Security Practices in Agile Software Development Process : A literature review

Arpit Thool

arpitthool@vt.edu
Department of Computer Science, Virginia Tech

May 2022

Abstract

Agile methods are quite popular and used for software development. Today, a software system is expected to be secure and robust. Thus it is necessary to include security practices in Agile software development. This short paper presents a literature review on the security practices conducted or suggested in agile software development. The findings say that efforts have been made to include security activities in agile methods, but more work needs to be done to make the process more efficient by also taking into account the perspective of software engineers.

Keywords

Agile Software Development, Literature Review, Software Security

Introduction

Software Security

Security is an important quality of a software system. It aims to prevent software against malicious attacks and other risks so that the correct functioning of the software can be guaranteed.

Security consists of various properties, these are availability, confidentiality and integrity[1]. Availability means the guarantee that users can access the resource they can access through the software system[6]. Confidentiality means revealing information to authorized users only[6]. Integrity means ensuring that the information can be manipulated by authorized users only[6].

If the security of a software is compromised it may lead to a huge financial loss to the company. Also, the reputation of the company may take a hit. Hence, a company should invest in making their software systems more securer and robust. Therefore, security practices need to be explicitly included into the software development life-cycle.

Agile Development Method

Agile is a broad term that refers to a set of software development principles. It is framework for software engineering. It starts with a planning phase and progresses through iterative and incremental steps to the deployment phase. The main purpose of agile methodologies is to decrease costs in the software development process by allowing changes to be implemented without jeopardizing the process or requiring unnecessary rework[9]. A lightweight [5] adaptable technique was developed and pushed by an official partnership of 17 software engineering consultants in 2001, which led in the release of the "Agile Software Development manifesto" [3], which outlines a set of values and principles in software and system agility. Four values and twelve principles supported and constituted the essence of being agile.

Values of Agile

1. Individuals and interactions over processes and tools: Communication and interactions between individuals is emphasised over the process and the development tools used.
2. Working software over comprehensive documentation: The manifesto states that the progress in the agile methods are evaluated through delivery of tested working software rather than concise and heavy documentation.
3. Customer collaboration over contract negotiation: Customer collaboration and feedback is given more emphasis over the formal contract agreement.
4. Responding to change over following a plan: During the development, the client may find that a stated feature is not needed or that a new feature might be needed. Hence, adapting to changes is given more importance over following a strict defined plan.

The Problem

Software Engineers have moved from sequential software development process to iterative software development. In sequential process having planning and design documents available meant that security practices can be easily incorporated into the development process. But with the Agile process which emphasizes more on direct person-to-person communication rather than heavy documentation to cope up with changing customer requirements, which makes the incorporation of security activities into the development process difficult[2].

Agile methods are widely adopted and used by many teams for the software development process. Hence, it is of interest to researchers and practitioners to know which security practices they should include in the agile methods to make their software more secure and robust.

Method

This literature review addresses the following research question:

RQ1

What security practices are suggested to increase the security and robustness of a software system developed using agile software development process.

Results and Discussion

The suggested security practices to be used in agile software life-cycle as mentioned in [7] are as follows:

- Misuse stories
- Addressing security from early iterations with requirements and testing.
- ScrumS risk analysis with little documentation

- Evaluation of the rework for introduced security costs
- Systematic security
- Security disciplines
- Acceptance tests and unit tests
- Information sharing
- Security master
- Combining security activities from multiple engineering processes
- Weigh cost of integration vs. benefit of continuous use
- Agility feature selection
- Assigning relative weight
- Integration of security activities from agility degree
- Security stakeholder
- Security testing
- Countermeasure graphs
- External knowledge
- Parallel to Scrum eases integration
- Clearly state security requirements
- Adding a security specialist role
- Providing knowledge of security
- Iterative and incremental risk
- analysis, countermeasure graphs
- Security policies
- Acceptance and unit test
- Automatic testing
- Scrum with security activities added, countermeasure graphs
- Project planning
- Extending the testing technology
- Lessen unnecessary documentation
- Iterative work on security

The suggested security practices to be used in agile software life-cycle as mentioned in [4] are as follows:

- Guidelines
- Specification analysis
- Review
- Application of specific architectural approaches
- Use of secure design principles
- Formal validation
- Informal validation
- Internal review
- External review
- Informal correspondence analysis
- Requirements testing
- Informal validation
- Formal validation
- Security testing
- Vulnerability and penetration testing
- Test depth analysis
- Security static analysis
- High-level programming languages and tools
- Adherence to implementation standards
- Use of version control and change tracking
- Change authorization
- Integration procedures
- Security evaluation

Above we see various security activities suggested to be included into agile software development lifecycle. These are suggested based upon various security related challenges found when following the agile process.

Limitations

The study [8] suggests that the myth Agile methods are less secure, is untrue. It analyzed various Agile processes and found that there are security activities included in every phase of agile methods, with some activities being more popular. However, it also concludes this on theoretical evidence and not on actual real-world practice.

Conclusion and Future Work

We see that there is some research work done to improve security and robustness via suggestion of various security practices to be included into agile methods. However, very little is known about the real-world implementation of these security practices into agile software development process. The next steps could be surveying software engineers to gain insight into how they perceive these security practices and how the inclusion of these would effect the various aspects of agile methods like team velocity, confidence in security of production software, how likely the software engineers are to adopt these practices, etc. Potential future work would be surveying the practitioner's of Agile on a few popular suggested security practices. And through the analysis of this survey better judgements can be made to include the security practices into the software development life-cycle to improve the overall security and robustness of the software.

References

[1] Algirdas Avizienis et al. "Basic concepts and taxonomy of dependable and secure computing". In: *IEEE transactions on dependable and secure computing* 1.1 (2004), pp. 11–33.

[2] Konstantin Beznosov and Philippe Kruchten. "Towards agile security assurance". In: *Proceedings of the 2004 workshop on New security paradigms*. 2004, pp. 47–54.

[3] Kieran Conboy. "Agility from first principles: Reconstructing the concept of agility in information systems development". In: *Information systems research* 20.3 (2009), pp. 329–354.

[4] Ronald Jabangwe et al. "Challenges and Solutions for Addressing Software Security in Agile Software Development: A Literature Review and Rigor and Relevance Assessment". In: *Research Anthology on Recent Trends, Tools, and Implications of Computer Programming* (2021), pp. 1875–1888.

[5] Kiran Jammalamadaka and V Rama Krishna. "Agile software development and challenges". In: *International Journal of Research in Engineering and Technology* 2.08 (2013), pp. 125–129.

[6] Richard Kissel. *Glossary of key information security terms*. Diane Publishing, 2011.

[7] Klaus Reche Riisom et al. "Software security in agile software development: A literature review of challenges and solutions". In: *Proceedings of the 19th International Conference on Agile Software Development: Companion*. 2018, pp. 1–5.

[8] Kalle Rindell, Sami Hyrynsalmi, and Ville Leppänen. "Busting a Myth: Review of Agile Security Engineering Methods". In: Aug. 2017. DOI: 10.1145/3098954.3103170.

[9] Samar Al-Saqqa, Samer Sawalha, and Hiba AbdelNabi. "Agile Software Development: Methodologies and Trends." In: *International Journal of Interactive Mobile Technologies* 14.11 (2020).