Volume 5, Issue 11, November 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Agile Model of Software Security: Risk Perspective

Mohd. Nazir*
Department of Computer Science, Jamia Millia Islamia
(Central University), New Delhi, India

Abstract—Building automated security scanning facilities should be an early focus. Software security Industry is facing a lot of difficulties in choosing a truthful security development process when software has to meet a lot of security risks ranging from low to high to catastrophic. When security development is becoming complex in nature due to various risks, corporation's usual practice is to switch over to traditional models for security risks detection. Some models are considered to be the best conventional models for security risks analysis. But in modern security developmental style, all the security development process around a single trend called the Agile. The key objective of this paper is to revise the agile model and to get a conclusion on the impact of security risks assessment on demanding security development of software.

Keywords— Software security, Security Risks, Security Risk Assessment, Agile Model, Agile Model security

I. INTRODUCTION

Development in contemporary agile methodologies happens at fast pace. Frequent iterations and fast releases often translate to dynamic application, with new components or modules that added and required changes incorporated in a regular fashion throughout SDLC. This iterative approach enables teams to adjust course early and generally addressing problems as they arise. Addressing problems with application early sounds like a great approach to security. For any security activity that to be integrated into agile development process it needs to be light weight and delivered in chunks that seamlessly adjust or fit into existing development process [11].

In this fast growing modern Information Technology world, software security development has become a great challenge for the security developers as well as for the organization. The main challenge is related to various security risks associated with the development. The security risks identification, assessment, management and mitigation have really paved a challenging situation for the companies of security development [1-2]. Most of the security development designs found to use more resources, more time and more budget than the specified and reach at a lesser security quality and functionality of software, giving rise to an unsatisfied consumer. On analysis, it is found that, all these problems occurred due to the lack of assessment of security risks during the inception of the software and the various activities during Secure-SDLC. Software security risks are those that could prevent the achievement of the objectives stated by the security manager and the security development team. Security risks usually arise from the relationships among the technology and persons. Inefficient and ineffective security assessment and poor management of risks creates a huge negative impact on the business progress of the corporation itself [3][4].

In this paper, researcher tried to find out some of the various generic risks factor of the security. Author also studied on the impact range of security risks on security developmental issues by taking into account, the main Secure-SDLC model and latest new generation lightweight model that is 'Agile Model'. Just like developing agile software, adopt an iterative approach to implement security capabilities using check points in order to analyse the efficacy of existing capabilities and adjustment made as and when required. A robust agile security model improves visibility, leverage automation in order to reduce time required for security analysis. Remainder of this paper is organized as: Section II gives the related work in the area. Section III presents security risk assessment in the context of agile model. Section IV concludes the paper

II. RELATED WORK

A lot work in the area of security development methodologies is reported in the literature. These methodologies are compared with different models as well as the studies based on the security risks factor and their effect on security developments of software in various perspectives. However, these studies are not complete in the extent of pinpointing exact security risks and how the models succeed from those effects. Several research contributions are available in the literature that address the concern and highlighted pertinent issues in the area security management and risk assessment.

In 1989, Boehm Barry W. has indicated about the risk factors of security and its assessment techniques using various criteria [1]. In 2010, Michael Lant emphasizes on the concept of security risk assessment and security management knowledgeable in Agile Methodologies [2]. This paper clearly specifies five different steps in easy management of those security risks. This was the main source of this study in this area. In 2011, Boehm tried to explain the major steps and

techniques involved in security risk management of software [3]. In 2004, Sanajana Taya gave an insight about the models of security development process and their comparison based on many features and related aspects [4].

This paper gets a good idea about the overall nature of each models of software security development process. In 2011, V. Szalvay emphasizes on the overall idea about agile methodology for security and how it helped security managers to improve their efficiency of security [5]. In 2015, R. Kumar, S. A. Khan, R. A. Khan helped in reviewing about the leading software security process and explained about the security risks states and their management methods [6]. Thus, they have tried to reveal the concept that some of the development methodologies inherently possessed security risk management capability and are inevitable in nature.

In 2010, N. M. A. Munassar, A. Govardhan refers to the comparison between the five different software security models by stating their advantages and disadvantages very categorically [7]. In 2010, R. Dash and R. Dash have discussed about the linear sequential model and its risk factors of security. All these contributions discussed above altogether helped to gain an insight about security risks and their effect on various security models. A risk based approach to security guides the decision making process around how deep and broad security assessment go, as well as what to look for.

III. SECURITY RISKS ASSESSMENT IN CONTEXT OF AGILE MODEL

Security risk assessment and its management has now become a vital part in software development. There is a huge transformation from the traditional security risk analysis model towards the latest trendy model that is nothing but obviously 'Agile Model'. This change has created new challenges in the field of security risks analysis and their management. This paper has made a comparative study on different aspects of security risks and the efficiency of the models while dealing and assessing these factors of security risk [8]. This study has chosen the famous Agile Model. Security risk driven approach of the model helps to accommodate any type of specification oriented, model-based or any other transformation-oriented approach to the security development of software. Similarly, security risk management factors help to determine the amount of time and effort that is committed to other activities of security like planning, change security management, formal technical reviews & revision, security testing etc.

The highpoint of the model is that each of its cycle is completed through a fruitful interaction between the consumers and the security developers related with the software. Agile model is the modern trend in software security development methodology, which is used to quicken the operational software security delivery within a scheduled time frame using set of values that include adaptability, transparency, simplicity and unity in effective and light weighted manner. Agile model is extensively practiced model which has a frequent approach in simplifying the process by dividing it into short and light weighted phases such as Requirements, Specification, Architecture, Design, Implementation, Testing, Deployment and Maintenance that results in effective software security. There are many specific agile development methods [9].

Most encourage the security development, team spirit, association, and process compliance throughout the security life-cycle of the software design. Agile methods break tasks into small increments with minimal security planning and do not directly involve long range security planning. Iterations are very short time frames which are also called time boxes that typically range from one to four weeks. Each of the iteration involves a cross functional team working in all tasks like security planning, requirement analysis, architectural design, coding ,unit level testing, and finally the acceptance security testing[10].

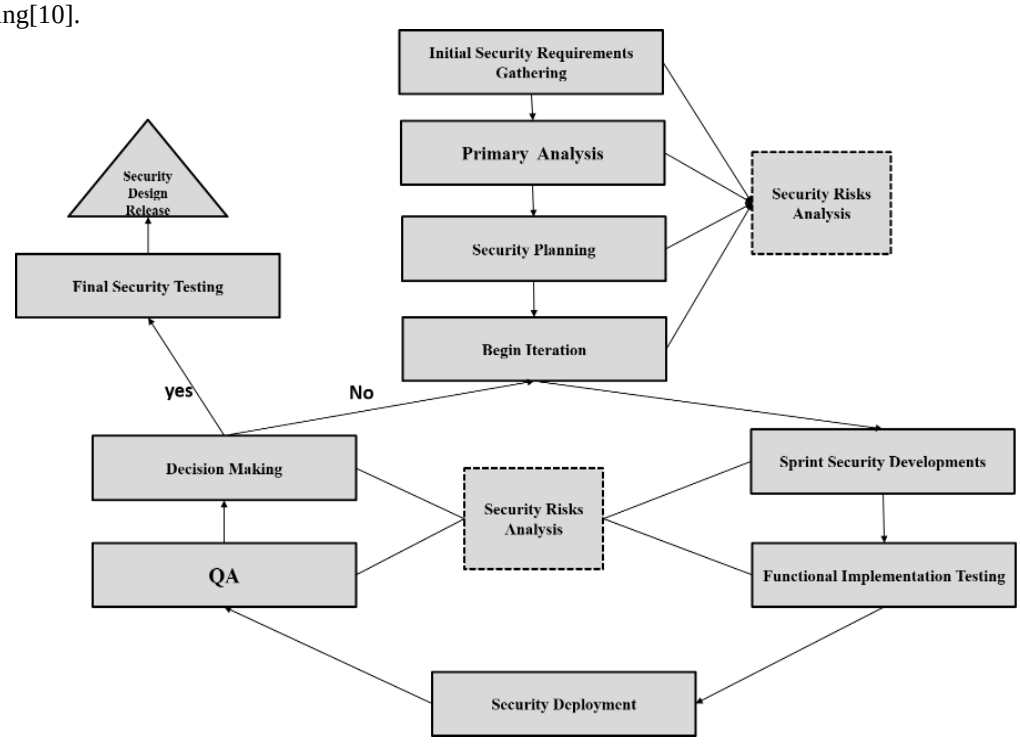

Figure 1: Agile Model with respect to Security Risks

Every iteration actually ends after the discussion and communication with potential customers and the working of security oriented software are also conveyed to the stakeholders. This greatly helps in minimizing the overall security risks and hence, the changes are adapted by software quickly. Much number of iterations might be required to release software. A model showing the agile life cycle along with its security risks analysis phase is depicted in figure 1 below.

Advantages

- Consumer satisfaction may be assured and guaranteed by releasing rapid, continuous delivery of the required security of software.
- Interactions are accentuated rather than security process and tools. Consumers, security developers and security testers constantly involved and interact with each other.
- Working software of security is delivered regularly.
- Close and daily interaction, coordination and cooperation between business experts, other stakeholders and security developers are the essential requirements.
- Continuous attention to technical perfection and good security design is taken into consideration for the enhancement of security.
- Regular adaptation to changing security environments is accepted.
- Welcomes and accommodates changes in security requirements even at the later stages of development process.

Disadvantages

- In case of larger security of software, it is really difficult to evaluate the effort, the security required at the starting of the security development lifecycle of software.
- There occurs a lack of prominence on necessary security designing and documentation.
- The software can easily change track if the consumer is not clear about the final outcome that they require.

Many models are found to have higher order security risks than Agile Model. Even then, it can be concluded that based on the type of security and size of software, other models also play a very significant role in software security development and dealing with the security risks associated with the software development. Even though security risks level is lower for Agile Model when compared to another, under many conditions like Software Size, Consumer Experience and Nature of Work Flow, other models are also taken into consideration for software security development by various organization now a days. But from analysis done, it is estimated that, majority of the modern security development companies support the Agile Model considering it as their core model for live, fast deliverable, software development model of security in recent years.

IV. CONCLUSION

The study reveals that the level of security risks is higher when dealing with development of software security. Though, it has a notion that agile methodologies are inefficient in large organizations while for certain types of security of software, it seems to be best for security development of small and non-sequential software based on the security risk assessment done herewith. To achieve security success in agile environments, it is now inevitable to break down tradition and start treating security as an integrated piece within agile processes rather than an afterthought. Many organizations believe that agile methodologies, adopt a hybrid approach that mixes elements of agile and plan-driven approaches.

Security risk assessment and security development of software always go hand in hand and without proper security risk assessment, never ever quality software can be developed. Just like developing agile software, adopt an iterative approach to implement security capabilities using check points in order to analyse the efficacy of existing capabilities and adjustment made as and when required. A robust agile security model improves visibility, leverage automation in order to reduce time required for security analysis. Thus, it can be concluded that depending upon the type , complexity and size of the security, proper selection of software development model helps the organization to assess the various security risk factors and based on which the organization can release a quality product on time and within the given budget.

REFERENCES

[1] Boehm Barry W, "Software Risk Assessment", IEEE Computer Society Press, Vol.15 (7), pp.902-916, 1989.

[2] Michael Lant, "Five Simple Steps to Agile Risk Management", June 4, 2010.

[3] Boehm, B.W. "Software risk management: principles and practices"-Software, IEEE (Volume:8 , Issue: 1), ISSN :0740-7459.

[4] SanajanaTaya "Comparative Analysis of Software Development Life" – ISSN: 2229-4333 (print), SSN: 0976-8491(online), vol.2ISSUE 4, Oct- Dec 2011.

[5] V. Szalvay, "An Introduction to Agile Software Development," technical report, Danube Technology, 2004.

[6] R. Kumar, S. A. Khan, R. A. Khan, Revisiting Software Security Risks, British Journal of Mathematics & Computer Science, Volume 11, issue 6, 2015.

[7] Nabil Mohammed Ali Munassar and A. Govardhan," A Comparison Between Five Models Of Software Engineering", IJCSI International Journal of Computer Science Issues, Vol. 7, Issue 5, September 2010, ISSN (Online): 1694-0814.

[8] R. Dash and R. Dash, "Risk assessment techniques for software development," European Journal of Scientific Research, Vol 42, No. 4, 2010, pp. 629–636.

[9] HaneenHijazi, "A Review of Risk Management in Different Software Development Methodologies ", International Journal of Computer Applications (0975 – 8887) Volume 45– No.7, May 2012.

[10] M. Soumya Krishnan, "Software Development Risk Aspects and Success Frequency on Spiral and Agile Model", International Journal of Innovative Research in Computer and Communication Engineering, Jan 2015.

[11] Agile Methodology and Application Security_ A Promising Pair, URL: https://www.cigital.com/blog/agile-methodology-and-application-security-a-promising-pair/

