ANALYSES AND IMPLEMENTATION OF SECURITY FACTORS FOR SOFTWARE FUNCTIONING AT THE SECURITY SYSTEM OF CORPORATE NETWORK

Elshan Rahimov

Institute of Information Technology of ANAS, Baku, Azerbaijan
elshan_rahimoff@mail.ru

1. Introduction

Plentiful development of highly technological decisions in all fields of activity of the human life based on realization of corporate networks besides huge conveniences and possibilities also creates problems of not less small scale. Problems arising in realization of highly technological projects are connected with heterogeneity of software, platforms, architecture and distinction of algorithms of realization of the same problem. A question maintenance of information security as in corporate networks and also software security which are fundamental elements of information security system of corporate networks is a question rather actual and not solved up to the end. Last year's especially the huge attention to began to pay to the organizing of software security which makes a complex of information security system of corporate networks. The given interest has been caused on the basis of the statistical data infringements full-functionality of information security system on the base of information collected by the various international certified organizations of incidents registration at corporate networks with various architecture and scale.

2. The main aspects

For effective using of software which is stay on the base of information security system of corporate network besides maintenance of reliability of their functioning necessary measures are prevention of possible influences, both on the information, and on hardware, negative factors of casual or deliberate character, factors capable to cause to the user a damage. Problems of maintenance of protection of hardware from the infringements connected with refusals and failures, are problems which can be sorted out at the designing stage of corporate network information security system. However in current time does not exist the uniform theory of security systems at deliberate external influences and threats that does application of security system not always effective and economically profitable. For more clearance let us to consider the basic definitions and the concepts connected with security factors of software, resulted in work.

Threat - any circumstances or events which can be to stay a reason of a damage to software in the form of destruction, disclosing or updating of the data, or refusal in service. As a threat can be the thing, person, event etc., i.e. everything which can represents danger for software which is in complex of security system of corporate network.

Attack is the fixed attempt of overcoming of security, threat realization. That fact that attack has been carried out, does not mean that it is successfully resulted. Degree of success of attack depends on vulnerability of software and efficiency of security measures.

Vulnerability - lacks of security factors caused by absence of well guarded security mechanisms, errors in security mechanisms at realization of security system platform, at the internal control of system, or which can be used for infringement of working capacity of system at displaying of one or several threats simultaneously. Vulnerability at the concrete software or in complex of security system relating automatically with threats. For example, threat of unauthorized access is defined by lacks of system of passwords or some missing of authentication services which can active in any secured system [1].

Penetration is a successful overcoming of security system complex or some individual software which is stay for guarding the system. One of most complicated questions at construction of security process model against threats is the security estimation. As it is well

known from practice it is difficult to receive real values of security efficiency. Besides, the problem of a choice of indicators of security also is one of the problematic questions of security theory. There are some cases in practice when software behavior which is create a base of information security system of corporate network is well studied and initial data is exact and clear, there are techniques of reception of analytical and statistical estimations of quality of their functioning. These are estimations of such indicators as probabilities of transformation and data loss, probability-periodically characteristics of delivery of messages. Concerning boundary estimations of indicators of security corresponding criteria practically are absent. In practice existing some models where estimation of probability of maintenance of security by means of the concrete hardware, based on concept of a weak point which is close inherently to the analysis of reliability of systems in a context of the theory of possibilities.

In practice the security norm can be set in the various ways with use of such criteria as achievement of the maximum security at observance of restriction on a total cost of security systems, maintenance of the set level of protection taking into account cost of security systems, etc. The given criteria and estimations have a number of lacks which limit their use. The main lack consists that many sizes used in resulted criteria are unknown or inexact. Moreover, offered estimations and norms do not consider constant perfection of methods of carrying out of attacks.

For working out of estimations and norms of security it is necessary to consider at first a basis of threats processes and their consequences on functioning at security system and in its elements which are software with different platforms and measures. In reliability theory one of the parameters which is characterizing process of refusals of system this is time till refusal. At the analysis of software security and their protection, time cannot characterize to the full attack and its consequences. It is necessary to consider efforts (E), spent by attacking person for security overriding. Efforts can sometimes be characterized by time of penetration and security overcoming. However in the more general case of effort represent the whole family of parameters or their combination, including financial expenses, time, experience and abilities attacking and etc. In particular it is possible to consider as effort such behavior attacking, as its studying of software functioning at security system of corporate network for the further use of the received knowledge in the course of attack. The effort is already used as the characteristic of security systems or its elements. For more clearance of above mentioned it's quite enough to imagine that efficiency of means of cryptography and enciphering is defined as the relation of cost expenses for decoding of the data to cost of this data.

Use of effort as security parameter allows to analyze following situations for which use of the characteristic of time is not meaningful. We will consider a case of the attack arising owing to entering of a special program code in system for its later use. In this case the brought code any time is not active, i.e. does not render any influence at software. Moreover, the condition of its activity can and not come. There are cases when expenses of efforts occur instantly or in enough short time intervals. For example, success of process payoff of the manager or power user of system completely depends on size of a effort and does not depend on time and there are several examples where time is not central indicator.

The analysis of process of refusals in reliability theory is not meaningful without consideration of consequences of these refusals. Similarly in the security analysis it is necessary except process of efforts for security overcoming to consider the process characterizing consequences of these efforts as not all penetrations into system have identical value both for attacking person, and for the corporate network owner. It is the process of continuously collecting awards (A) resulting in process of interaction with software even if this interaction does not lead to penetration. Compensation which will receive attacking person at penetration into software, defines its motivation and its readiness to spend the certain efforts necessary for successful attack and penetration. Compensation examples are own satisfaction, reception of money, curiosity. Thus, process of attacks is characterized not only efforts for penetration, but also compensations for the spent efforts. Thus it is supposed that compensation will be more than the spent efforts, differently what sense to spend attack [2].

The account of process of compensations does obvious consideration of characteristics of protection not only from the point of view of attacking person, but also from the point of view of the corporate network owner. From the point of view of the corporate network owner it is possible to consider also process of losses (L) which arise at penetration into system. This process of losses of the corporate network owner is some function of compensations attacking person. In this case compensation of attacking person, in general, does not coincide with losses of the corporate network owner. Let there is some "true" value of security or the effort necessary for penetration which nobody knows. Then losses of the corporate network owner can be considered as the top border of this "true" value, and compensation of attacking person - as the bottom border. It is similarly possible to tell that the effort is the bottom border for compensation of attacking person as there is no sense to spend efforts to attack carrying out if compensation does not correspond to these efforts. It is obvious that such parities it is not always carried out. However "on the average" is possible to consider parities fair. In most cases compensation of attacking person difficult enough to estimate, while is possible to present losses of the owner in many situations in the form of cost estimations.

On efforts of attacking person are influence expenses (X) of owner on software for security systems of corporate network. Thus the more expenses on software for security system were spent, correspondently the big efforts are necessary for overcoming of these means. Hence, basic characteristics can be a basis for reception of indicators of security: efforts of attacking person for penetration into system through software, compensation of attacking person for carrying out of attack, an expense for security systems and losses of the corporate network owner and also users and the system administrator, resulting with penetrations into system. As in most cases quantitatively to describe first two characteristics difficult enough we will consider further expenses and losses or potential losses of the corporate network owner as a basis for the analysis of software security. However it does not mean that first two characteristics cannot be used. At creation or tests of security systems through software, in some cases it is possible to receive numerical estimations of efforts and compensations of attacking person and to use them as the bottom generalized average values of losses as a result of penetration.

3. Implementation of security factors for software

It's very important to demarked that the award of attack realize person do not depend on software for security system expenses, but depend on only looses of corporate network owners. And also effort coefficient do not depend on corporate network owners looses, but depend on only expenses which is expend on software for security system [2-3]. So from such approach it possible to dedicate two pair of relations: attack release person effort (E) – expenses on software for security system (X), attack realize person award (A) – corporate network owners losses (L). If become all parameters to unique dimension system, then in best situation the next relation is right: $X \le E \le A \le L$. But in practice existing such situation that effort of attack realize person do not becomes to some successful results, then in this case $L = 0$ or $E > L$. In this situation we will obtain discrepancy. Let call interrelations of attack realize person, corporate network and owner by coordinated, if the relations are held by the middle value, such as: $\tilde{X} \le \tilde{E} \le \tilde{A} \le \tilde{L}$, where $\tilde{X}$, $\tilde{E}$, $\tilde{A}$, $\tilde{L}$ are middle value of X, E, A, L.

If we assume interrelation process of attack realize person and corporate network owners by the means of some generally probably parameters X, then the behavior of this parameter is possible to describe by help of interval generally middles. In this case $\tilde{Z} = \underline{V}$, $\tilde{L} = \overline{V}$, where $\underline{V}$ and $\overline{V}$ are infimum and supremum middles of V. Approach to the problem from this point of view is allow to observe from one position absolutely different security parameters and threats parameters in one frame. And it really well known from practice that parameters which is describe security, threats, attacks, vulnerabilities and etc., can be characterizing by different functions. If the parameters characterizing by time, i.e. $V=t$, then $\underline{V}$ and $\overline{V}$ are

infimum and supremum middles time of interrelation of attack realize person and corporate network owners. If V is holds characteristics of the indicator function, i.e. $V(v)=1$, when $v \in [a,b]$ and $V(v)=0$, when $v \notin [a,b]$, then $\underline{V}$ and $\overline{V}$ are infimum and supremum probability of that parameter of interrelation between attack realize person and corporate network owner is located in the interval $[a,b]$. Leaning to the practice here is possible to assume that parameter x is interrelation time $(v=t)$, interrelation expenditure $(v=C)$, quantity of successful attack realizing $(v=k)$ and etc. Also if take into account sequences of attached intervals $[a_1,b_1] \subset ... \subset [a_n,b_n]$ where defining the middles, then we will obtain the distribution function of interrelation parameter possibilities.

Let's call the infimum middles by general function of security and supremum middles by general function of vulnerability. For both of them it is possible to give absolutely different explanations. For example: the security function is possible explain as maximum expenditures, which corporate network owners ready to pay for organizing of security system on the base of software. The function of vulnerability it is possible to review as minimal looses, which corporate network owners is ready to lose during successful realizing of attack [4].

Let's $\underline{V}_{ij}$ and $\overline{V}_{ij}$ - infimum and supremum middles value of V_{ij} for i element of corporate network, which have place at the result of j threats, $i \in \Phi$ - set of system elements numbers, $j \in \Psi$ - set of possible threats numbers. Assume that interrelation of all attack realize persons, owners and users of the corporate network characterizing by means of variable W, which is defining as some function $W = Q(V_{ij})$. Then infimum $\underline{W}$ middles value of W is defining on the base of continuous principle:

$$\underline{W} = \sup\left\{ m_0 + \sum_{i\in\Phi} \sum_{j\in\Psi} [a_{ij}\underline{V}_{ij} - b_{ij}\overline{V}_{ij}] \right\}$$

where supremum is located on all values of $m_0 \in A, a_{ij}, b_{ij} \in A^+$ when next restriction has a place

$$m_0 + \sum_{i\in\Phi} \sum_{j\in\Psi} [a_{ij}V_{ij} - b_{ij}V_{ij}] \le Q(V_{ij})$$

$\overline{W}$ supremum middles value of W is defining from next equation

$$\overline{W} = \inf\left\{ m_0 + \sum_{i\in\Phi} \sum_{j\in\Psi} [a_{ij}\overline{V}_{ij} - b_{ij}\underline{V}_{ij}] \right\},$$

where infimum is located on all values of $m_0 \in A, a_{ij}, b_{ij} \in A^+$ when next restriction has a place

$$m_0 + \sum_{i\in\Phi} \sum_{j\in\Psi} [a_{ij}\overline{V}_{ij} - b_{ij}\underline{V}_{ij}] \ge Q(V_{ij})$$

So if take into account all listed items of above calculation of security indicators of software, functioning as the main element of corporate network security systems are coming to solving of linear programming problems.

References

1. Rahimov E.R. Corporate Networks management. Baku – «Information Technologies», 2008, 322 p.
2. Cai K.Y., Wen C.Y., Zhang M.L., A novel approach to software reliability modeling // Microelectronics and Reliability. 1993 – V.33, pp. 2265-2267.
3. Musa J.D., Iannino A., Okumoto K. Software reliability: Measurement, Prediction,Application. McGraw-Hill, 1987.
4. Popentiu Fl., Boros D.N. Software reliability growth supermodels // Microelectronics and Reliability. 1996 – V.36(4), pp. 485-491.