International Journal of Information Processing, 7(4), 76-86, 2013
ISSN : 0973-8215
IK International Publishing House Pvt. Ltd., New Delhi, India

Qualitative and Quantitative Evaluation: Measuring Effectiveness of Security Activities

Sonia[a], Archana Singhal[b]

[a]Department of Computer Science, University of Delhi, Research Scholar, Delhi, India,
Contact: soniacsit@yahoo.com

[b]Department of Computer Science, University of Delhi, IP College for Women, Delhi, India,
Contact: singhal_archana@yahoo.com

The ongoing journey of secure software development process since the creation of security discipline has been marked with the advent of different security activities. Although each activity has its context and cognoscenti, developers often face the difficulty of choosing one activity over other as each activity has some pros and cons. To ease up the task of selecting security activity for decision makers in this paper we first suggest an approach that performs meaningful measurement providing effectiveness of security activity qualitatively. The MOD analysis (Mission Objective Driver Analysis) presents the systematic analysis and provides base for measuring security activity effectiveness. In the next section we provide a quantitative approach for measuring effectiveness of security activities in terms of its Risk Removal Efficiency Factor (RREF). Here, we have considered security activities of CLASP (Comprehensive, Lightweight Application Security Process) software development process. In order to complement the theoretical discussions, the results of applying proposed approach on some security activities confirm findings of the theoretical study.

Keywords: CLASP Process, Effectiveness Measure, MOD Analysis, Risk Removal Efficiency Factor, Security Activity.

1. INTRODUCTION

Software security has to be defined, measured and studied and even experienced in project development. As a security activity has many dimensions, it has to be looked through a variety of factors including its effectiveness during integration with system software. Developers ability to decide about integration of security activities from a set of activities starts and ends with his perception of the effectiveness of security activities. Therefore the goal of this paper is to measure effectiveness of security activities for secure software development process qualitatively and quantitatively. We have already presented qualitative analysis as our previous research work in [1]. In this best possible activity is selected from the pool of security activities at the time of integration. By effectiveness of security activities we mean that the considered activity will produce the intended result and shows its impression in achieving security of software system. The foundation of our qualitative approach is kept on MOD analysis suggested in [2]. It describes a way for conducting systematic analysis of interactively complex software reliance system.

Proposed approach first identifies the set of factors, called drivers used to measure effectiveness in relation to its mission and objectives. After considering CLASP security activities as drivers we have framed an associated question related to each driver individually. To answer each driver question certain key aspects are considered, named as considerations. Then driver is analyzed on five-point scale, assisting developers to incorporate different levels of probability in their response. Furthermore, rationale with the consideration is shown using which analyst can describe the reason for choosing particular response. Response speci-

Table 3
Result Interpretation of One Tail T- Test

Probability of Type I error	**0.05 to 0.01**	**0.01 to 0.0025**	**0.0025 to 0.0005**
Equivalent Confidence Level	95% to < 99%	99% to < 99.75%	99.75% to 99.95%
Effectiveness in terms of Risk Removal Efficiency	Effective	Very Effective	Extremely Effective

Table 4
Combined Evaluation Results

Sr. No.	**Security Activities**	**1**	**2**	**3**	**4**	**5**	**Others**	**Total Responses**	**Mean**	**Median**	**Variance**
1	Specify Operational Environment	2	10	20	11	3	7	46	3.0	3.0	0.9
2	Detail Misuse Cases	3	12	14	8	6	4	43	3.0	3.0	0.01
3	Identify Global Security Policy	2	4	14	2	2	6	24	2.9	3.0	1.0
4	Identify User Roles and Trust Boundaries	1	3	22	12	2	13	40	3.3	3.0	0.5
5	Identify User Roles and Resource Capabilities	2	9	8	20	2	8	41	3.3	4.0	1.1
6	Document Security-Relevant Requirements	6	9	5	22	12	11	54	3.5	4.0	1.7

nity in measuring the effectiveness of each security activity separately. For measuring effectiveness, first of all we have determined objective of analysis and then factors affecting that objective. For qualitative implementation security activities have been considered as factors, as they affect the software security in a significant manner. Afterwards, for each security activity we create certain considerations to be assessed for reaching to a conclusion.

Finally, decision or effectiveness of a security activity is given in the form of response by analyst after analyzing considerations and specifying rationale or reasons behind the response. We have also measured here security activities quantitatively in terms of their risk removal efficiency using hypothesis testing. This paper concludes that measuring effectiveness of security activity will further assist decision maker by providing guidelines to select security activity which could be more beneficial to integrate with the development process. Empirical evidence based on interview conducted and supporting literature validates our approach. The main aim of our research is to develop a structured framework for addressing security issues during software development. Present approach assists us in fulfilling this aim by providing an inevitable step for overall secure development process. In future this approach must be extended by adding more aspects in measurement. Also we look to incorporate other factors useful for building a secure software system.

REFERENCES

1. Sonia, Archana Singhal. An Evaluation Approach: Measuring Effectiveness of Security Activities. *in Proceedings of Seventh International Conference on Data mining and Warehousing (ICDMW)*, Elsevier 2013.

2. Alberts C, Allen J and Stoddard R. Integrated Measurement and Analysis Framework for Software Security, *Software Engineering Institute, Carnegie Mellon University*, 2010.
3. Al-Ahmad W. Building Secure Software using XP, *In International Journal of Secure Software Engineering (IJSSE)*, 2(3), 2011.
4. Sonia and Singhal A. Integration Analysis of Security Activities from the Perspective of Agility, *in Proceedings of International Conference on Agile and Lean software methods (AI 2012)*, FEBRUARY 17 -19, Bengaluru, India, 2012.
5. Ayalew Eyader T, Kidne Abreham T. Identification and Evaluation of Security Activities in Agile Projects: A Systematic Literature Review and Survey study, *Blekinge Institute of Technology*, September 2012.
6. Misuse cases: Build Security, In https://buildsecurityin.uscert.gov/bsi/articles/bestpractices/requirements/548BSI.html
7. Sindre G and Opdahl A L. Eliciting Security Requirements by Misuse Cases, *in Proceedings of the 37th International Conference on Technology of Object-Oriented Languages and Systems*, Sydney, Australia, pages 120–131, 2000.
8. Alberts C, Allen J and Stoddard R. Risk-Based Measurement and Analysis: Application to Software Security, *Software Engineering Institute, Carnegie Mellon University*, 2012.
9. Butler S. Security Attribute Evaluation Method: A Cost-Benefit Approach, *in Proceedings of the 24th International Conference on SoftwareEngineering*, Orlando, Florida, USA, May 19 - 25, pages 232–241, 2002.
10. Bartol N and Hamilton B A. Practical Measurement Framework for Software Assurance and Information Security, *Practical Software and Systems Measurement Support Center*, 2008. http://www.psmsc.com/Prod_TechPapers.asp
11. OWASP, CLASP Security Process, https://www.owasp.org/index.php/Category:OWASP_CLASP_Project, 2006
12. Jalote P. An Integrated Approach To Software Engineering, *Narosa Publishing House*, Second Edition.
13. Win B D, Scandariato R, Buyens K, Grgoire J and Joosen W. On the Secure Software Development Process: CLASP, SDL and touchpoints compared. *In Information and Software Technology*, Elsevier, 51(7), July 2009.
14. Baca D and Carlsson B. Agile Development with Security Engineering Activities, *in Proceedings of the 2011 International Conference on Software and Systems Process ICSSP*, pages 149–158, ACM New York, USA, 2011.
15. Heikka J andSiponen M T. Abuse Cases Revised: An Action Research Experience PACIS 2006.
16. Mead N R, Hough E D and Stehney T R. Security Quality Requirements Engineering (SQUARE) Methodology. Pittsburgh.
17. Kothari C R. Research Methodology- Methods and Techniques, *New Age International Publishers,* Second Edition.
18. R Shirey, Security Architecture for Internet Protocols: A guide for Protocol Designs and Standards, *Internet Draft: Draft- irtf-psrg-secarch-sect1-00.txt*, November 1994.
19. http://www.owasp.org/index.php/Category:OWASP_CLASP_Project
20. http://www.spsstools.net/spss.htm

Sonia is a Ph.D Research Scholar at University of Delhi, India. She is also working as an Assistant Professor with University of Delhi. Her research work focuses on Agile software development and Systems Security. She has published many research papers related to her area of interest.

Archana Singhal is working as an Associate professor at University of Delhi, India. She has been awarded her Ph.D from Jawaharlal Nehru University, Delhi. Her main research areas are Natural language processing, Semantic Web, Multi-agent Systems, Agile software development, Intelligent Software Engineering, Requirement Engineering, Information Retrieval and Ontologies. She has many publications to her credit.