Development of secure software

Valentina Petrova
Nikola Vaptsarov Naval Academy, Varna, Bulgaria
vmb75bg@gmail.com

Abstract: *The main goal of this paper is to present methods and tools for secure software development. The process of creating secure software involves analysis, design and implementation based on multi criteria decision making risk assessment. The results of this study give readers some proposals how to produce secure software systems and conduct cost-benefit analysis.*
Keywords*: Fuzzy AHP, MULTI-CRITERIA DECISION MAKING (MCDA)*

1. Introduction

Several research studies have been presented in literature for analysing and classifying the ways for assessing software security [16]. The gap between research proposals and actual practices that appear due to this is difficult to bridge completely. The main purpose of this study is to secure systems from malicious attacks. It is achieved through identification, authentication, information assurance availability, integrity, confidentiality, analyses, and their assessment.

The assessment of software security is a decision-making problem. The author of this paper proposes Fuzzy Analytic Hierarchy Process (Fuzzy AHP) for developing security systems.

Information security assessments include following triad: confidentiality, integrity and availability (CIA triad). The confidentiality, integrity and availability are fundamental principles for software security. Security developers apply each requirement when analyzing how to protect information systems. Confidentiality refers to the allowance of authorized access to sensitive and secure data [1]. Integrity is a quality of appeal established by the ethical assurance and resolution. Availability, in the context of a computer system, refers to the ability of a user to access information or resources for a specified duration [1].

P.L. Gorski and L.L. Iacono propose a critical review based on security of software [7].

Yasser M. Hausaw provide a framework for integrating and assessing security during software development life cycle [9].

Security software is concerned with whether a system can survive accidental or intentional attacks on it from outside. One of the most important problems in security software is the multi-criteria assessment of the security efficiency. A valuable approach to evaluating and predicting the security of a system is Fuzzy Analytic Hierarchy Process (Fuzzy AHP). The state of the software application is considered from attaker's point of view. It is useful to include expenses as a factor of the evaluation of security. The author presents fuzzy multi-criteria decision making theory to assess the system security characteristics and alternatives.

Software security is concerned with whether software applications can survive cyber attacks and unauthorized access on it from outside.

System measures can be computed as solutions to programming problems. Programming computations become impracticable when a number of components in the system is large[2,3,10].

For computing total loses, probabilities of various type of attacks or their possibilities have to be known. In presented paper, the author applies the probability theory for computing the security measures.

2. Security risk

The risk dimension to capital budgeting of software solutions is a crucial factor in the valuation of assess. Acceptance of a profitable but highly risky investment proposal in software systems may increase the perceived riskiness of the software and result in an actual reduction in the value of the security. Nowhere is the gap between theory and practice wider than in the area of risk analysis.

This paper considers the important method to the analysis and assessment of software risk within the multi criteria decision technique and a description of the main statistical methods for measuring security risk within multi-period. It commences by defining the various forms of risk discussed in this paper and examining experts' attitudes towards risk. These fall conveniently into methods intended to describe or highlight risk and methods incorporating security riskiness within the programming code in software applications. The paper concludes by examining the extent to which the methods discussed are found in programming languages C++, Python, and Java.

Perfect certainty arises when expectations are single-valued, that is, a particular outcome will arise rather than a range of outcomes. Some investments come fairly close to a certain investment.

Risk and uncertainty are not synonymous. Risk refers to the set of unique consequences for a given decision which can be assigned probabilities, while uncertainty implies that it is not possible to assign probabilities.

For most investment software decisions, empirical evidence is hard to find. The decision makers utilise subjective probabilities where objective statistical evidence is not available. They can subjectively assess the software risks involved based on the available information about the success of a software development projects.

Because subjective probabilities may be applied to investment decisions in a manner similar to objective probabilities, the distinction between risk and uncertainty is not crucial, in practice, and the two are often used interchangeably.

The software security assessment is presented to analyze capabilities of software based on a tool proposed by the author of the paper. In order to make multi-criteria decisions, all these measures are combined. A method includes a wide variety of kinds of uncertainty.

Risk identification and assessment is a crucial element of software security analysis.

3. A multi-criteria decision-making method

The assessment of risk associated with software security comprises attacks come through vulnerabilities in the code, and threats that software applications faces. Criteria common to information security assessment have been identified and proposed in a Multi-Criteria Decision Making (MCDA) method.

Risk assessment of information security is an essential part of development of secure systems.

It is important to recognize the distinction between the prediction of likely events and the course of action that may stem from such prediction. Different options gives rise to different considerations and qualitative assessments. Relevant and useful information is central in predicting the degree of risk surrounding future events and in selecting the best investment software options.

The problem of security of information systems and its solving takes considerable effort.

The author of the paper uses the fuzzy method working with triangular fuzzy elements described by Prof. Ramík [14, 15, 16, 27].

The FuzzyAHP is used to evaluate elements for decision-making under risk to predict the outcomes. The end result will be efficient to solve the problem presented through the tool.

The AHP realises the evaluation process connected with the Multiple-criteria decision-making under risk. The study proposes a new method for a risk assessment of software development.

The qualitative and qualitative criteria for risk events and scenarios are used as preliminary lists for calculating the triangular fuzzy evaluations and the risk assessment.

The weights of the criteria determine the relative importance extracted from interviews with decision makers and risk analysis experts. Therefore, with adjustments they can serve as risk indicators for other multi-criteria decision making studies.

The statistic information is beneficial to propose sensitivity analysis, and come up with a solution. They can be compared with results obtained from other decision makers in different assumptions of risk assessment [11,12,13].

University lecturers can use the proposed method to teach and explain the FAHP technique for risk assessment in various studies for software security.

The experts propose their choices in form of triangular fuzzy elements in a pair-wise comparison matrix. In order to derive the weights from a matrix and to calculate the consistency of the information on decision maker's preferences, the pair-wise comparison matrixes with triangular fuzzy elements are used.

The author of the paper implements the approach described by Ram´ık [16]. The mathematical theory described in this paper has been implemented into a software tool.

The Fuzzy AHP (FAHP) method ranking elements includes the following steps:

Step 1: The author of the paper proposes the eight criteria presented in figure 1 named attacks, vulnerabilities, penetration testing, threats, assets, security measures, unauthorized access, and security alerts.

The weights of criteria of the pair-wise comparison matrix are expressed by triangular fuzzy elements. It can be problematic for the decision makers to compare certain pairs of criteria. In these cases, the experts use the data not only in form of real numbers, but also fuzzy numbers.

Fig. 1 *Define criteria*

Step 2: The list of alternatives that are estimated are Java, Python, and C++.

Step 3: Contain the decision makers (experts).

The experts of the software security play crucial roles for discovering, analyzing, and responding to security problems. They maintain and preserve software from security vulnerabilities, threats, and risks.

The assessment is performed by decision makers (experts). The expert measures the importance of the criteria.

Step 4: Propose the scenarios

Scenarios 1: A flexible model – It is includes structured language, strict syntactic rules, no errors, simplicity etc. Modules are expanded and have scripting possibilities that can be supplemented in other software systems.

Scenarios 2: Useful Libraries

The security library are utilized by researchers and ethical hackers.

Scenarios 3: Clear Syntax

The clear syntax contributes cyber security professionals to quickly specify and improve programming code and to find errors in the software.

Scenarios 4: Increase capacity and functionalities of software possibilities based on security demand. The programming code must be suitable for testing and maintenance.

Scenarios 5: Adjusting to overhauls, new resources, deconstructions and upgrades.

Upgrading security features integrate other possibilities to improve and increase software usability.

All scenarios are united to reply to security challenges and to prevent from future vulnerabilities and threats. They are presented in figure 2.

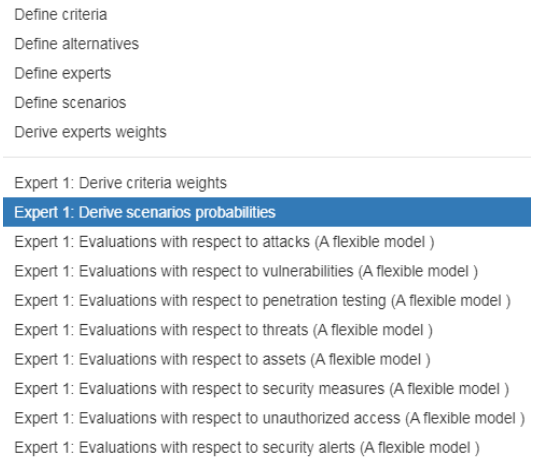

Fig. 2 *Define scenarios*

Step 5: Elements of the matrixes are set. The fuzzy weights are appear. The NI index is calculated. The result is presented in a graph.

A matrix $\tilde{A}$ is of the following form:

$$\tilde{A} = \begin{bmatrix} (a_{11}^L, a_{11}^M, a_{11}^U) & \cdots & (a_{1n}^L, a_{1n}^M, a_{1n}^U) \\ \vdots & \ddots & \vdots \\ (a_{n1}^L, a_{n1}^M, a_{n1}^U) & \cdots & (a_{nn}^L, a_{nn}^M, a_{nn}^U) \end{bmatrix}$$

where for all i. j =1,…,n:

$a_{ij}^L, a_{ij}^M, a_{ij}^U$, are real numbers such that $1/\sigma \le a_{ij}^L \le a_{ij}^M \le a_{ij}^U \le \sigma$ for a chosen fixed $\sigma > 1$. $\tilde{a}_{ij} = \tilde{a}_{ij} = (a_{ij}^L, a_{ij}^M, a_{ij}^U)$ implies that $\tilde{a}_{ji} = \frac{1}{a_{ij}^U}, \frac{1}{a_{ij}^M}, \frac{1}{a_{ij}^L}$. (reciprocity)

$\tilde{A}$ is an n×n matrix with triangular fuzzy elements. The matrix $\tilde{A}$ is reciprocal, if the following condition is satisfied: $\tilde{a}_{ij}=(a_{ij}^L, a_{ij}^M, a_{ij}^U)$ implies that $\tilde{a}_{ji} = \frac{1}{a_{ij}^U}, \frac{1}{a_{ij}^M}, \frac{1}{a_{ij}^L}$, (reciprocity) for all i,j = 1,2,...,n, i.e.:

$$\tilde{A} = \begin{bmatrix} 1,1,1) & \cdots & (a_{1n}^L, a_{1n}^M, a_{1n}^U) \\ \vdots & \ddots & \vdots \\ \left(\frac{1}{a_{ij}^U}, \frac{1}{a_{ij}^M}, \frac{1}{a_{ij}^L}\right) & \cdots & 1,1,1) \end{bmatrix}$$

where $0 \le a_{ij}^L \le a_{ij}^M \le a_{ij}^U, i,j = 1,2,\dots,n.$

The fuzzy weights $\widetilde{w_k} = \left(w_k^L, w_k^M, w_k^U\right)$, k=1,…,n, are then derived in this procedure as follows [14,15,16,27]:

$$w_k^L = C_{min} \cdot \frac{\left(\prod_{j=1}^n a_{kj}^L\right)^{1/n}}{\sum_{i=1}^n \left(\prod_{j=1}^n a_{ij}^M\right)^{1/n}}, \text{where } C_{min} = \min_{i=1,\dots,n} \left\{ \frac{\left(\prod_{j=1}^n a_{ij}^M\right)^{1/n}}{\left(\prod_{j=1}^n a_{ij}^L\right)^{1/n}} \right\}$$

.

$$w_k^M = \frac{\left(\prod_{j=1}^n a_{kj}^L\right)^{1/n}}{\sum_{i=1}^n \left(\prod_{j=1}^n a_{ij}^M\right)^{1/n}},$$

$$w_k^U = C_{max} \cdot \frac{\left(\prod_{j=1}^n a_{kj}^U\right)^{1/n}}{\sum_{i=1}^n \left(\prod_{j=1}^n a_{ij}^M\right)^{1/n}}, \text{where } C_{max} = \min_{i=1,\dots,n} \left\{ \frac{\left(\prod_{j=1}^n a_{ij}^M\right)^{1/n}}{\left(\prod_{j=1}^n a_{ij}^U\right)^{1/n}} \right\}$$

.

To measure the consistency of the pair-wise comparison matrix with triangular fuzzy elements, Ram´ık proposed the following index [14, 15, 16, 27]:

$$NI_n^{\sigma}(\tilde{A}) = \gamma_n^{\sigma} \cdot \max_{i,j} \left\{ max \left\{ \left| \frac{w_i^L}{w_j^U} - a_{ij}^L \right|, \left| \frac{w_i^M}{w_j^M} - a_{ij}^M \right|, \left| \frac{w_i^U}{w_j^L} - a_{ij}^U \right| \right\} \right\}$$

,

where

$$\gamma_n^{\sigma} = \begin{cases} \dfrac{1}{max\left\{\sigma - \sigma^{(2-2n/n)}, \sigma^2 \left(\left(\frac{2}{n}\right)^{\frac{2}{n-2}} - \left(\frac{2}{n}\right)^{\frac{2}{n-2}} \right)\right\}} \\ if\ \sigma < \left(\frac{n}{2}\right)^{n/(n-2)}, \\ \dfrac{1}{max\{\sigma - \sigma^{(2-2n/n)}, \sigma^{(2n-2/n)} - \sigma\}} \ otherwise. \end{cases}$$

The value of the index ranges from 0 to 1, where 0 means that the matrix is fully consistent.

Step 5.1: a pair-wise comparison decision-making matrixes with triangular fuzzy elements are constructed. The experts determine the weights of the elements above the main diagonal. The decision makers propose each triangular fuzzy element as three numbers, divided by a space. The triangular fuzzy elements are proposed by multiple experts in figure 3(the assessments of Expert 2).

Step 5.2: The results estimated from the pair-wise comparison matrix are displayed in form of a graph. The derived fuzzy weights are presented and then the consistency through the NI index is calculated. They are presented in Figure 4.

The MCDM technique derives fuzzy weights from a matrix and then measures the inconsistency of the suggestions provided by the decision makers.

Fig. 3 *Define scenarios with the assessments of expert 2*

The assessment of criteria is done by multiple experts in figure 4.

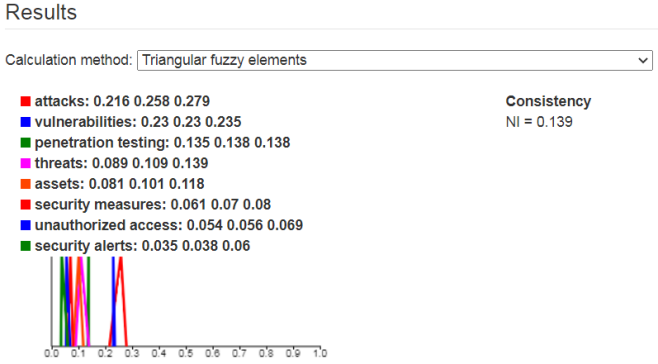

Fig. 4 *The assessment of criteria*

Various scenarios (states of the world) are proposed together with their probabilities and results in figure 5.

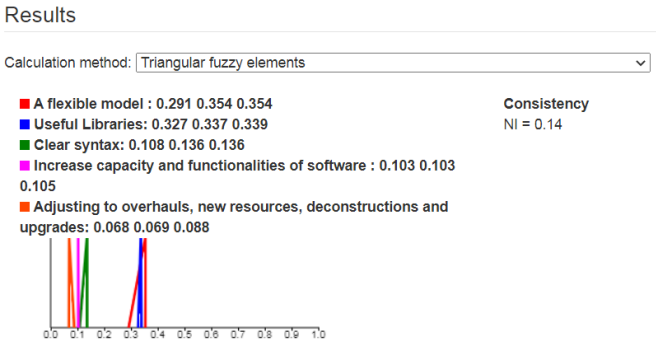

Fig. 5 *Assessment of scenarios*

The alternatives are then estimated for each of the scenarios.

6. Viewing the results

The resulting overall assessments are calculated for each of the experts. When all pair-wise comparison matrices are made, the resulting overall assessments of the elements can be considered. The resulting assessments of the alternatives are presented for each of the experts in figure 6.

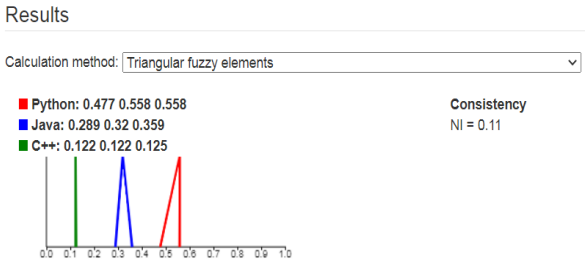

***Fig. 6** Assessment of scenarios*

The developer of software need to be aware of the vulnerabilities in the used programming language and execute secure code. Secure programming is accepted to be practice to minimize the risk from cyber attacks. Specific security scenarios that must be used by a programmer to minimize security programming gaps are proposed.

The method is utilized to assess security capability of three languages: Java, Python, and C++. The results show that C++ programming language has the lowest security features. Python has high-security capability.

The method for security software presented in this paper can be applied by programmers and software security developers for measuring the level of security capability of used programming languages, and mitigate vulnerabilities and attacks on software applications.

4. Conclusion

A review of security risk methods is provided in this report, including Multi-Criteria Decision Making (MCDA) approaches. A security risk assessment technique based on the AHP fuzzy method is proposed.

This paper applies the probability theory for computing security measures of systems and to generalize the probabilistic security methods. From the presented results, it is concludes that the obtained security assessments are non-trivial and intuitively explainable. The security of the system is analyzed with information about the probability distributions of attack, of costs, etc.

5. References

1. Agrawal, Manish, Alex Campoe, and Eric Pierce. *Information Security and IT Risk Management*. Hoboken, N.J: John Wiley and Sons, Inc, 2014.

2. Andreev, E., M. Nikolova, and V. Radeva. "Educational NASA Project: Artificial Intelligence and Cybersecurity at a Mobile Lunar Base." Information & Security: An International Journal 46, no. 3 (2020): 321-333,https://doi.org/10.11610/isij.4624

3. Andreev, E., Radeva, V., Nikolova, M., 2021, Cybersecurity of information in space telemedicine, CEMA'21 conference, Athens, Greece, pp. 54-57, ISSN: 1314-2100

4. Biener, C. ,M. Eling, and J. H. Wirfs, "Insurability of cyber risk: an empirical analysis," The Geneva Papers on Risk and Insurance—Issues and Practice, vol. 40, no. 1, pp. 131–158, 2015.

5. Chockalingam, S.; Hadžiosmanovic', D.; Pieters, W.; Teixeira, A.; van Gelder, P. Integrated safety and Security risk assessment methods: A survey of key characteristics and applications. In International Conference on Critical Information Infrastructures Security; Springer: Cham, Switzerland, 2016; pp. 50–62.

6. Dey P.., Managing project risk using combined analytic hierarchy process and risk map., Applied Soft Computing 10 (2010) 990–1000. doi:10.1016/j.asoc.2010.03.010.

7. Gorski, Peter & Lo Iacono, Luigi & Wiefling, Stephan & Möller, Sebastian. (2018). Warn if Secure or How to Deal with Security by Default in Software Development?.

8. Holeček P., Talašová, J.: A free software tool implementing the fuzzy AHP method, Proceedings of the 34th International Conference on Mathematical Methods in Economics 2016, Liberec, Czech Republic, p. 266 – 271, ISBN 978-80-7494-296-9.

9. Hausawi, Y.M., & Allen, W.H. (2015). Usable-Security Evaluation. *HCI*.

10. Koleva, E., Lefterova, M., Nikolova, M., Automated information system for evaluation the stability of the ship, Communication, Electromagnetics and Medical Application, 2018-October, pp. 22-26. ISSN: 1314-2100, https://www.scopus.com/inward/record.uri?eid=2-s2.0-85056254582&partnerID=40&md5=c56c1e2b795745e8b8772f60d991d802

11. Petrova V., Using the Analytic Hierarchy Process for LMS selection, CompSysTech '19: 20th International Conference on Computer Systems and Technologies, June 2019, Ruse, Bulgaria, Pages 332–336, ISBN: 978-1-4503-7149-0.

12. Petrova V., The Hierarchical Decision Model of cybersecurity risk assessment., 12th National Conference with International Participation "Electronica 2021", May 27 - 28, 2021, Sofia, Bulgaria.

13. Petrova V., A cybersecurity risk assessment, SOCIETY & "INDUSTRY 4.0", Vol. 6 (2021), Issue 1, pg(s) 37-40.

14. Ram´ık, J., and Korviny, P.: Inconsistency of pair-wise comparison matrix with fuzzy elements based on geometric mean. Fuzzy Sets and Systems 161, 11 (2010), 1604–1613.

15. Ram´ık, J., and Perzina, R.: Solving decision problems with dependent criteria by new fuzzy multicriteria method in Excel. Journal of Business and Management 3, 4 (2014), 1–16.

16. Ruoti, Scott & Roberts, Brent & Seamons, Kent. (2015). Authentication Melee: A Usability Analysis of Seven Web Authentication Systems. 916-926. 10.1145/2736277.2741683.

17. Saaty, T.L., 1980. The Analytic Hierarchy Process. McGraw-Hill, New York.

18. Saaty T., Theory and Applications of the Analytic Network Process, RWS Publications, 2005.

19. Saaty T., L. Vargas, Models, methods, concepts, and application of the analytic hierarchy process, New York: Springer, 2012.

20. Santini, S., G. Gottardi, M. Baldi, F. Chiaraluce., A Data-Driven Approach to Cyber Risk Assessment. Data-Driven Cybersecurity, 2019.

21. Sum, R., Risk Prioritisation Using The Analytic Hierarchy Process. Innovation and Analytics Conference and Exhibition (IACE 2015)AIP Conf. Proc. 1691, 030028-1–030028-8; doi: 10.1063/1.4937047.

22. Tubis A., Sylwia Werbinska-Wojciechowska, Mateusz Góralczyk, Adam Wróblewski and Bartłomiej Zietek, Cyber-Attacks Risk Analysis Method for Different Levels of Automation of Mining Processes in Mines Based on Fuzzy Theory Use. Sensors 2020, 20, 7210;

23. Tuma, K.; Çalikli, G.; Scandariato, R. Threat analysis of software systems: A systematic literature review. J. Syst. Softw. 2018, 144, 275–294.

24. Ugur Aksu M., M. Hadi Dilek, E. Islam Tatli et al., "A quantitative CVSS-based cyber security risk assessment methodology for IT systems," in Proceedings of the 2017 International Carnahan Conference on Security Technology, pp. 1–8, ICCST, Madrid, Spain, October 2017.

25. PN-ISO 31000:2018-08: Risk Management—Principles and Guidelines; Technical Committee ISO/TC 262. Available online: https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:en

26. PKN-ISO Guide 73:2012L Risk Management—Terminology; Polish Committee for Standardization. Available online: https://infostore.saiglobal.com/en-us/standards/pkn-iso-guide-73-2012-948094_saig_pkn_ pkn_2229185/.

27. http://fuzzymcdm.upol.cz/FuzzyAHP/Information/FuzzyAHP_user_guide.pdf