of active influence (modification and connection of additional technical means, connection to data channels, introduction of software bookmarks and use of special tool and technology programs).

2) Level of qualification and range of knowledge of the penetrator.

3) Possibility of access of the penetrator to specific resources of the information system - probable places (through the networks of the control zone of the information system, but without access to the allocated space, in the middle of the allocated premises, but without access to technical means of the information system, with access to technical means of the information system and from the workers places of users; access to the data area) and time (in the process of functioning of the information system; during scheduled breaks in the system; in non-working hours; during system repairs) for accomplished illegal actions. Taking into account the place and time of the penetrator's actions also allows to specify its possibilities for access to information resources and take them into account in order to improve the quality of the information security system [4].

4) The set of threats and internal vulnerabilities of the information security system.

The algorithm for constructing a penetrator model (Fig. 1) at the output should determine the probability of realization of threats and timeliness of detection of unauthorized intrusion.

Any high-quality anti-a priori system provides high expertise (high level knowledge in the field of computer technology, programming, designing and operation of information systems, possession of information on the functions and mechanisms of action of remedies) and the qualifications of the penetrator (the possibility of using the design flaws of a comprehensive information security system with the help of methods and means of active influence on the information system that change the configuration of the system).

It is also anticipated that at the place of action penetrators can gain access to the means of administration of the automatic system and the means of management of an integrated security system.

The action of the data registration model is not the level of file authentication.

The first condition for the functioning of the model is the autonomy of the control of the integrity and availability of information (independence from the actions of the system administrator).

The second condition is the mandatory use of algorithms for monitoring the integrity and availability of each element of the flow.

The third condition is the compactness of the means of the system for monitoring the integrity and availability of information (the use of minimal computing resources).

Condition fourth - response to intervention (complex of organizational tools to violate the integrity of the object).

In addition, the creation of a mechanism for the effective protection of restricted access information presupposes, first of all, that there is a standard system consisting of an object of attack and a subject who tries to use information in contravention of the established standards of treatment.

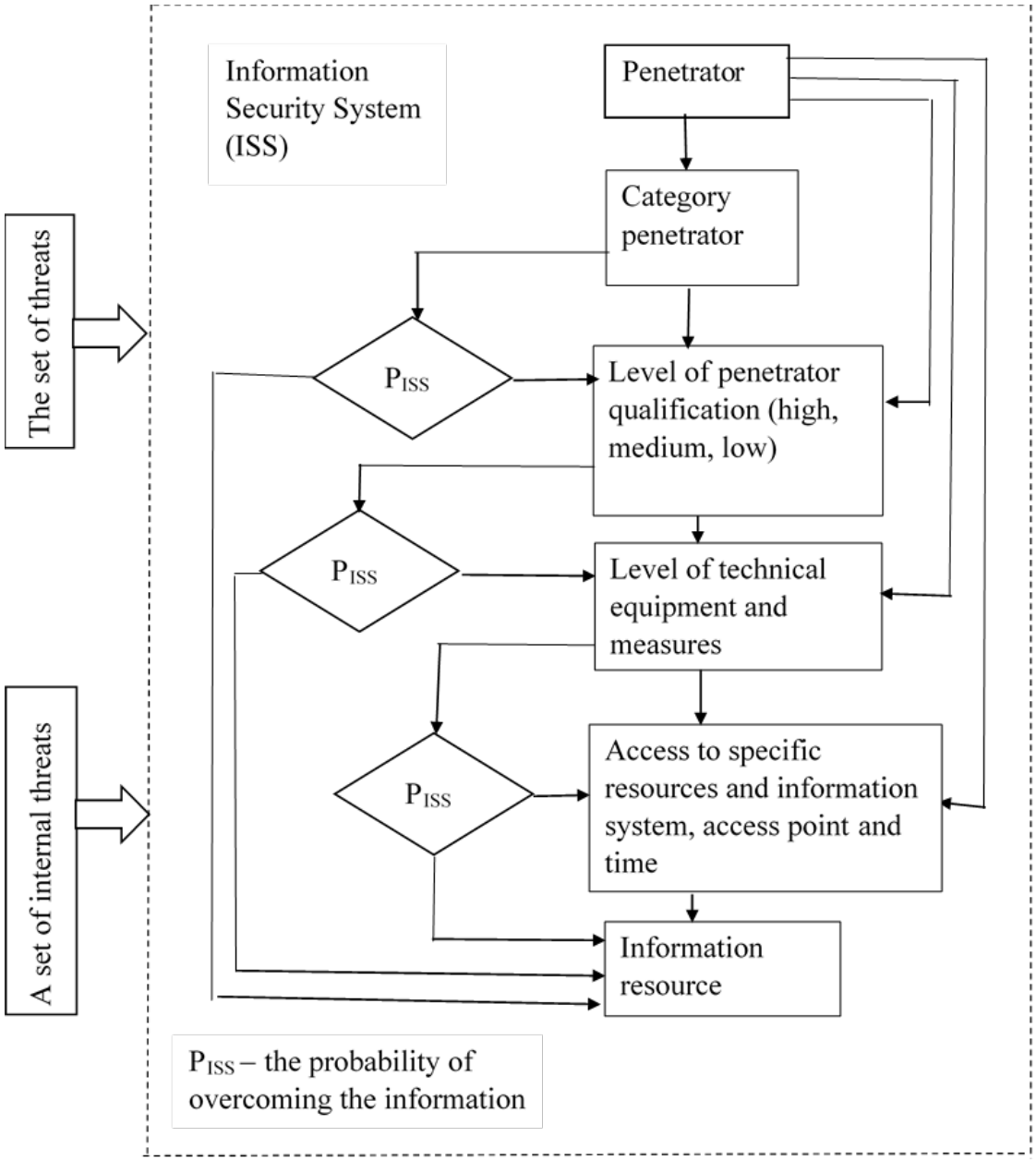

Fig. 1 Algorithm for constructing a penetrator model

Controlled information flow will mainly be transmitted openly (for immediate further processing) with the subsequent mandatory processing of the system control of the integrity and availability of information. In the presence of such a functional mechanism in the event of an attack on the information transmitted, timely detection of this fact will provide additional opportunities for preventing the further development of negative events. In this case, the algorithm of maintaining the integrity and availability of information is based on the principles of hashing data stream segments [5].

A one-way hash function H (N) handles an arbitrary length length message Ni returns a hash of a fixed length h:

$$h = H(N),$$

where h is the length n.

Many functions can take the input of the appropriate length and return the output of a fixed length, but one-way hash functions have three additional characteristics:

- by N it is easy to calculate h;
- for h it is difficult to calculate N so that H (N) = h;
- it is difficult to find another N 'such that H (N) = H (N') is difficult to find.

The hash length can be changed by the user. The proposed method involves the generation of a longer hash than this function of its output.

Based on the study, the following conclusions may be drawn. Consideration of the existence of information allows you to highlight the following features of the information model of data registration.

Information transmission in telecommunication networks takes place in the form of information flows, the classification of which depends on their perception by the user and is characterized by the internal structure of the flow format. Information in modern automated systems in many cases is prone to unauthorized modification. The most vulnerable of the main stages of the information lifecycle is the stage of its distribution among correspondents of the network.

The penetrator model is an important component for a qualitative analysis of threats and the definition of requirements for the composition and characteristics of the protection system. It should be constantly changed and adjusted to take into account the emergence of new data on the capabilities of the penetrator and changes in the protection system. In addition, the penetrator model can be presented in several variants, because the existence of a set of models of the penetrator will allow to predict the probability of penetration into the system and build a reliable information security system using modern intelligence support to control both the security system and the system for monitoring the integrity and reliability of information.

When considering the protection of automated systems, it is expedient to use a 4-level gradation of access to information stored, processed and protected in an automated system: the level of information carriers, the level of presentation of information, the level of means of interaction with carriers, the level of presentation of information and the level of information content.

REFERENCES

[1] Lenkov S.V., Peregudov D.A., Khoroshko V.A. Methods and means of information protection. In 2 volumes – K: Arii, 2008 (in Russian)

[2] Koboseva A.A., Machalin I.O., Khoroshko V.O. Analysis of the security of information systems. - K .: View. DUIKT 2010 - 316 p. (in Ukrainian)

[3] Buryachok V.L., Grishchuk R.V., Khoroshko V.O. Information Security Policy. - K .: PVP "Zadruga", 2014 - 222 p. (in Ukrainian)

[4] Brailovskyi N.N., Orlenko V.S., Khoroshko V.A. Assessment of the quality of the information security system functioning // Modern information security, #4, 2010. - p. 9-15. (in Russian)

[5] Brailovskyi N.N., Orlenko V.S., Khoroshko V.A. Formation of complex programs for the protection of objects in the presence of threats and risks // Modern information security, № 1, 2011. - p.34-41. (in Russian)