IOSR Journal of Engineering (IOSR JEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
PP 32-36

Revisiting Secured Software Development: Information Security Perspective

Syed Wajahat Abbas Rizvi, Pawan Singh
Department of Computer Science and Engineering, Amity University Lucknow Campus

Abstract: *Current scenario of Information Technology has been witnessing the development of variety of software applications. These applications are being developed by various developers in order to cater the customer requirements those are exponential growing day by day. No doubt, it has facilitated the end user but on the other side also raised the possibilities of weaknesses, defects and the vulnerability of the system that further reduces the desirable security of the information handled through these software. Subsequently, make the application more unsecure and highly complex, and at the same time losing the trust as well as the good will of the end user. As Information Security in software applications is a critical issue, its prediction and tracking cannot be ignored. this paper, the researcher has presented the key elements of the Information Security, along with the role of requirements phase and the software metrics in improving the information security. Finally, the paper provides a list of key observations and recommendations based on the literature review.*

Keywords:*Information Security, Secured Software Development, Software Metrics, Security Measurement, Software Requirements, Early Stage Measures.*

I. Introduction

In general, the software application, whether stand-alone or web-based, are the loco that drive the scientific investigation, business decision making and engineering problem solving. In the modern scenario computerization and electronic system contain a significant presence of information. Information is not restricted to a specific domain or sector, it has been spreading exponentially. All most every vertical market, whether it is banking, retail, health, education, defense, transportation, telecommunication, become highly dependent on information systems (Kumar et al., 2012), (Rizvi et al., 2016a). Such an exponential growth has been resulted into the increased public access to these information systems and related resources(Gupta et al., 2012a). Consequently, these resources become more and more vulnerable to attacks. In general information security as a discipline is still in its embryonic stage. The root cause that makes a resource unsecure or vulnerable is the defect in the software applications. Mostly, the major cause of these bugs includes the non-conformance to satisfy requirements or absence of quality requirements(Rizviet al., 2017). One of the alternative way to reduce ambiguity, inconsistency and incompleteness in the collected requirements is to adopt formal methods. The use of formal methods has proved their utility in a variety of mission critical software applications (Rizvi and Khan, 2013).

The aim of the information security is to safeguard the confidentiality, integrity, and availability of the information assets as well as resources, those are created, stored and transmitted by software applications (Gupta et al., 2012b). In order to ensure confidentiality developer, take care of unauthorized disclosure, for ensuring integrity unauthorized alteration are discouraged, while preserving the availability developers write the code to prevent unauthorized devastation or denial of access. Review of the literature highlights several unpleasant happenings in the financial domain, whose root cause was the breach of confidentiality, integrity and availability(Rizvi and Khan, 2010). The actual cause of this breach is the lack of information security measure that were overlooked during the different stages of development cycle. This paper is organized as follows; Section 2 presents the key elements of Information Security, while third section of the paper highlights the criticality of requirements phase in order to ensure information security. Section 4 provide a review of some of the studies those have highlighted and discussed the role of various early stage software metrics for the development of secured applications. Section 5 presents critical observations and recommendations based on the literature review, while the paper concludes in Section 6.

II. Information Security

The key aim of Information Security is to guard critical assets of an enterprise like hardware devices, software applications and human resource. In order to protect the physical and financial resources, goodwill, legal status, human resources and other tangible and intangible assets, and at the same time meeting the organizations mission, it is highly desirable to choose and apply appropriate mechanisms for ensuring information security.Security of any Information systems are always affected with the people within the organization and the persons interacting with the software application(Michael and Herbert,2007). The end-users who try to access the information which the security professionals are trying to protect may be the weakest connection in the chain of information security (Singh and Kumar, 2012).In a study (Thomas, 2002) researcher has postulated guiding principles for effectively managing the Information Security (Rizvi and Khan, 2009). The author further stated that information security must be based on following key elements:

a. There must a proper post for Information Security Officer specially in an organization that has critical information. Besides, Information guarding should also support the fundamental objectives along with the mission of the company.
b. As long as the responsibilities of a senior management is concerned it should focus on the two issues one is duty of loyalty and another, duty of care. A duty of loyalty focuses on the decisions concerning the best interest of the organization, while and duty of care implies the protection of the enterprise's resources. Therefore, senior management must take informed decisions to take care of both.
c. Information security should not be expensive. Appropriate application of risk analysis process is one the key element for ensuring information security in an organization. Timely identification of unforeseen risk along with there contingency planning should not be ignored.
d. The responsibilities and accountabilities regarding Information security should be defined explicitly. Information security policy must classify various roles and responsibilities of all the stakeholders of an organization. In order to make the policy further effective it should also be reflected into the communication documents like purchase order and business contracts or MOUs.
e. Sometimes when it required to extends the access to information beyond the organization then it should be the responsibility of information owner to monitor the usage in order to safeguard that it complies with the user profile and authorization of the person accessing the information. This will give an impression on the external person to realize that there is adequate security.
f. In case of big organization implementing Information security policies for an enterprise is not enough, but at the same time it should also has a proper representation in every department. Each business unit should designate an appropriate individual for implementing the information security program in order to cater the specific objectives of the business unit.
g. Information security is not a static entity. It is very challenging to make it dynamic. Therefore, it is mandatory for an enterprise to periodically reevaluate and update the security policies with time, need and aims. However, if the enterprise has global presence in different countries, then the overall information security policy should be adjusted as per the region and culture where it would be implemented.

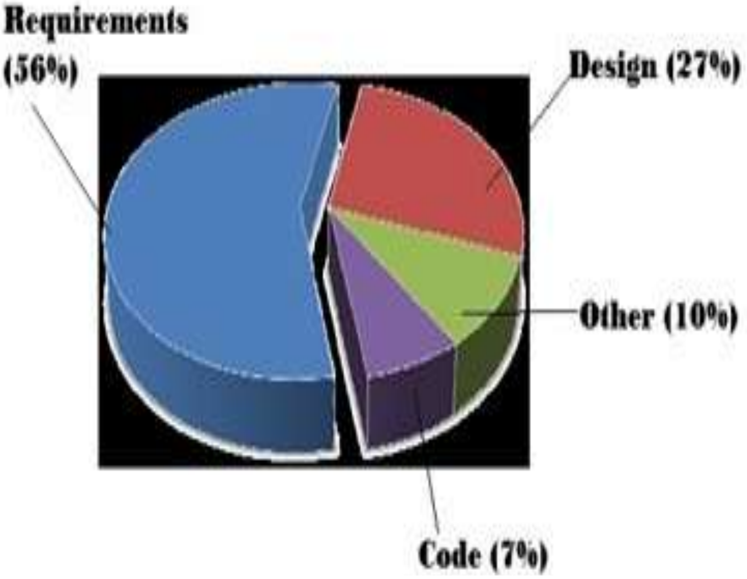

Figure 1: Distribution of Faults in Software Projects(Kong, 2009)

III. Requirements Phase And Information Security

It is a well-accepted fact that requirements stage is key to the success of any major software development. There are sufficient studies in the literature that early stages of the software development are prone to defects. The major risks for the software's success are confusion and misunderstanding about the requirements. (Easterbrook and Paul, 1998). In a study of a US Air Force project by Sheldon(Sheldon, 1992), defects were classified by their origins. It had found that software requirements comprised 41% of the total defects, while design faults are only 28% of the total faults. Other studies also support this result as well. For example, a study conducted by James Martin(Martin,1986) had reported that over half of all project defects have their roots in the requirements stage as indicated in Figure 1 (adapted from (Martin, 1986)). Further, the study stated that approximately fifty percent of requirements defects originated from the poorly written, ambiguous and incorrect requirements. The rest fifty percent faults could be attributed to the requirements specifications that are incomplete or those were just omitted.According to the industrial data, the cost of detecting and fixing a defect that is introduced during the requirements and design stage of the software development life cycle increases exponentially as the development progresses through the later stages (Graham et al., 1993). This fact is pictorially represented in the following figure 2. In another study, (MacDonell,1997) author concludes that a requirements fault that is left undetected and is not arrested till the testing and maintenance phase will cost 50 to 200 times of the cost if would have fix in the requirements phase. By the time that software starts its operational life in the real time environment, it becomes very difficult as well as expensive to meaningfully improve its security related features.

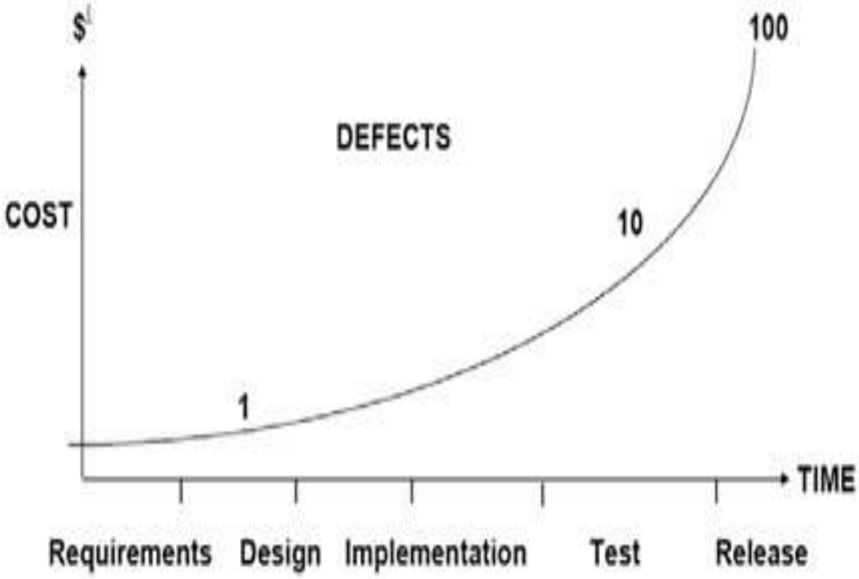

Figure 2: Industry Standard Cost Ratio to Fix a Defect

In today’s scenario software requirements are keep changing and evolving in a dynamic environment throughout the development phases. Therefore, it becomes very crucial to deal with such dynamic change requirements. The major cause of these change requests are conflicts between stakeholder groups, evolving vertical markets, less time to market the software application, market competition, and so on.

IV. Security Measurement

When measurement is discussed in the context of science and engineering, it is comprised of collection of relevant data followed by its validation and subsequent processing of the validated data. The first step defines what type of data is required and which approach of data collection will be suitable for studying the domain under study. The second phase of measurement is to validate the collected data for ensuring its consistency and integrity. Finally, the knowledge or trends could be inferred using appropriate quantitative techniques in the context of software or information security(Wang, 2005). In order to measure the security level of the developing software in its early stages of development, it is needed to identify the security characteristics those are measurable, because anything cannot be controlled until it is not measurable.

The next important stage is identification of suitable metrics those can be used to measure identified security characteristics. There are two key terms one is measurement and other is metric, there is difference between these two terms Measurements offer single-point-in-time views of specific aspects. While, metrics are derived from comparing two or more measurements taken over time with a predetermined baseline. In a study Alger differentiated metric from measurement and suggests that measurements are made by counting, whereas metrics are the result from regress analysis (Hallberget al., 2005).

V. Role Of Various Early Stage Software Metrics

In the last two decades substantial number of studies focusing on software quality and information security has been performed by various researchers where they have used a variety of techniques to meet their targets(Rizvi et al., 2016b, 2016c). In a study based on software security the researcher (Hadaviet al., 2008) has proposed a system that provide security through preventing pre-deterministic vulnerabilities. The study has explored more than twenty susceptibilities along with their impacts on information security. Subsequently the author had also highlighted the application method of identified vulnerabilities in the different phases of SDLC. In another study,(Gilliam et al., 2003)Gilliam emphases the development of Information Security Checklist for the software development. The researcher has also focused on assimilating security during the development of software right from the starting.In order to measure vulnerability indicators, (Chowdhury and Zulkernine, 2011) Chowdhury and Zulkernine proposes software metrics on the three key object-oriented attributes coupling, complexity and cohesion that can be quantified in the early phases of software life cycle.

While in another research effort on information security the author has compared three processes to develop secured applications. All the three processes were comprehensively evaluated, followed by a list of suggestions for improving the security of software application and information.In a study (Yanguo and Issa, 2007) focusing on the properties of security measures, in this paper the researchers have worked on identifying some of the internal attributes of the developing application those are associated with key qualities of information security. These properties were aligned with the broadly recognized security design principles (Mir et al., 2011).

VI. Critical Findings And Recommendations

This section of the paper is presenting some critical finding inferred from the literature along with some recommendations for project managers involved in the development of secured quality software:

a. Review and evaluate the existing practices that are being currently applied. If these practices are not properly focused on requirements engineering, then incorporate a requirement engineering practice that can help in ensuring information security.
b. Reevaluate whether the organization is taking care of those aspect that may follow a requirement process, does it take care of security requirements? If not, then develop a suitable course of action to decide how to strengthen the requirement document and lead to the development of secure software.
c. Always try out the newly developed process on a few ongoing software projects in order to critically observe and debug them, without directly experimenting these new and untested processes on all the projects.
d. In order to further improve processes, always document the results, whether they are positive or negative and use them.
e. If there is an existing approach to security requirements engineering, developed by someone else, that could potentially be useful, give it a try. It’s not required to reinvent the wheel every time.
f. When security requirements are considered, they are often developed independently of other requirements engineering activities. As a result, specific security requirements are often neglected, and functional requirements are specified in blissful ignorance of security aspects.
g. It has been observed while reviewing requirements documents, that security requirements, whenever they exist, are in a section by themselves and have been copied from a generic list of security features. The requirements elicitation and analysis that are needed to produce a better set of security requirements seldom take place.
h. In general, most of the requirements engineering studies and practice focuses on the system’s properties. Therefore, their focus remains on the functional aspect of the system that is how they will facilitate the end user, but it is ignored what the software application should not function.
i. Another key aspect is how the attacker will take on the application. Attacker’s focus is to find a space among the existing functionality of the application to breach the security. Therefore, they always try to find any defect/fault or any weaknessthat will provide them an opportunity for getting access to what they are interested in. The only way to handle this is to think from attacker’s perspective along with user.

VII. Conclusion

Finally, it could be concluded that ensuring the information security is becoming a challenge day by day. Every day new incidents are happening, that has been forcing the application developers to devise counter strategies in order to make the information secure from attackers. As it has been noticed in the literature that issue of information security must be taken care of in each phase of development cycle, specially, in the early stages. The paper has described the key elements of Information Security in the second section of the paper.The importance of requirement phase is highlighted in the third section, while, some of the earlier studies focusing on metrics are discussed in section fifth. Finally, the last section listed some of the critical findings and recommendation for improving the information security.

References

[1]. Chowdhury, I., &Zulkernine, M. (2011). Using complexity, coupling, and cohesion metrics as early indicators of vulnerabilities, Journal of Systems Architecture, 57(3), 294-313

[2]. Easterbrook, S., & Paul, A.S. (1998). An Experience Report on Requirements Reliability Engineering Using Formal Methods. IEEE Transactions on Software Engineering, 24(1), 4-14.

[3]. Gilliam, D. P., Wolfe, T. L., Sherif, J. S., & Bishop, M. (2003). Software Security Checklist for the Software Life Cycle, Twelfth International Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises, ACM Digital Library

[4]. Graham, D., Finzi, S., & Glib, T. (1993). Software Inspection. New York: Addison-Wesley, ISBN-10: 0201631814

[5]. Gupta, P. N., Singh, P., Singh, P. K., & Kumar, A. (2012b). A Comparative Analysis of Page Ranking Algorithms, International Journal of Computer Science and Telecommunications, 3(10), October 2012,33-39

[6]. Gupta, P. N., Singh, P., Singh, P. P., Singh, P. K., & Sinha, D. (2012a). A Novel Architecture of Ontology based Semantic Search Engine, International Journal of Science and Technology, 1(12), 650-654

[7]. Hadavi, M. A., Shirazi, H., Sangchi, H. M.,&Hamishagi, V. S. (2008). Software Security: A Vulnerability-Activity Revisit, Third International Conference on Availability, Reliability and Security, IEEE, Barcelona, Spain

[8]. Hallberg, J., Hunstad, A., & Peterson, M. (2005). A Framework for System Security Assessment, IEEEWorkshop on Information Assurance and Security, United States Military Academy, West Point, NY, 224-231

[9]. Kong, W. (2009). Towards a Formal and Scalable Approach for Quantifying Software Reliability at Early Development Stages. Ph.D. Thesis University of Maryland

[10]. Kumar, S., Rana, R. K., &Singh, P. (2012). A Semantic Query Transformation Approach Based on Ontology for Search Engine, International Journal on Computer Science and Engineering, 4(5), pp. 688-693

[11]. MacDonell, S.G. (1997). Establishing relationships between specification size software process effort in case environment. Journal of Information and Software Technology, 39(6), 35–45

[12]. Martin, J. (1986). An Information Systems Manifesto.1st Edition, Upper Saddle River, New Jercy, USA: Prentice Hall PTR, ISBN:0134647696

[13]. Michael E. W. & Herbert J. M. (2007). Principles of Information Security, Thomson Learning- Course Technology, Second Edition, 188

[14]. Mir, I. A., Dar, M., &Quadri, S.M.K. (2011). Towards the Application of Security Metrics at Different Stages of Information Systems, Journal of Global Research in Computer Science, 2(2), 24-28

[15]. Rizvi, S. W. A., & Khan, R. A. (2009). A Critical Review on Software Maintainability Models. Proceedings of the Conference on Cutting Edge Computer and Electronics Technologies, 144-148

[16]. Rizvi, S. W. A., & Khan, R. A. (2010). Maintainability Estimation Model for Object-Oriented Software in Design Phase (MEMOOD). Journal of Computing, 2(4), 26-32

[17]. Rizvi, S. W. A., Singh, V. K., & Khan, R. A. (2016b). The State of the Art in Software Reliability Prediction: Software Metrics and Fuzzy Logic Perspective. Advances in Intelligent Systems and Computing, Springer, 433, 629-637

[18]. Rizvi, S.W.A., & Khan, R.A. (2013). Improving Software Requirements through Formal Methods. International Journal of Information and Computation Technology, 3(11), 1217-1223

[19]. Rizvi, S.W.A., Khan, R.A., & Singh, V.K. (2017). Early Stage Software Reliability Modeling using Requirements and Object-Oriented Design Metrics: Fuzzy Logic Perspective. International Journal of Computer Applications, 162(2), 44-59

[20]. Rizvi, S.W.A., Singh, V. K., & Khan, R. A. (2016a). Fuzzy Logic based Software Reliability Quantification Framework: Early Stage Perspective (FLSRQF), Elsevier Procedia-Computer Science, 89, 359-368.

[21]. Rizvi, S.W.A., Singh, V.K., & Khan, R.A. (2016c). Software Reliability Prediction using Fuzzy Inference System: Early Stage Perspective. International Journal of Computer Applications, 145(10), 16-23.

[22]. Sheldon, F., (1992). Reliability Measurement from Theory to Practice. IEEE Software, 9(4), 13-20.

[23]. Singh, P., Kumar, A., &Prashast, (2012). Studies on Research and Development in Web Mining, International Journal of Computer Applications, 44(9), April 2012, pp. 28-32.

[24]. Thomas R. P., (2002). Information Security Policies, Procedures and Standards, Guidelines for Effective Information Security Management, Auerbach Publications, 1-3

[25]. Wang, A. J. A. (2005). Information Security Models and Metrics, 43rd ACM Southeast Conference, ACM, March 18-20 Kennesaw, GA, USA.178-184

[26]. Yanguo M. L., & Issa T. (2007). Properties for Security Measures of Software Products. Applied Mathematics & Information Sciences, 1(2), 129-156.