Scientific and Practical Cyber Security Journal (SPCSJ) 1(1):32-37

Scientific Cyber Security Association (SCSA), 2017 ISSN: 2587-4667

MATHEMATICAL MODEL OF EVALUATION OF INFORMATION AND TELECOMMUNICATION SYSTEMS SECURITY

V. Vialkova, Y. Shestak

Taras Shevchenko National University of Kyiv

ABSTRACT

Mathematical model for assessing the security of the information and telecommunications system proposed and the most common vulnerability considered in this article.

KEYWORDS*:* information security, information and telecommunications system

The fourth information revolution that began with the invention of the personal computer, allowed access to a huge number of the accumulated knowledge of mankind, and greatly accelerated the development of new areas and allowed us to share huge amounts of information over large distances using the network. The first network consisted of only few nodes, and it couldn't connect to anyone. Eventually, when computers became more accessible, the network also expanded, resulting in a worldwide network – the Internet.

Modern information networks transmit a variety of information, allowing to keep the businesses, providing access to entertainment, communication and much more – everything that can be digitized and transmitted as information. All of this information has value, therefore, it needs to be protected from theft, deliberate damage, destruction or any other action.

However, due to the huge size of existing information and telecommunication systems the complete security ensuring is not possible. Modern ITS are organized by many different hardware, with different characteristics, and they also are controlled by different software. This diversity leads to the fact that it is not possible to guarantee absolute security of data transfer in such complex ITS.

However, you must regularly evaluate the security of ITS that will increase its safety by identifying and eliminating the unreliable components of the system, and plan for network development.

Currently, there are a lot of documents that define the safety assessment of ITS and the implementation of the functions of their protection. They are international ISO standard [1-3], and adopted in the state regulatory legal acts, standards, regulations [4-8]. In Ukraine the State service of special communication and information protection is the regulator of such documents at the legislative level.

There are also a lot of works in which the issue of computer intrusions modelling and the justification of the security metrics are described.

Many different information security tools have already been developed. They are about to be implemented at different stages of their transmission in various ways. Despite their diversity and the principle of operation, it is necessary to use the tool, which allows to calculate the parameters of the security network and the probability of attacks reflection of various means at the time [4].

BUILDING OF MODEL

Let’s present the reliability of the protection system of individual session *pi* as the ratio of reflected attacks to their total number:

$$p_i = \frac{N_{отраж}}{N_{общ}} \tag{1}$$

In this case, the probability of breaking the entire network can be represented as:

$$p_c = 1 - p_1 \cdot p_2 \cdot \ldots \cdot p_{i.} \tag{2}$$

Now let’s change the equation taking into account active defense against attacks, instead of the standard value of probability of hacking the system, we get the probability of breaking the system with the fact that during that time, as it will go, it will be overloaded.

$$p = 1 - p_0 = 1 - exp\{-t \cdot \lambda\}, \tag{3}$$

where p_0 – the probability of the absence of effects at a certain period of time,
t – the average time of use of the resource.
We get:

$$p_c = 1 - (1 - p_1) \cdot (1 - p_2) \cdot \ldots \cdot (1 - p_{i.}). \tag{4}$$

Let’s represent the violation of the integrity of information in the form:

$$P = p_j \cdot \lfloor 1 - (1 - p_i) \cdot (1 - p_m) \cdot (1 - p_n)], \tag{5}$$

where p_j – control and recovery, p_i – violations of confidentiality, p_m – impact on information in a telecommunications network, p_n – integrity from threats in a telecommunication network. Here is a complex quantity expressing the probability of security information on the system which can be expressed as:

$$P = 1 - (1 - P_i) \cdot (1 - P_j) \cdot (1 - P_n), \tag{6}$$

where P_i – the probability of violation of integrity, P_j – the probability of breach of confidentiality, P_n – the probability of breaches of service availability.

The efficiency of neutralization of multiple threats U with the declared protection measures in the system can be represented as follows:

$$\sum_{j=1}^{m} \sum_{i=1}^{n} d(i,j) p(i,j) \Rightarrow \max \tag{7}$$

Taking into consideration the limitation of costs C:

$$\sum_{i=1}^{n} c(i) * sign \sum_{j \in U}^{n} p(i,j) \leq C \tag{8}$$

$p(i,j) \in (1{,}0); \quad j = 1, \ldots m; \quad i = 1, \ldots n$

If to describe the costs of the neutralization of multiple information threats while limiting the level of effectiveness we’ll get:

$$\sum_{i=1}^{n} c_i * sign \sum_{j=1}^{m} p(i,j) \Rightarrow \min \tag{9}$$

$$\sum_{j=1}^{m} \sum_{i=1}^{n} d(i,j) p(i,j) / \sum_{i=1}^{n} (\max_j d(i,j)) \leq P$$

$$p(i,j) \in (1{,}0); \quad j = 1, \ldots m; \quad i = 1, \ldots n$$

It is assumed that the highest level of efficiency will be when the remedy with maximum efficiency will be the selected to neutralize each threat. The highest level of effectiveness is equal to the sum of the maximum elements in each column of the matrix d(i,j).

Let's consider the method of ITS protection assessment based on attack trees by expanding it to three stages.

In the first preparatory stage let's analyze each node of ITS software, search vulnerable software and run the analysis using separate vulnerabilities from the dictionary and templates. The obtained information is used for the primary building attack trees, each element of which is a vector.

$$M = \langle S, S_0, G, \pi \rangle \tag{10}$$

Element of attack model depends on many network states S, initial state of the network S_0, many parameters G, which determine the percentage of achievement by the violator of his goals and a set of transitions between States π=S·S, which can identify his attacking actions.

Each node of the tree specifies possible actions. They are connected in the order of their possible run to a specific attacker.

The route of attack is also the part of the tree, which is a sequence of states of ITS (S_0, S_1, …, S_n), and (Si, Si+1) $\in \pi \; \forall$ i $\in$ [5].

To calculate the weakness of the host the following form is used:

$$C(s) = \sum_{i=1}^{n} \max(0, S(w_i) - 60) / n \tag{11}$$

where s – ITS node, $S(w_i)$ – the rating for the weak w i the node place s, n – the number of nodes of ITS with the rating of S over 60.

In general, we can provide the IS protection in the form of two blocks – perimeter and internal IS. Naturally, with large and complex architectures of IS it is impossible to ensure its complete safety regardless the resources allocated. To identify the most vulnerable components of the IS and to implement preventive measures of analysis of security, such as penetration testing, are used. Statistical analysis of vulnerabilities.

Statistical analysis is also relevant in determining the risks in complex ITS. It does not indicate particular vulnerability, but allows to assess the scope of risks in general [6]. So according to statistics it is possible to highlight the most common vulnerabilities at the network perimeter:

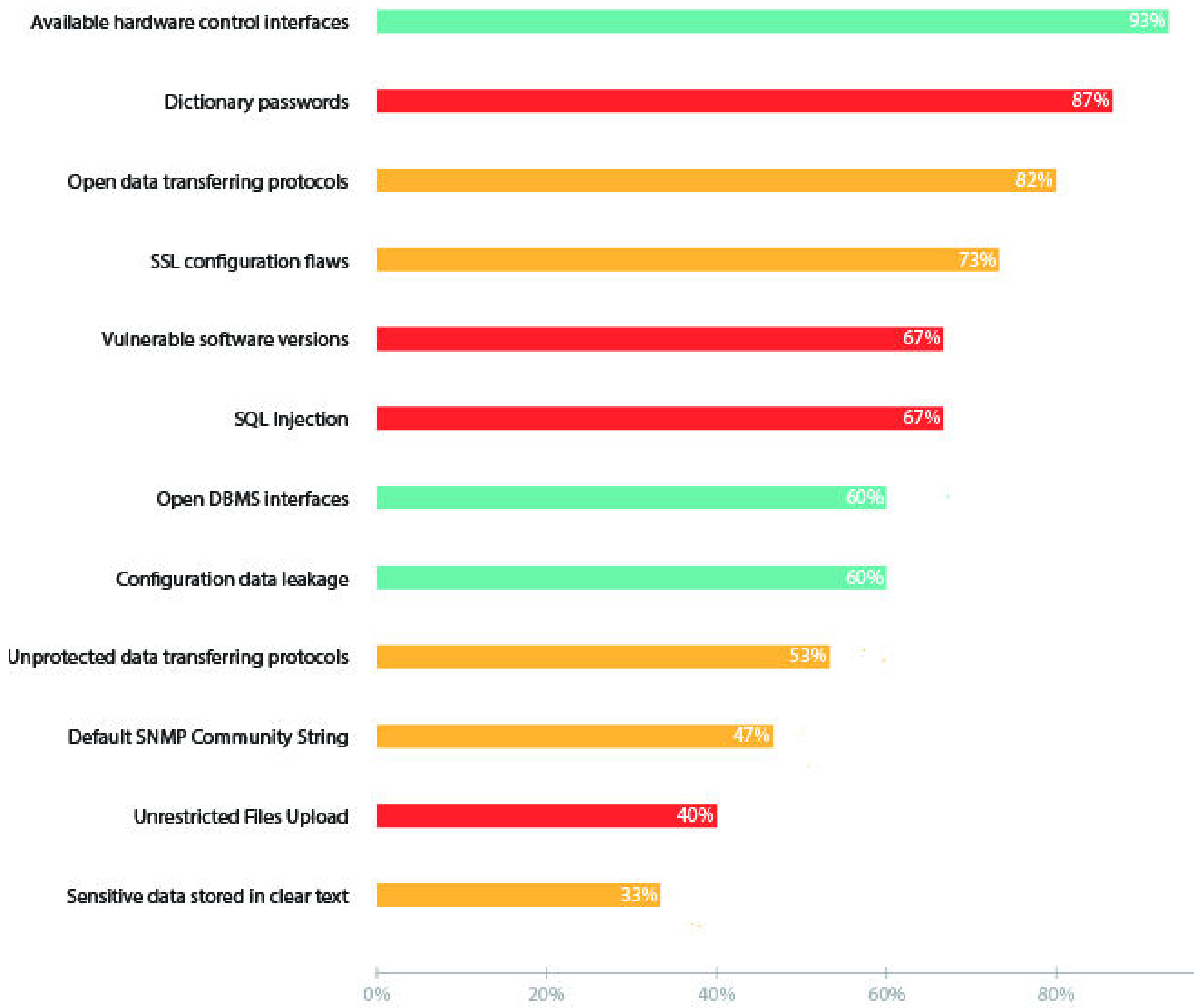

Fig.1. – Main vulnerabilities at the network perimeter

Based on the presented graph we can say that in most cases the vulnerability results in cases from neglecting to implementation the basic regulations, a little less often – inadequate level of competence.

For example, among the absolute leaders of the passwords are the passwords of the “admin”, “123456” and etc, passwords of multiple consecutive characters such as “qwerty” and some common words like “DEFAULT”, “password”, etc.

Similarly, using data statistics the most frequently used protocols can be identified, and consequently, the most likely target for penetration (Fig.2)

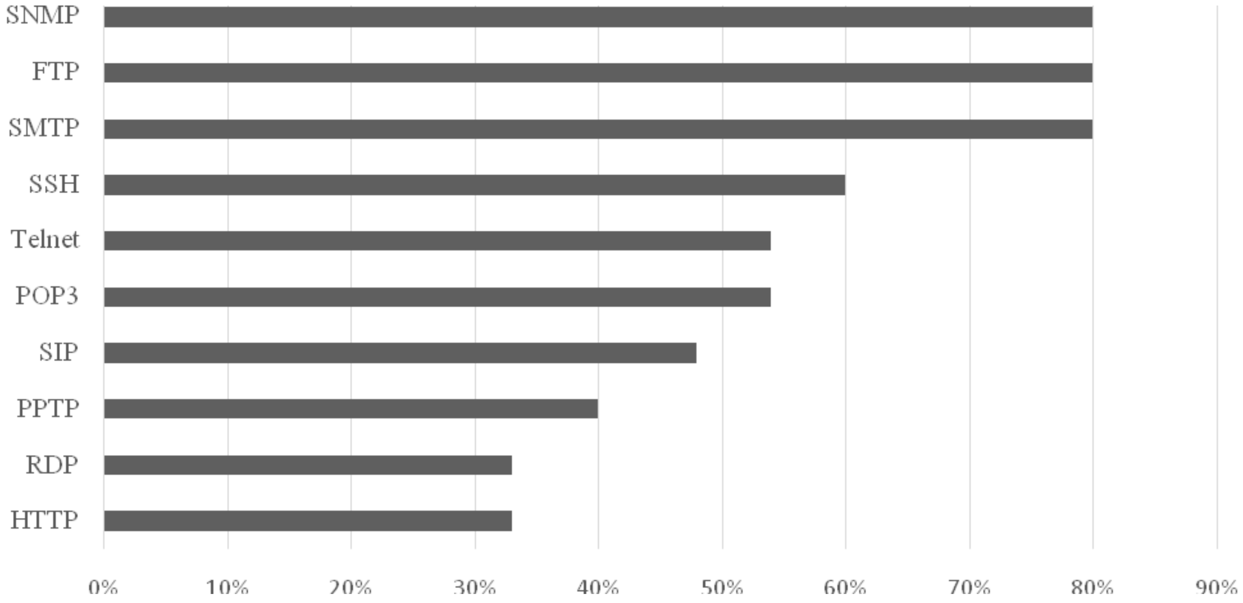

Fig.2. Statistics on the use of protocols at the network perimeter.

It is also important to assess the security of the internal network and as in the case with the network perimeter, to take the necessary measures for its protection. Usually the weak points are the wrong policy of privileges, storage of sensitive data in the public domain, inadequate anti-virus protection and weak password protection, including privileged users. In 3rd and 4th cases of penetration because of the disadvantages mentioned above it is not possible to have a complete control over the IS, as a result, receiving the maximum privileges by an attacker to critical IS [7,8].

Conclusions

The main goal of any information security system is to build such a security model where on the one hand the information assets will reach maximum protection as well as information from abuse by third parties, loss of information in result of the actions of third parties, or other actions that may lead to the malfunctioning of information systems or the loss/theft of information. On the other hand, it will be possible to maximize the quality of provided services and guarantees of security of property rights and interests of clients.

REFERENCES

1. Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model. – ISO/IEC 15408-1.1999.
2. Information technology – Security techniques – Evaluation criteria for IT security – Part 2: Security functional requirements. – ISO/IEC 15408-2.1999.
3. Information technology – Security techniques – Evaluation criteria for IT security – Part 3: Security assurance requirements. – ISO/IEC 15408-3.1999.
4. Oficial website TPI) [Online]. Available: http://www.caine-live.net/
5. TDP 2.7-011-2012. Criteria for assessing the security in computer systems from unauthorized access. State Service of Special Communications and Information Protection of Ukraine, 2012.

6. 19. Gorodetski V., Karsayev O., Kotenko I., Samoilov V. Multi-Agent Information Fusion: Methodology, Architecture and Software Tool for Learning of Object and Situation Assessment // The 7th International Conference on Information Fusion. Proceedings. Stockholm, Sweden. June 28 – July 1, 2004
7. Kotenko I.V. Perspective directions of research in the field of computer security / I.V. Kotenko, R.M. Yusupov // Data protection INSIDE № 2’2006. P-50-54.
8. Abramov E.S. Application of attack graphs for modeling of malicious network impacts / E.C. Abramov. [Online]. Available: https://cyberleninka.ru/article/n/primenenie-grafov-atak-dlya-modelirovaniya-vredonosnyh-setevyh-vozdeystviy.