MATRIX Academic International Online Journal of Engineering and Technology
ISSN: 2348–3326 © MAIOJET
Volume III Issue I, April 2015

RESEARCH ON SECURITY REQUIREMENTS ENGINEERING: PROBLEMS AND PROSPECTS

Arpita Banerjee[#1], Megha Sharma*[2], C. Banerjee*[3], Santosh K Pandey^[4]
[#] *Dept. of Comp. Sc., St. Xavier's College, Jaipur, Rajasthan, India*
1arpitaa.banerji@gmail.com

[*] *Amity Institute of Information Technology, Amity University, Rajasthan, India*
2 meghasharma134@gmail.com

[3]chitreshh@gmail.com

[^] *Dept of Electronics & Info. Technology, Ministry of Communications & IT, New Delhi, India*
4santo.panday@yahoo.co.in

Abstract **- Due to constant pressure on software development team for development of workable software at a fast pace, the focus of the development team has always been on the functional requirements. As such, the identification and implementation of nonfunctional requirements, especially, security which otherwise is considered as a time consuming and quality providing process has always been neglected. But as per the available statistics, security has played a vital role in the success and failure of software systems. The nonfunctional requirement not only introduces characteristics like quality, they also present constraints under which the system must operate. This process maximizes the success of the software system. As per the recent trend, software security is gaining attention from the industries, experts and research communities. The aim of development of secure software is that it attempts to mitigate risks from assets so that the business goals could be achieved. Measuring security of software is still in its infancy and the properties and metrics for measuring security needs to be properly defined. Further, methods need to be made comprehensive for accurate and complete measurement of security properties of software. This research paper reviews the existing work done in the field of security requirements engineering. In addition, it identifies the future research work which could be carried out for betterment of security incorporation in the software development process.**

Keywords **- Software Security, Security Requirements, Non Functional Requirements, Software Security Requirements Engineering, Security Requirements Elicitation.**

I. INTRODUCTION

Each and every software product demand constricted security embedded within it to avoid being exploited. Security is an instinctive property of the software which most of the applications are lacking today. To incorporate software security measures, organization need to improvise their existing application development lifecycle. The conventional security practices which were used to safeguard the development and deployment of products are no more efficient. For example anti-virus software firewalls, intrusion detection and intrusion prevention etc. were being used to provide security because today's organizational environment is replete with high degree of risks. So a holistic and systematic effort should be undertaken by the organization in imposing software security requirements [1].

Most of the security can be enhanced by improved software development methods and tools. The available and existing methods and tools do not satisfy the pre requisites of security threats, risk assessment, security mechanisms, and software security. Their proper determination and identification at an early phase will result in a real base for software development. To handle the present situation almost all companies have started incorporating security in the early phases of software development life cycle to restrain the risks attacks of application security [2].

As per the conventional method of software development process, software requirements were divided into categories like functional and physical requirements. The role of functional requirements was to describe system objectives whereas physical requirements stated the physical accountability like time and place. The present scenario has changed the categorization of software requirement to functional and non-functional requirements. The functional attributes are compulsory for the organization to follow and their timely evaluation is also required. The functional need also controls the interaction of the system with the environment. The non-functional attributes defines the functions of the system and imposes certain restriction for the smooth and successful working of the organization. Security is also one of the non-functional requirements which require utmost importance in today's age [3].

The security requirement is one of the most important intangible requirements which could be taken as burden on the smooth functioning of the system. For developing a secured system it is essential to

correctly put focus on the important security needs and rules. Adding security to software requirements indicates that security has been considered from the very first step of software development. Security requirements objectives can be categorized as authentication, authorization, integrity, intrusion detection, non-repudiation, confidentiality, and auditing [4]. Keeping this in mind, we present the research advances in this area. The rest of the paper is organized as follows: Section II provides a brief description of security requirements engineering, Section III presents a brief overview on the current research in the area, Section IV, focuses on the future research directions, whereas conclusion and future works are reported in Section V.

II. SECURITY REQUIREMENTS ENGINEERING

The engineering of the requirements for a business, system or software application, component, etc. involves far more than merely engineering its functional requirements. One must also engineer its quality, data, and interface requirements as well as its architectural, design, implementation, and testing constraints. Whereas some requirements engineers might remember to elicit, analyze, specify, and manage such quality requirements as interoperability, operational availability, performance, portability, reliability, and usability, many are at a loss when it comes to security requirements [5].

Most requirements engineers are not trained at all in security, and the few that have been trained have only been given an overview of implementation of security architectural mechanisms such as passwords and encryption rather than actual specification of security requirements. Thus, the most common problem with security requirements, when they are specified, is that they tend to be accidentally replaced with security-specific architectural constraints that may unnecessarily constrain the security team from using the most appropriate security mechanisms for meeting the true underlying security requirements [6].

III. A SURVEY OF RESEARCH IN THE AREA

Although significant work and rapid growth has been carried out in the recent years and reported in the field of security requirements engineering with respect to security issues. A selection of some noteworthy contributions from the researchers from the recent years covering most of the closely related journals, conference proceedings, and research / technical reports which are valuable and bears weight are briefly described one by one for analysis on the advances, as follows:

Shareeful Islam & Paolo Falcarin in their research work has identified Security requirements through asset based risk management process to describe software security goals using accepted ISO/IEC 17799:2005 standard. Further they measured software security using Goal question metric approach and applied it to the identified security requirements. The limitation of this study is that its subjective evaluation has not been carried out thoroughly [7].

Bejamin Fabian & Seda Gurses has proposed a conceptual framework in the field of security engineering focused upon security requirements elicitation and analysis. They have mentioned their conceptual framework for comparison and evaluation of security requirements engineering approaches like Common Criteria, Secure Tropos, SREP, MSRA, UML and problem frames. The limitation of the study is the integration of the different SRE methods which still poses a challenge [8].

Abderrahman Matoussi and Regine Laleu in their study have presented an implementation of non-functional requirements like performance and security for a software development process. The limitation of the research work is the informal treatment of NFRs since the first level of development and the difficulty to define one method which can cope up with all the NFRs [9].

C. Banerjee and S. K. Pandey have proposed 21 Security Rules which needs to be following in the software development life cycle. They stressed upon the need of implementation of security right from the beginning i.e. the requirements engineering phase. The limitation of the study is that the rules suggested needs to be converted from conceptual model to a practical approach [4].

Helen Yesiwas Bogale and Zohaib Ahmed demonstrated that how the gap can be reduced between academia and industry in the field of security requirements engineering using Misuse case techniques. The limitation of this study is that it is hard to reach to an approach to a mature process of security requirements elicitation [10]. Nancy Mead has suggested a measurement approach to security requirements engineering by align it with the Security Quality Requirements Engineering (SQUARE). The limitation of this research work is the dependency upon the expertise of the assessor for its implementation and proper usage [11].

Haley, Charles B, and Laney, Robin has presented security requirements as constraints and developing satisfaction arguments [12]. Golnaz Elahi, et al. has described through a survey that what modeling methods are used for eliciting, analyzing and documenting security requirements in real world practice. The limitation of the study is lack of security training [13]. Inger Anne Tondel, and Martin Gilje Jaatun have presented state of the practice,

broaden to the software community's knowledge of software development. The limitation of the study is that the practitioner needs unique sets skills, tools and techniques [14].

IV. FUTURE RESEARCH DIRECTIONS

Based on the review of the existing literature given in the earlier section, further research may be undertaken in the following areas:

- Future research could be done on the development of methods for requirement conflict resolution.
- The future work could also include identification and implementation of a practical security requirement engineering method which could suggest guidelines and methods for software professionals.
- Future work may involve development of a mature process which could be developed at lower cost and results in less time consuming process.
- The future work could also be to extending and relate the formal methods to support major nonfunctional requirements. Further, modeling and analyzing functional and non-functional requirements separately.
- The future work can also be done to examine other security requirements engineering process as well as on the security requirements driver.
- As it is hard to evaluate the metrics subjectively, hence, refinement of the security aspect and its associated value would be a potential future research area.
- Incorporation of appropriate security metrics into broader quality models that can be operationalized would also be a likely future research area.
- The future work could be done by broaden up the software community's knowledge.

V. CONCLUSION AND FUTURE WORK

This article contributes to security requirements engineering in two major aspects: first, it introduces the conceptual and practical aspect of security requirements engineering which necessitates the implementation of security measurements from the requirements elicitation phase and second, it highlights the future research directions which could lead to some major developments in the field of software security.

It is quite evident from the research findings that implementation of the security during the software development process is a very difficult and expensive proposition. Still the various security incidents which have resulted in the loss of data, finances, reputation and other assets have forced the organisations, research communities and experts to take it seriously. As such the security has not started to become an integral part of software development process with its role starting from the requirements engineering phase. However, many critical issues, challenges and shortcoming still have to be dealt with.

The paper tried to present the exhaustive as well as critical review some concrete research work on various methods of promoting and implementing security requirements engineering among the software development team. At the same time, a number of noteworthy research areas are also identified for further investigations in the concerned area. The paper will help the researchers who want to pursue their research in security requirements engineering by providing a brief but complete review on the existing literature along with the current research topics. The paper will serve as a base paper for the researchers who will take the research topics through our paper.

Future work may include the development of metrics which could be applied during the security requirements engineering phase for proper identification of security requirements so that secure software could be developed and the security aspect could be quantified for further analysis and refinement of security requirements. Existing security requirements engineering model or framework could be extended or a more comprehensive and new model or framework could be developed for the quantification of the values. This work will surely help the industry in implementing security among the software development team *right from the beginning* in the software development lifecycle.

REFERENCES

[1] Tondel, I. A., Jaatun, M. G., & Meland, P. H. (2008). Security requirements for the rest of us: A survey. *Software, IEEE*, *25*(1), 20-27.

[2] Fabian, B., Gürses, S., Heisel, M., Santen, T., & Schmidt, H. (2010). A comparison of security requirements engineering methods. *Requirements engineering*, *15*(1), 7-40.

[3] Hadavi, M. A., Hamishagi, V. S., & Sangchi, H. M. (2008, March). Security Requirements Engineering; State of the Art and Research Challenges. In *Proceedings of the International MultiConference of Engineers and Computer Scientists* (Vol. 1, pp. 19-21).

[4] Banerjee, C., & Pandey, S. K. (2009). Software Security Rules, SDLC Perspective. *arXiv preprint arXiv:0911.0494*.

[5] Salini, P., & Kanmani, S. (2011). A Survey on Security Requirements Engineering. *International Journal of Reviews in Computing*, *8*(1), 1-10.

[6] Banerjee, C., & Pandey, S. K. (2010). Research on software security awareness: problems and prospects. *ACM SIGSOFT Software Engineering Notes*, *35*(5), 1-5.

[7] Islam, S., & Falcarin, P. (2011, September). Measuring security requirements for software security. In *Cybernetic*

Intelligent Systems (CIS), 2011 IEEE 10th International Conference on (pp. 70-75). IEEE.

[8] Fabian, B., Gürses, S., Heisel, M., Santen, T., & Schmidt, H. (2010). A comparison of security requirements engineering methods. Requirements engineering, 15(1), 7-40.

[9] Matoussi, A., & Laleau, R. (2008). A Survey of Non-Functional Requirements in Software Development Process. Departement d'Informatique Universite Paris,12.

[10] Bogale, H., Ahmed Z. (2011). A Framework for Security Requirements - Security Requirements Categorization and Misuse Cases. Master's Thesis, Blekinge Institute of Technology, Sweden.

[11] Mead, N. R., & Stehney, T. (2005). Security quality requirements engineering (SQUARE) methodology (Vol. 30, No. 4, pp. 1-7). ACM.

[12] Haley, C. B., Laney, R., Moffett, J. D., & Nuseibeh, B. (2008). Security requirements engineering: A framework for representation and analysis.*Software Engineering, IEEE Transactions on*, *34*(1), 133-153.

[13] Elahi, G., Yu, E., & Zannone, N. (2010). A vulnerability-centric requirements engineering framework: analyzing security attacks, countermeasures, and requirements based on vulnerabilities. *Requirements engineering*, *15*(1), 41-62.

[14] Tondel, I. A., Jaatun, M. G., & Meland, P. H. (2008). Security requirements for the rest of us: A survey. *Software, IEEE*, *25*(1), 20-27.