Information Security Risk Management in Computer Networks Based on Fuzzy Logic and Cost/Benefit Ratio Estimation

Igor Anikin
Kazan National Research Technical University named after A.N.Tupolev-KAI
Kazan, Russian Federation
K. Marx str., 10
tel: +7(843) 2310056
email: anikinigor777@mail.ru

Lilia Yu. Emaletdinova
Kazan National Research Technical University named after A.N.Tupolev-KAI
Kazan, Russian Federation
K. Marx str., 10
tel: +7(843) 2310056
email: lilia@stcline.ru

ABSTRACT
We suggested a method for quantitative information security risk management in computer networks. We used fuzzy estimations of the risk factors and quantitative risk assessment method under the safeguards. We used analytic hierarchy process for quantitative assessment of qualitative risk and cost/benefit subfactors. We used optimization tasks for selection the best set of safeguards.

Keywords
Information security, Risk management, Fuzzy logic, AHP.

1. INTRODUCTION
Modern computer networks are influenced by a large number of different threats, which can violate confidentiality, integrity or availability of the assets. It is very important to find an effective way for detection actual threats and selection adequate security controls for them. Information security risk assessment and management methods provide an effective way to realize it.

Information security risk is a function of the likelihood of a given threat-source's exercising a particular potential vulnerability, and the resulting impact of that adverse event on the organization [12]. There are two main approaches exist to estimate risk factors and evaluate risk values - quantitative approach and qualitative approach [13]. The first one is used in such methods as NIST SP 800-30 [12], OCTAVE [1], CRAMM [14] etc. It assumes estimation of the risk factors on qualitative scales. The second one is used in RiskWatch [6], ISRAM [11], FAIR [15], iRisk [7] etc. It assumes estimation of the risk factors on the quantitative interval. The major advantage of the second approach is a possibility to get more certain risk values and further use them for their optimization. Therefore the second approach is often more effective in practice. However, there are some difficulties in practical implementation of quantitative risk assessment:

– the benefits of quantitative assessments is often outweighed by the cost in terms of expert time and effort;

– statistic about some information security incidents is not often available, thereby expert judgments take a great role; experts often doesn't have precise information about risk factor values, their judgments often have inconsistent and fuzzy character;

– risk factors involve a lot of qualitative subfactors. It is difficult to estimate them by quantitative way;

– uncertainty and gaps in information about threats and vulnerabilities.

To eliminate these difficulties we use fuzzy logic [5] and analytic hierarchy process (AHP) [16]. We suggest a new method for information security risk management based on obtained quantitative risk values, fuzzy logic, AHP and cost/benefit ratio estimation for security safeguards.

2. INFORMATION SECURITY RISKS ASSESSMENT METHOD

2.1 Assets Evaluation
We consider such types of assets as information, hosts, servers, telecommunication equipment, IT-services and such properties as confidentiality, integrity and availability.

At the first step we determine the fuzzy value of information assets. We suggested the set $\{PII_i\}$ of 25 particular indicators of impact (*PII*) to evaluate their security properties [2]. The examples of these PII are technological disasters, terrorist acts, company reputation reduction, firing of specialists, cost of manual processing of queries, reducing competitiveness, direct money losses etc. Most of these PII are qualitative, thereby we use AHP and 4-level hierarchies for their quantitative evaluation. We take a group of n experts with weights δ_i. These experts analyze the hierarchy and evaluate confidentiality, integrity and availability weights for all information assets. Then we use algorithm *FZ_STAT* [4] to evaluate fuzzy values of security properties based on statistic of corresponding expert judgments.

At the second step we assess fuzzy values of confidentiality, integrity and availability for hosts and servers. We use fuzzy values from the first step to realize it. At the third step we assess availability fuzzy value for IT-services. We used AHP, fuzzy

SIN '15, September 08 - 10, 2015, Sochi, Russian Federation
 ISBN 978-1-4503-3453-2/15/09…$15.00
DOI: http://dx.doi.org/10.1145/2799979.2800022

values from the first step and graph (fault tree) which provides information about depended IT-services. Finally we assess availability fuzzy value for servers and telecommunication equipment with using fuzzy values from the third step.

We evaluate fuzzy impact level for specific threat with using fuzzy value of assets and bipartite graph to detect the set of assets, which are violated by the threat.

2.2 Threat's Exercising Possibility and Vulerability Level Evaluation

It is difficult to get quantitative values of threat's exercising possibility because statistic about incidents is not often available. Moreover, a lot of qualitative factors affect possibility value.

We suggested a method for quantitative evaluation of threat's exercising possibility, which is based on questionnaires. These questionnaires include questions Q_i about possibility factors for specific threat and some possible answers $Answer_{ij}$ for these questions. Expert selects one of the answers for every question and we assign number of points p_{ij} for choosing it. We evaluate threat's exercising possibility based on sum of the points after answering all questions. We construct 3-level hierarchy, use AHP and expert judgments to evaluate fuzzy values p_{ij} .

We proposed a method for evaluation a vulnerability exploitation fuzzy level. It is based on CVSS V2 metrics [9]. Despite the widespread use of the CVSS method, it has some disadvantages and difficulties in practice: all CVSS metrics are defined on qualitative scales and equally important, expert can't express any doubts or define fuzzy values, we can't assess vulnerability if we don't have precise information about BaseScore metrics. To eliminate these difficulties we suggested a new method based on expert judgments, fuzzy production rules and fuzzy logic.

To evaluate vulnerability level we modify fuzzy IF-THEN rules suggested in [3] and use them in following form:

Rule R^j :

IF P_1^j *is* $\widetilde{A}_1^j$ $\left(w_1^j\right)$ AND … AND $P_{s_j}^j$ *is* $\widetilde{A}_{s_j}^j$ $\left(w_{s_j}^j\right)$

THEN Vulnerability Value is $\widetilde{L}_1^j$ $\left[CF^{\,j}\right]$

Here P_i^j are the vulnerability metrics from CVSS defined as linguistic variables, $\widetilde{A}_i^j$ are the values of linguistic variables, $\widetilde{L}^j$ is the value of linguistic variable "Vulnerability Value", $w_i^j \in [0;1]$ are the weights of importance of the metric P_i^j, $CF^{\,j} \in [0;1]$ is a certainty factor for the rule R^j .

We suggested new fuzzy inference scheme to make a decisions with using new type of fuzzy IF-THEN rules. We also assess confidence degree for the result. Then we use fuzzy inference scheme and CVSS V2 metrics to develop new method for vulnerability fuzzy evaluation under the partial degree of confidence. Suggested method can also be easily used with updated metrics of CVSS 3.0. We assess risk fuzzy level for specific threat by multiplication fuzzy impact, fuzzy threat's exercising possibility and fuzzy vulnerability level (optionally).

3. QUANTITATIVE RISK ASSESSMENT METHOD UNDER THE SECURITY SAFEGUARDS

Let $T_i \in T$ be the threat and $v_j \in V$ be the vulnerability, $Poss(v_j)$ be a vulnerability fuzzy level, $Poss(T_i)$ be a threat's fuzzy exercising possibility, $Impact(T_i)$ be a fuzzy impact level from the threat T_i. Let $Risk(T_i)$ be an information security risk value associated with the threat T_i without any security countermeasures. We use information security model in computer network defined by (1)

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

Here

– Z is the full set of security safeguards;

– $R_S^V : \{Z \times V\} \to F([0;1])$, $R_S^T : \{Z \times T\} \to F([0;1])$ are the matrixes with fuzzy decreasing coefficients $\widetilde{k}, \widetilde{p} \in F([0;1])$ for vulnerability levels and threat's exercising possibilities;

– $R_S^{I-C}, R_S^{I-I}, R_S^{I-A} : \{Z \times T\} \to F([0;1])$ are the matrixes with fuzzy decreasing coefficients $\widetilde{c}^{\,C}, \widetilde{c}^{\,I}, \widetilde{c}^{\,D} \in F([0,1])$ for impact levels from the threat by confidentiality, integrity and availability.

We use expert judgments to define fuzzy coefficients.

Let $Poss(v_j)_Z$ be a vulnerability fuzzy level, $Poss(T_i)_Z$ be a threat's fuzzy exercising possibility, $Impact(T_i)_Z$ be an impact, $Risk(T_i)_Z$ be a risk level under the set of safeguards Z. We use expressions (2), (3), (4) to evaluate these values:

$$Poss(v_j)_Z = Poss(v_j)_{\{z_1\}} = Poss(v_j) \cdot \min_{z \in Z}\left(1 - R_S^V(v_j, z)\right) \tag{2}$$

$$Poss(T_i)_Z = Poss(T_i)_{\{z_2\}} = Poss(T_i) \cdot \min_{z \in Z}\left(1 - R_S^T(T_i, z)\right) \tag{3}$$

$$Impact(T_i)_Z = \widetilde{cc}(T_i)_Z + \widetilde{ci}(T_i)_Z + \widetilde{cd}(T_i)_Z \tag{4}$$

Here $z_1, z_2 \in Z$ are the safeguards with minimum value at the right part of the expressions; $\widetilde{cc}(T_i)_Z, \widetilde{ci}(T_i)_Z, \widetilde{cd}(T_i)$ are the impact levels from the threat T_i by confidentiality, integrity or availability under the set of safeguards Z. We evaluate these impacts with using expressions (5), (6), (7).

$$\widetilde{cc}(T_i)_Z = \sum_{a^j \in A^C(T_i)} \widetilde{pc}^{\,j}(T_i) \cdot \widetilde{cc}_{a^j} \cdot \left(1 - \max_{z \in Z} R_S^{I-C}(T_i, z)\right) \tag{5}$$

Here $A^C(T_i)$ is the set of the assets which are influenced by confidentiality from the threat T_i; $a^j \in A^C(T_i)$ is the asset which is influenced by confidentiality from the threat T_i; $\widetilde{cc}_{a^j}$ is the fuzzy confidentiality level of the asset a^j; $\widetilde{pc}^{\,j}(T_i)$ is the fuzzy coefficient which defines percent of confidentiality damaging of the asset a^j by the threat T_i .

$$\tilde{c}\tilde{i}(T_i)_Z = \sum_{a^j \in A^I(T_i)} \tilde{p}\tilde{i}^{\,j}(T_i) \cdot \tilde{c}\tilde{i}_{a^j} \cdot \left(1 - \max_{z \in Z} R_S^{I-I}(T_i, z)\right) \quad (6)$$

Here $A^I(T_i)$ is the set of the assets which are influenced by integrity from the threat T_i; $\tilde{c}\tilde{i}_{a^j}$ is the fuzzy integrity level of the asset a^j; $\tilde{p}\tilde{i}^{\,j}(T_i)$ is the fuzzy coefficient which defines percent of integrity damaging of the asset a^j by the threat T_i.

$$\tilde{c}\tilde{d}(T_i)_Z = \sum_{a^j \in A^A(T_i)} \tilde{p}\tilde{a}^{\,j}(T_i) \cdot \tilde{c}\tilde{a}_{a^j} \cdot \left(1 - \max_{z \in Z} R_S^{I-A}(T_i, z)\right) \quad (7)$$

Here $A^A(T_i)$ is the set of the assets which are influenced by availability from the threat T_i; $\tilde{c}\tilde{a}_{a^j}$ is the fuzzy availability level of the asset a^j; $\tilde{p}\tilde{a}^{\,j}(T_i)$ is the fuzzy coefficient which defines percent of availability damaging of the asset a^j by the threat T_i.

Finally we evaluate information security risk value $Risk(T)_Z$ under the set of safeguards Z with using two or three factors.

4. COST/BENEFIT RATIO ESTIMATION FOR SECURITY SAFEGUARDS

We evaluate efficiency of security safeguards through the cost/benefit ratio estimation [8,10]. We use expression (8) to estimate this ratio for the safeguard $z_i \in Z$.

$$K(z_i) = \frac{Benefit(z_i) - F\_Costs(z_i)}{LS\_Costs(z_i)} \quad (8)$$

Here $Benefit(z_i)$ are benefits for the safeguard $z_i \in Z$; $F\_Costs(z_i)$ are fixed costs for the safeguard $z_i \in Z$; $LS\_Costs(z_i)$ are lump-sum costs for the safeguard $z_i \in Z$.

We evaluate $Benefit(z_i)$ with using expression (9).

$$Benefit(z_i) = \Delta R = Risk(T) - Risk(T)_{\{z_i\}} \quad (9)$$

Here $Risk(T) = \sum_j Risk(T_j)$ is the fuzzy risk value for all threats; $Risk(T)_{\{z_i\}} = \sum_j Risk(T_j)_{\{z_i\}}$ is the fuzzy risk value for all threats under the security safeguard $z_i \in Z$.

We also can use the expression (10) for cost/benefit estimation if $Benefit(z_i) - F\_Costs(z_i)$ much more than $LS\_Costs(z_i)$.

$$K(z_i) = Benefit(z_i) - F\_Costs(z_i) \quad (10)$$

We assess $LS\_Costs(z_i)$ as a fuzzy number with using expert judgments. We assess $F\_Costs(z_i)$ as a fuzzy number with using AHP and 8 partial cost indicators (PCI): Personnel's salary, Personnel's training, License extension, Bad interface, Unproductive user's work, Number of staff, Requirements for processing power, Idle time. Safeguard z_1 is more efficient than safeguard z_2 if $K(z_1) > K(z_2)$.

5. INFORMATION SECURITY RISK MANAGEMENT

Let $Z = \{z_i\}_{i=1,M}$ be the set with all possible safeguards, $Z' \subseteq Z$ be the set of safeguards which have been selected for implementation in computer network. For each set $Z' \subseteq Z$ we consider the vector $X = (x_1, \ldots, x_M)$, where $x_i = 1$ if corresponding safeguard $z_i \in Z$ has been selected for implementation and $x_i = 0$ if corresponding safeguard $z_i \in Z$ has not been selected.

Let's denote $K(x_1, \ldots, x_M) = \sum_{i=1}^{M} K_i$, where $K_i = K(z_i)$ if $x_i = 1$ and $K_i = 0$ if $x_i = 0$. Let's denote $Risk(T, x_1, \ldots, x_M) = Risk(T)_{Z'}$. Let $LS\_Costs(x_1, \ldots, x_M)$ be a lump-sum costs for the set of security safeguards Z'. We realize information security risk management by deciding optimization task (11). We need to find a vector $X = (x_1, \ldots, x_M)$ such as

$$\begin{cases} K(x_1, \ldots, x_M) \to \max \\ Risk(T, x_1, \ldots, x_M) \le Risk^t \\ x_i \in \{0,1\} \end{cases} \quad (11)$$

Here $Risk^t$ is a threshold level of information security risk acceptable for the company.

6. EXPERIMENTAL RESULTS

We developed the software for risk assessment/management and made an experiences in computer network of KNRTU-KAI university. We considered 51 information assets, 10 groups of hosts, 3 servers, 4 units of telecommunication equipment, 13 IT-services. Table 1 includes the results of risk assessment for virus infection threats in some departments. We evaluated risks with using two factors approach, got an impact and threat's exercising possibility with using methods discussed in the Sections 2.1, 2.2.

Table 1. Some results of risk assessment

Threat	Impact ($)	Exercising possibility	Risk level ($)
Virus infection for the host in HR Department	$\overline{3055}$	$\overline{0.61}$	$\overline{1864}$
Virus infection for the host in Accounting Department	$\overline{16300}$	$\overline{0.61}$	$\overline{9943}$
Virus infection for the host in the Selection Committee Department	$\overline{7199}$	$\overline{0.61}$	$\overline{4391}$

Then we used cost/benefit ratio estimation with using AHP to find the best antivirus. We considered Kaspersky Endpoint Security, Dr.Web Enterprise Suite, Symantec Protection Enterprise Edition, ESET Endpoint Antivirus, Panda Security for Business and Avast! Enpoint Protection. The results of cost/benefit estimation with using expression (10) is presented in the Table 2.

Table 2. Results of cost/benefit ratio estimation

Antivirus	ΔR	F_Costs	LS_Costs	$K(z_i)$
Kaspersky Endpoint Security	16198	94.2	21	16104
Dr. Web Enterprise Suite	16198	169.56	103.6	160028
Symantec Protection Suite Small Business Edition	16198	103.62	18.4	160094
ESET Endpoint Antivirus	16198	160.14	39.3	160038
Panda Security for Business	16198	207.24	19.3	15991
Avast! Endpoint Protection	16198	207.24	16.65	15991

We can claim that Kaspersky Endpoint Security is the best decision for our situation. Moreover, this decision gives us the benefit 682$ in a year (for 100 hosts) in comparing with the second rating decision "Symantec Protection Suite Small Business Edition".

7. CONCLUSION

Information security quantitative risk assessment and management as well as cost/benefit ratio estimation in computer networks is a very controversial and difficult area due to many practical challenges. The main of them are: qualitative character of various costs (also including risk) and benefits subfactors; uncertainty, fuzziness, imprecise and gaps in information about threats and vulnerabilities.

Using AHP allows us involve qualitative subfactors into quantitative risk and cost/benefit estimation processes, whereas fuzzy logic and fuzzy inference scheme (Section 2.2) allow us overcome uncertainty, fuzziness, imprecise and gaps in the background information. It makes qualitative risk management process easier under considered challenges.

8. REFERENCES

[1] Alberts, C., Dorofee, A. 2002. Managing information security risks. The OCTAVE[SM] approach. Addison Wesley. pp 512.

[2] Anikin, I. 2014. Information Security Risks Assessment Method Based on AHP and Fuzzy Sets. In *Proceedings of 2nd Intl' Conference on Advanced in Engineering Sciences and Applied Mathematics (ICAESAM'2014)*, May 4-5, 2014 Istanbul (Turkey), pp. 11-15. DOI= http://dx.doi.org/10.15242/IIE.E0514043.

[3] Anikin, I. 2014. Knowledge Representation Model and Decision Support System for Enhanced Oil Recovery Methods. In *Proceedings of Intl' conference on Intelligent Systems, Data Mining and Information Technology (ICIDIT'2014)*, April 21-22, 2014 Bangkok (Thailand), pp. 101-105. DOI= http://dx.doi.org/10.15242/IIE.E0414004.

[4] Anikin, I. 2015. Vulnerability Risk Assessment Method Based on Fuzzy Logic. In *Proceedings of the 2nd National Conference on Information Technology and Computer Science (CITCS 2015)*, 2015, Shanghai, March 21-22, pp. 1554-1560.

[5] Anikin, I.V., Gilmullin, T.M. 2013. The Method and Fuzzy Expert System for Information Security Risk Assessment and Management. In *Varia Informatica*. 2013. Lublin: PIPS Polish Information Processing Society, 2013. – pp. 55-68.

[6] Behnia, A., Rashid, R.A., Chaudhry, J.A. 2012. A Survey of Information Security Risk Analysis Methods. *Smart Computing Review*, vol. 2, № 1, 2012, pp. 79-94. DOI= http://dx.doi.org/10.6029/smartcr.2012.01.007

[7] Clymer, C., Stasiak, K., Neely, M., Marchewitz, S., iRisk Ecaluation. *SecureState Whitepaper*. https//www.securestate.com

[8] Conkling, W.R., Hamilton, Jr, J.A.D. 2008. The importance of information security spending: An economic approach. In *Proceedings of the 2008 Spring Simulation Multiconference, SpringSim'08*. 2008. Pages 293-300.

[9] CVSS V.2.0. A Complete Guide to the Common Vulnerability Scoring System. http://www.first.org/cvss/cvss-guide.pdf.

[10] Kanungo, S., Jain, V., Forman, E.H. 2011. Maximizing resource allocation effectiveness for IT security investments. *International Journal of Business Information Systems*. Volume 7, Issue 2, February 2011, Pages 166-180.

[11] Karabacaka, B., Sogukpinar, I. ISRAM: information security risk analysis method. *Computers app. Security*, vol. 24, pp. 147-159, 2005.

[12] NIST SP 800-30 Revision 1. 2012. Guide for Conducting Risk Assessments (September 2012).

[13] Peltier, T.R. 2010. Information Security Risk Analysis, third ed. Auerbach Publications. 2010. 456 pp.

[14] PRINCE User's Guide to CRAMM. Stationery Office Books, 1993. 140 pp.

[15] Risk Management Insight LLC. FAIR (FACTOR ANALYSIS OF INFORMATION RISK) *Basic Risk Assessment Guide*. Risk Management Insight LLC, 2006.

[16] Saaty, T.L. 2001. Decision Making for Leaders: The Analytic Hierarchy Process for Decisions in a Complex World. 3rd Revised edition. RWS Publications. 2001. 323 pp.