Information security risks assessment and management framework

I.V Anikin[1]

[1]Kazan National Research Technical University named after A.N. Tupolev - KAI, Kazan, Russia, 420111.

Abstract. Providing of information security becomes very essential for modern telecommunication networks. This task is often decided from the perspective of information security risks, but some problems arise in practice with risks assessment and management in quantitative form. They are uncertain, incomplete, fuzzy and qualitative character of source information about existing threats and vulnerabilities. In this paper we developed the framework for quantitative information security risks assessment and management under these challenges. We used the framework for risks assessment and management in electronic trading platform and found the optimal set of security safeguards.

Keywords: information security risks, fuzzy logic, analytic hierarchy process.

1. Introduction

Nowadays, telecommunication networks are an objects of influence of different information security threats and vulnerabilities. Therefore, providing of information security becomes very essential for them. There are two basic ways for ensuring information security in telecommunication networks - baseline and advanced. Nowadays, advanced security level which is related with information security risks assessment and management [1,2,3], becomes more actual. This approach enables to construct information security safeguards bundle more effectively. There are a lot of white papers, standards and guidelines which are dealing with deciding this task. Some of them assume operating with risks in qualitative form [4,5] whilst others – in quantitative form [6,7,8]. Moreover, a lot of frameworks exist for information security risks assessment in both form [9,10,11].

Information security risks assessment and management in quantitative form becomes more important today because anyone can obtain more precise risk values. We can estimate an economic indicators for information security systems and optimize them more easily [13]. Nevertheless some problems arise in practical implementation of these methods due to uncertain, incomplete, fuzzy and qualitative character of source information about existing threats and vulnerabilities in telecommunication networks [3,13]. So, it is extremely essential to implement risks assessment, analysis and management methods in telecommunication networks under these challenges.

To overcome these challenges, in our previous works [3,12,13] we suggested some methods and algorithms based on fuzzy logic [14] and analytic hierarchy process [15]. Based on these methods in

this paper we developed the framework for quantitative information security risks assessment and management in telecommunication networks.

The structure of this paper is organized as follows: in the section II we describe briefly technology, methods and algorithms for quantitative risks assessment and management. In the section III we describe our framework which implements suggested technology. In the section IV we used the framework for risks assessment and management in secure electronic trading platform [16]. We discussed some experimental results and found optimal secure safeguards based on information security risks values.

2. Technology for quantitative information security risks assessment and management in telecommunication networks

Suggested information security risks assessment and management technology includes following interacting components:

- math model of telecommunication network;
- threat's model in telecommunication network;
- safeguard's model in telecommunication network;
- fuzzy impact assessment methods and algorithms for existing threats;
- fuzzy possibility assessment methods and algorithms for existing threats and vulnerabilities;
- fuzzy risks assessment/optimization methods and algorithms in telecommunication networks.

Math model of telecommunication network [3] involves some useful components for risk assessment: existing assets of telecommunication network (information, hardware components, IT-services), relations between these assets and their impact values, logical structure of network, information flows, fault tree for IT-services.

Threat's model in telecommunication network has been defined by ternary graph with vulnerabilities, threats and assets.

Safeguard's model in telecommunication network [3] was defined by expression (1)

$$M_S = \left\langle Z, R_S^V, R_S^T, R_S^{I-C}, R_S^{I-I}, R_S^{I-A} \right\rangle \quad (1)$$

with the set Z of security safeguards, matrixes $R_S^V, R_S^T, R_S^{I-C}, R_S^{I-I}, R_S^{I-A}$ with fuzzy decreasing coefficients for vulnerability levels, threat's exercising possibilities, impact levels from the threat by confidentiality, integrity and availability.

We used following methods and algorithms for fuzzy impact assessment from the specific threat [12]:

- FZ_STAT algorithm [18] for membership functions construction for fuzzy values of security properties based on expert judgments.
- Method for fuzzy values estimation of information assets confidentiality, integrity, availability). Implementation of the method is based on quantitative assessment of 25 particular indicators of impact with using analytic hierarchy process (AHP).
- Method for estimation of fuzzy values of hosts, servers, telecommunication equipment and IT-services. Implementation of the method is based on processing of fuzzy values of information assets and on using analytic hierarchy process and fault tree.
- Method for estimation of fuzzy impact from the certain threat. Implementation of the method is based on processing of fuzzy values of assets on the threat's model.

We used following methods and algorithms for fuzzy possibility assessment for existing threats and vulnerabilities [12]:

- Method for evaluation of threat's exercising possibility based on questionnaires. We suggested the questionnaires for more than 100 possible threats in telecommunication network which include questions about possibility factors and available answers for selection. We used analytic hierarchy process for getting the number of points for each available answer in the questionnaire.
- Method for evaluation of vulnerability level. Implementation of the method is based on new fuzzy IF-THEN rules, new fuzzy inference scheme [12] and CVSS v3.0 metrics [18]. This

method enables getting possibility levels for vulnerabilities under the gaps, inconsistency and fuzzy character of source information. We can use this method for vulnerability ranking and vulnerability's possibility evaluation.

We used following methods and algorithms for fuzzy risks assessment/optimization:

- Fuzzy risks assessment method without safeguards which is implemented with using expressions (2) or (3) and based on fuzzy risk factors evaluated before.

$$Risk(Threat) = Impact(Threat) * Possibility(Threat) \quad (2)$$

$$Risk(Threat) = Impact(Threat) * Possibility(Threat) * * Possibility(Vulnerability) \quad (3)$$

- Fuzzy risks assessment method with safeguards which is implemented by considering fuzzy decreasing coefficients and safeguard model (1).
- Cost/benefit ratio estimation method [9] for security safeguards. Method is implemented with using 8 partial cost indicators and analytic hierarchy process.
- Information security risks management method. Two possible optimization tasks is decided: maximization of cost/benefit ratio where residual risks are less than selected threshold; minimization of overall information security risk level where payback period of the project and lump-sum costs are less than selected thresholds.

These methods have been implemented in the special framework for quantitative information security risks assessment and management in telecommunication network.

3. Framework for quantitative information security risks assessment and management in telecommunication network

Developed framework consists of following modules:

- Impact assessment module is developed on Microsoft .NET 4 platform. We can use this module for deciding following tasks: creation a formal model of a telecommunication network, defining particular indicators of impact and constructing impact hierarchy, getting expert judgments, applying AHP, developed methods and algorithms for evaluation of the impact from the specific threat.
- Threat's exercising assessment module is developed on C#, Visual Studio platform. We can use this module for deciding following tasks: defining particular indicators of threat's exercising possibility, constructing possibility hierarchy and questionnaire, applying AHP, developed methods and algorithms for answer's points assignment in questionnaire and threat's exercising assessment. We use SQLite database for storing the questionnaires.
- Vulnerability fuzzy level evaluation module is developed on Delphi platform. We can use this module for deciding following tasks: defining CVSS metrics for evaluation of vulnerabilities and their importance level, defining linguistic variables [19,20] related with these metrics, constructing knowledge base for evaluation of vulnerabilities based on fuzzy IF-THEN rules, defining source information about metrics (may be incomplete), applying developed fuzzy inference scheme for vulnerability evaluation.
- Library for working with fuzzy data is developed on C#. This library suggests special operators for working with fuzzy numbers. FZ_STAT algorithm for construction of membership functions based on expert judgments is included in the library. We can also use this library for deciding risk optimization tasks with fuzzy data. We used genetic algorithm to reduce the algorithmic complexity of these tasks.

4. Information security risks assessment and management in electronic trading platform

We used developed framework for quantitative information security risks assessment and management in telecommunication network of electronic trading platform [16]. This platform is one of the sixth platform in Russia which have an accreditation as a platform for implementation of procurement procedures in electronic form for federal structures. Such platforms are very essential for Russian business and must be secured from various cyber threats. That's why effective selection of security safeguards is very important for such platforms.

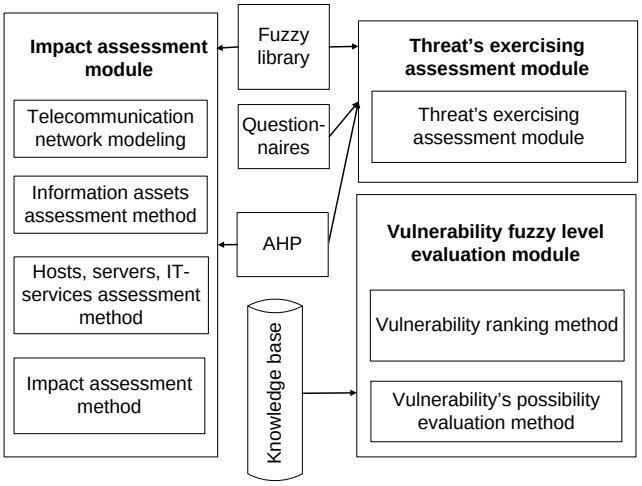

Figure 1. The structure of the developed framework.

The structure of the developed framework is presented on figure 1.

We considered 23 different information assets in this platform, such as: WEB-site content, information about bargaining, personal data of stakeholders, program code of electronic trading platform, project's documentation, application review protocols, different registers, information about accounts and financial transactions etc.

We considered operator's and administrator's hosts, database and WEB servers, vendor work area server, terminal server and all telecommunication equipment.

We considered 14 main IT services in telecommunication network of this platform, such as: active directory, information systems "Operator", "Customer", "Provider", 1C and DBMS access, corporate mail, external WEB-site access, providing of terminal access, WTS, WSUS, DNS etc.

After the modelling of telecommunication network, we used developed framework for assets evaluation. We considered following threats in telecommunication network:

T.006 - code or data injection;

T.008 – disclosing of authentication information;

T.018 - abnormal operating system booting;

T.067- unauthorized acquaintance with the confidential information;

T.091- unauthorized erasing of a sensitive information;

T.116- sniffing;

T.128 - masquerade;

T.140 - denial of service;

T.167 - infection of the computer due to visiting untrusted web-sites;

T.179 - unauthorized modification of the sensitive information.

We used developed framework for risks assessment in telecommunication network of electronic trading platform. Final fuzzy risks values (as fuzzy triangles) are presented in the table 1.

Table 1. Risks Assessment Results.

Threat	*Fuzzy risk values*
T.006	(8343094, 8849024, 9243317)
T.008	(11294401, 13466755, 14960988)
T.018	(1000158, 1001031, 1001483)
T.067	(11749832, 14075063, 15637973)
T.091	(1935139, 1977732, 1998857)
T.116	(16517114, 20072955, 22575080)
T.128	(12544643, 15245282, 17145631)
T.140	(21099175, 21565227, 21768789)
T.167	(1230962, 1232038, 1232594)
T.179	(4629550, 4732746, 4778225)

We considered the following full set of possible safeguards for electronic trading platform:

- Z1 - software for protection hosts/servers from unauthorized access;
- Z2 - antivirus;
- Z3 - embedded protection mechanisms in telecommunication equipment;
- Z3 - firewall;
- Z4 - IDS/IPS;
- Z5 - network scanner;
- Z6 - using cryptography for telecommunication channels;
- Z7 - backup system;
- Z8 - analysis and consolidation of information security events;
- Z9 - protection of the virtual environment.

For each safeguard we used expert's judgments to define decreasing coefficients for vulnerability levels, threat's exercising possibilities, impact levels from the threat by confidentiality, integrity and availability. Then we used developed framework to evaluate residual risks and cost-benefit ratio for all combinations of safeguards. Finally we decided two optimization tasks:

1. Maximization of cost/benefit ratio where residual risks are less than selected threshold. We have got that the following set of safeguards is optimal – Z1, Z2, Z3, Z4, Z6, Z7, Z10 (annual residual risk threshold is 100 000 $). This set of safeguards reduces overall risk value in 21.4 times.
2. Minimization of overall information security risk level where payback period of the project and lump-sum costs are less than selected thresholds. We have got that the following set of safeguards is optimal – Z1, Z2, Z3, Z4, Z5, Z6, Z7, Z1 (payback period threshold is 1 year, initial lump-sum threshold is 33 000 $). This set of safeguards reduces overall risk value approximately in 21.7 times.

We have got that residual risk value in the second task on 1200 $ less than in the first task, however it requires approximately 16000 $ additional lump-sum money which is too much. So, we selected following set of safeguards - Z1, Z2, Z3, Z4, Z6, Z7, Z10, which is the decision of the first optimization task.

5. Conclusion

In this paper we suggested the framework for quantitative information security risks assessment and management. This framework can decide these tasks under uncertain, incomplete, fuzzy and qualitative character of source information about existing threats and vulnerabilities. We used fuzzy logic, analytic hierarchy process, questionnaires, new fuzzy IF-THEN rules and new fuzzy inference scheme for dealing with these challenges.

We used the developed framework for information security risks assessment and management in electronic trading platform. We found optimal set of security safeguards for this platform based on information security risks values. This set of safeguards reduces overall risk value in 21.4 times. In comparing with the full set of possible safeguards we save 46500$ on acquisition of information security system and do not exceed acceptable residual risk value.

6. References

[1] Alberts, C. Managing information security risks. The OCTAVE^{SM} approach / C. Alberts, A. Dorofee. – Addison Wesley, 2002. – 512 p.

[2] Peltier, T.R. Information Security Risk Analysis / T.R. Peltier. – Auerbach Publications, 2010. – 456 p.

[3] Anikin, I.V. Information security risk assessment and management method in computer networks / I.V. Anikin // IEEE, Proc. Int. Siberian Conf. on Control and Communications (SIBCON 2015). – Omsk, 2015.

[4] NIST Special Publication 800-30, Revision 1, Guide for Conducting Risk Assessments. – DOI: /10.6028/NIST.SP.800-30r1 (September 2012).

[5] PRINCE User's Guide to CRAMM – Stationery Office Books, 1993. – 140 p.
[6] Karabacaka, B. ISRAM: information security risk analysis method / B. Karabacaka, I. Sogukpinar // Computers app. Security. – 2005. – Vol. 24. – P. 147-159.
[7] Risk Management Insight LLC. FAIR (FACTOR ANALYSIS OF INFORMATION RISK) Basic Risk Assessment Guide, Risk Management Insight LLC, 2006.
[8] Clymer, C. IRisk Evaluation. SecureState Whitepaper / C. Clymer, K. Stasiak, M. Neely, S. Marchewitz. – [Electronic resource]. – Access mode: https//www.securestate.com
[9] Makarevich, O. The method of the information security risk assessment in cloud computing systems / O. Makarevich, I. Mashkina, A. Sentsova // Proc. 6th Int. Conf. on Security of Information and Networks (SIN'2013). – Aksaray, Turkey. – 2013. – P. 446-447.
[10] Shamala, P. A conceptual framework of info structure for information security risk assessment (ISRA) / P. Shamala, R. Ahmad, M. Yusoff // Journal of Information Security and Applications. – 2013. – Vol. 18(1). – P. 45-52.
[11] Joshi, C. Information security risks management framework – A step towards mitigating security risks in university network / C. Joshi, U.K. Singh // Journal of Information Security and Applications. – 2017. – Vol. 35. – P. 128-137.
[12] Anikin, I.V. Information Security Risk Managament in Computer Networks based on Fuzzy Logic and Cost: Benefit Ratio Estimation / I.V. Anikin, L.Yu Emaletdinova // Proc. 8th Int. Conf. on Security of Information and Networks (SIN'15). – Sochi, Russia, 2015. – P. 8-11.
[13] Anikin, I.V. Information security risks assessment in telecommunication network of the university / I.V. Anikin // IEEE Conf. Dynamics of Systems, Mechanisms and Machines. – Omsk, Russia, 2016.
[14] Zadeh, L.A. Fuzzy Sets / L.A. Zadeh // Information and Control. – 1965. – Vol. 8. – P. 338-363.
[15] Saaty, T.L. Decision Making for Leaders: The Analytic Hierarchy Process for Decisions in a Complex World / T.L. Saaty. – RWS Publications, 2001. – 323 p.
[16] Russian e-commerce system [Electronic resource]. – Access mode: www.zakazrf.ru.
[17] Anikin, I.V. Vulnerability Risk Assessment Method Based on Fuzzy Logic / I.V. Anikin // Proc. 2nd National Conference on Information Technology and Compuer Science . Shanghai. – 2015. (CITCS 2015). – P. 1554-1560.
[18] CVSS V.3.0. A Complete Guide to the Common Vulnerability Scoring System. – Access mode: https://www.first.org/cvss/cvss-v30-user_guide_v1.4.pdf.
[19] Zadeh, L.A. Linguistic approach to system analysis / L.A. Zadeh // IEEE Int. Symp. on Circuit Theory, Proc. Dig Pap; Toronto, Ont, Can.
[20] Zadeh, L.A. Linguistic variables and approximate reasoning / L.A. Zadeh // Proc. – 6th Annual Symposium on Computer Applications in Medical Care. – 1982. – P. 787-791.