ISSN 1512-1232

UDC 004.05

BASE PRINCIPAL OF MANAGING OF NETWORK SOFTWARE SECURITY BY VULNERABILITIES DETERMINATION MODEL

Rahimov Elshan Rasif

Institute of Information Technology, Azerbaijan National Academy of Sciences, Baku, Azerbaijan
elshan_rahimoff@mail.ru

Abstract

At the given article have been parsed security problems which are existing in network software. On the basis of internal and external vulnerabilities analyses has been underlined importance of the security of network software as a basic element of corporate network information security system. Preceding from the given approach the model of vulnerabilities defining at the network software was offered.

Keywords: *network software, security, vulnerability, corporate network, attack, threat, information security system.*

I. Introduction

Rapid development of an information technologies, occurrence of new and is rather wide possibilities software involves more and more attention to computer industry from side of various organizations. Now many organizations make the decision on integration of the local and corporate networks in an open global network. Movement of an information technology towards open global networks, a wide circulation of a Internet as means of interoperate dialogue give to a security problem a special urgency. Losses of the organizations as a result of destruction or information leakage are capable to exceed repeatedly expenses for information security system of corporate networks. Therefore questions of security in wide meaning should dare already at design stages of corporate networks. In corporate networks it is necessary to develop a security policy for information security. One of the primary goals of a security policy is the choice of information security means. The choice of security systems at the earlier stages demands much smaller expenses, than performance of similar work with maintained corporate network. In the frame of current paper we will call software which is building the main fundaments of corporate network information security system by the network software.

Detection in program codes of the elements destroying network software, helps to solve a security issue of network software at earlier stage as on security directly executed code of the program, instead of the services given by network software is exposed to the analysis. For detection in program codes of the elements destroying network software, only the full-function network software intended for work at corporate network under control of one or of some operating systems without fail should be investigated. Among approaches to network software security the important place is occupied with a method of installation of used mechanisms of protection and a functioning principle. It in turn can be classified on: the systems established on compiled modules of network software; the systems which are built in an initial code of network software before compilation; and combined. The systems established on compiled modules of network software are most convenient for the manufacturer as can easily protect already completely the ready and tested network software. But, on the other hand, negative line of the given approach is its low enough firmness. The systems which are built in an initial code of network software before compilation, are accompanied by a number of inconveniences for the manufacturer as there is a necessity for carrying out of regular trainings of the personnel, work with the program interface. It in turn involves undesirable financial expenses. Process of testing of network software also becomes complicated and its reliability at the

ISSN 1512-1232

expense of inclusion of additional verification of program interfaces and its procedures decreases [1]. As at realization of information security system of corporate networks at the primary stage play main role the network software, then choice and estimation of these means holds the basic share of the organization of security.

II. The main aspects

One of the main aspects of security of network software is internal sources. Internal sources of threats at the security of network software functioning are:

- System errors at statement of the purposes and problems of designing of functional suitability of network software at the formulation of requirements to functions and characteristics of security means of problems decision;
- Defects and errors at definition of functions, conditions and environment parameters in which it is necessary to apply protected network software;
- Algorithmic errors of designing at direct algorithmization of security functions of hardware, network software and databases at definition of structure and interaction of components of functional network software complexes, and also at using of the database information;
- Errors and defects of programming in texts of programs and descriptions of the data, and also in initial and resulting documentation on components of network software;
- Insufficient efficiency of used methods and means of operative software operation and data, security of functioning and restoration of working capacity of network software in the conditions of casual and premeditated negative influences from an environment.

Full elimination of listed above threats of security of functioning of critical network software which provide information security system of corporate networks from practical point of view is impossible. At creation of difficult network software complexes the problem consists in revealing of factors on which they depend, in creation of methods and means of reduction of their influence to security. It is necessary to estimate vulnerability of functional components of network software for various negative influences and degree of their influence on the basic characteristics of quality and security and also on total risk. Depending on situation it is necessary to distribute resources for creation of network software and its components, with same security of functioning with the minimum generalized risk at any negative external influences. As a result should be formulated corresponding methods and counter-measures which, in turn define necessary functions and mechanisms of maintenance means of working capability and security.

For maintenance of functional security of network software corresponding counter-measures are created, specialized systems and means which include set of the interconnected standard documents, organizational-technical actions and methods corresponding to them and the network software intended for the prevention and liquidation of negative consequences rejection situations, various threats of security, their revealing and localization. Creation of such complexes of increase of security provides planning and realization of a purposeful policy of complex maintenance of network software functional security and also effective distribution of resources to counter-measures and security means. Counter-measures undertake for reduction of vulnerability and security policy performance. As well as should follow from a uniform security policy, one of the first development cycles of the specification for secured network software should be modeling of threats. That represents methodology of the analysis of security, which can be used at definition of risks and decision-making at architecture construction, coding and testing. The given methodology is applied mainly at initial stages of realization of the project which working out of specifications, architectural representations, diagrams of data flows and etc. The ultimate goal consists in elimination of potential threats for the network software, capable to cause damage. As a whole, modeling of threats assumes decomposition of the appendix and definition of its basic properties with the subsequent revealing and classification of the threats directed against each service or a component. Threats are classified depending on risk degree [2].

Revealing of existing and acquired vulnerability in the services given by network software, is one of widespread security methods offered by various corporations which are dealing with network

ISSN 1512-1232

software security used both in corporate networks, and on separate workstations. By means of the given approach is defining the basic strategy of vulnerability detection process at network software designing on the basis of errors found at realization and repeated operation of system. If to consider structure of the given approach, then gathering of the primary information on operating structures of network software and services is initially made, on the basis of the collected information possible variants of vulnerabilities which are existing at network software are assumed. Further on prospective vulnerable points are made same-directed attacks from outside and by that reliability of assumptions is checked. On the basis of successfully realized attacks the stream of vulnerabilities which are existing in network software is specified and grouped. As in many classical methods this given approach has weak places, such as impossibility of organization of formal vulnerabilities classification, obligatory primary knowledge of working principles as network software, and its internal architecture.

As a result of all above mentioned items, creating the strategy of threats liquidation at design stages, coding and testing. But also after introduction of these counter-measures residual risks which are admissible owing to limitation of resources can remain.

Requirements to the network software providing security, are usually represented as a part of the general specification of requirements to functional suitability of system and security complex. Measures in this case should be taken for distribution of system requirements to security between hardware and network software components of maintenance of functional security. If the software complex of security requires interaction with other additional software or hardware components in the specification of requirements interfaces between applied components should be stipulated directly or by means of references [3].

The instrumental means which have been built in an operating system or in corresponding components and functions of network software complex are necessary for direct quantitative measurements of functional security. These means should in dynamics of real functioning of network software complex automatically selected and register of refusal situations, defects and distortions of computing process of network software and the data, revealed by the hardware, program-algorithmic control or users. Accumulation and ordering of displays of refusals at execution of network software allows to estimating the basic indicators of security, helps to define the reasons of failures and refusals and to prepare the data for improvement of functional security of network software complex. Regular registration and generalization of such data promotes elimination of the situations negatively influencing functional suitability and other base characteristics of software complex.

III. The model of vulnerabilities defining at the network software

At the heart of realization of almost any security system of corporate networks is staying the network software complex which by means of what security of the information is provided. At such approach security of network software plays a primary and important role. The question of network software security which is functioning within the frame of information security system of corporate network is many-sided enough, as in model which the given approach will realize should be considered such factors as: services provided by network software; the platform in which environment functions network software modules; internal architecture; external factors influencing on workability of network software elements; instructions which is following from unique security policies of corporate network; compatibility of network software of various manufacturers both at level functioning, and at level of a program code on which realized given network software [4-5].

Carrying out of the analysis of potential possible threats of the information and the actions following from a security policy, are one of obligatory development cycles of a security network software complex. As making elements of security in each secured corporate network are resources and the software, which is organized process of security functioning of system we will designate through r – the resources used in network software, where $r \in R$, and through p where $p \in P$ we will designate set of the network software services used and having possibility directly to influence

ISSN 1512-1232

security of network software. Without dependence from internal architecture of network software and kinds of services, both sets are final.

In network software with any internal architecture, to resources *r* various levels of security are appropriated. These levels can be defined by both the international standards and by levels of security certain by manufacturers already fixed in ready platforms.

Further we will designate by N - quantity of network software vulnerable elements, and parameter K contains initial value of average quantity of the attacked software elements during unit time. Depending on internal architecture of network software the parameter K is in some measure defined by types of representative services with productive capacity of servers and workstations. We will be considering the variant where the parameter K does not depend on the restrictions set forth above. Also during calculations it is very important to taking into account that the same network software which is functioning on the one workstation cannot be attacked twice as realization of the first attack is absolutely successful.

Let $a(t)$ – a proportion of vulnerable points in network software which have been successfully attacked during time t, then $N \cdot a(t)$ is representing the total of successfully attacked network software, each of which will be potentially used for carrying out of the subsequent attacks with their average quantity K. As the part of network software functioning at information security system of corporate network already has been successfully attacked by each new grasped software, then grasped network software will undertake no more $K(1-a(t))$ new successful attacks. Thus, the quantity of the grasped network software during time dt is equal:

$$n = aN \cdot K(1-a)dt .$$

Take into account, that N – is constant, then

$$n = d(Na) = Nda .$$

Then next equation is right:

$$Nda = aN \cdot K(1-a)dt ,$$

which is conducts to the differential equation of following type:

$$\frac{da}{dt} = Ka(1-a) .$$

The result of solution of given equation is:

$$a = \frac{e^{K(t-T)}}{1+e^{K(t-T)}} ,$$

where, T - is time indicator parameters, which is characterized a maximum increasing of attacks. By choosing of method and attack strategy, the malefactor defines quantity of the information which will be has by realization of attack to separate network software. And from here is defining the security indicator of network software functioning at information security systems of corporate network.

Acknowledgment

Fistful at the beginning of this article has been parsed security problems which are existing in network software. On the basis of internal and external vulnerabilities analyses and researching of main aspects of network software has been underlined importance of network software security as a basic element of corporate network information security system. Preceding from the given approaches the model of vulnerabilities defining at the network software was offered. Which can help in the future to correct organizing of network software security and on the base of it designing of well guarded information security system of corporate networks.

Conclusion and future works

On the base of offered model, i.e. by prior analyses of security elements of corporate networks and by determining internal and external vulnerabilities of arbitrary structured network software

ISSN 1512-1232

by means of the model of vulnerabilities defining at the network software is possible to correctly organize full-functionality security mechanism of network software.
In the future, after correct organizing of functionality of network software security, it possible to applying the current vulnerabilities defining model to other security elements of corporate network information security system.

References

1. Martin L. Shooman, “Reliability of Computer Systems and Networks, Fault Tolerance, Analysis, and Design”, J.Wiley & Sons, Inc, 2002, ISBN: 0-471-29342-3.
2. E. R. Rahimov, "The role of software security at the complex protection system of corporate network”, Telecommunications, Moscow, vol. 10, pp. 23–26, October 2009.
3. Laural L. Pullum, “Software Fault Tolerance, Techniques & Implementation”, Artech House, Inc., 2001, ISBN: 1-58053-137-7.
4. Ann T. Tai, John F. Meyer, Algirdas Avizienis, “Software Performability: From Concepts to Applications”, Kluwer Academic Publishers Norwell, MA, USA, 1996, ISBN:0792396707.
5. Debra Herrmann. Software Safety & Reliability, IEEE Computer Society Press,1999.

Article received: 2010-10-01