Research Proposal

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

April 2022

Project summary

We request support to survey and study the effects of including security practices in Agile software development process. Security is an important requirement of any software system and if not implemented correctly, it has potential to make a major blow to the organization. There are hackers that may try to compromise vulnerabilities in the software of an organization and use the obtained information for malicious purposes. Hence, it is important for the software system to be secure.

Agile is an iterative approach to project management and software development. Agile methods give more emphasis on person-to-person interaction and less on documentation. Also Agile methods focus more on delivering the functional requirements of the software system and less on the non-functional ones. Security comes under non-functional requirements. These qualities of Agile make it harder for software teams to incorporate security into the software product. And with the growing use of Agile methods for software development, we need ways to incorporate security practices into them. This would require analyzing previous work done and to come up with new ideas to include security activities which solve the

Intellectual merits

The main research objective of this project is to find the effects of including security activities into Agile methods for software development. And also determine how these security practices are perceived by practitioners of Agile. Our work will start to better adaptation of agile methods with security and and help make rightful decisions to boost the security and robustness of the delivered software. As agile is used to build many types of software systems in a wide area of domain, the effects of this work would affect those areas as well. By increasing software security, our work would make it more difficult to hack the software for malicious purposes. This eventually would increase the trust of clients that use the software products.

Broader impacts

Prior research indicates that there is some work done in improving security in products developed using Agile methods in the form of phases under agile methods which focus on security. But yet these are theoretical efforts. Our research work focuses on interviewing the real-word practitioner's of agile methods. This would give us more insight into how the inclusion of these security activities or phases would affect the various factors such as sprint velocity, developer confidence, awareness, etc in Agile software development life-cycle. The results from this work would help organizations and stakeholders take better decision on how to make their software systems developed using agile methods, more secure and robust. And hence, this would ultimately contribute to the future success of the organization.

Related work

Agile methods are quite popular and used for software development. Today, a software system is expected to be secure and robust. 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. Thus it is necessary to include security practices in Agile software development. 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[4]. Confidentiality means revealing information to authorized users only[4]. Integrity means ensuring that the information can be manipulated by authorized users only[4].

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.

The suggested security practices to be used in agile software life-cycle as mentioned in [5] and [3] 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
- 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

The study [6] 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. Finally, 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 what effects would the inclusion of these would have on 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.

Proposed research

Surveying Prior Work

We will research the previous work done in this domain. We'll look over proposed security practices in agile methodologies in research papers, journals, and conference presentations. Then, based on the acquired data of suggested agile security measures, we'd pick the top ones. This would require going through various process methodologies and finding the security challenges and the corresponding proposed solutions. There are many research papers that have already done this survey and compiled a list if security challenges and the suggested security practices to be included into agile methods to overcome these challenges.

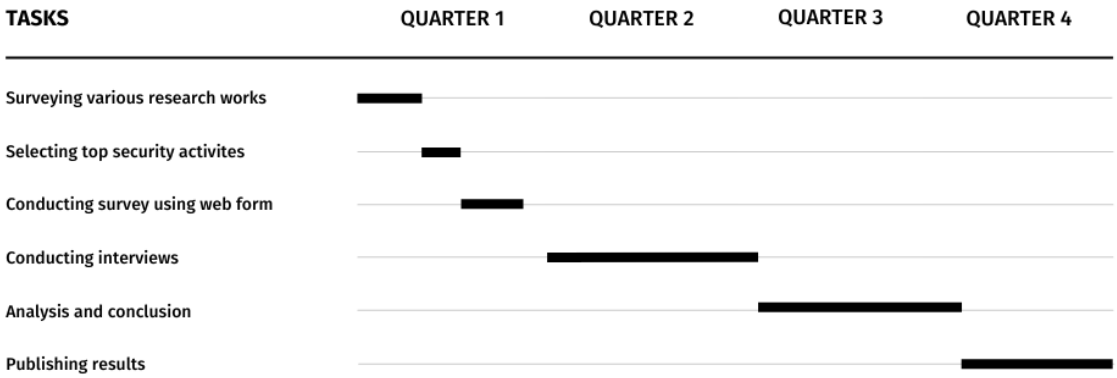
Conducting The Survey

This activity would consist on focus on conducting interviews with our participants throughout. This activity will mainly focus on gaining insights into the practitioners perspective of the proposed security activities and security of software product in general. The participant will be asked questions on how they see security activities. These questions would be ask how the inclusion of the security practices would affect the various aspects of agile method. How incorporating these tasks into the agile process might effect things like sprint pace, product security confidence, and the adoption of security practices into the software development life cycle, among other things. We'd also want to hear their thoughts on what further should be done to improve the software's security to prevent the software from malicious hackers.

Analyzing the Data

This activity would consist of us studying and formulating the outcomes from the interview replies. The interviews' recordings or transcripts will be extensively evaluated using qualitative analysis. This would provide us with more information about how agile practitioners view the integration of security principles into the software development process. Lastly, a conclusion would be drawn based on the findings, summarizing the entire research.

Timeline



The project is expected to be completed in a time span of twelve months or one year. In the first quarter we will be researching about the work that has already been done in this domain. We will go through research papers, journals and conference presentations about security practices in agile methods. Then from this gathered data of suggested security practices in agile, we would select the top five or ten. Our next step would be sending out an initial survey form to be filled by practitioners of agile such as software engineers and product owners. From this we would gain the background insights on our sample i.e. name of their organization, position in company, years of experience, etc.

In the second quarter we will solely be focusing on conducting interviews of our participants. This interview would contain questions about how the participant perceives security activities. And how the inclusion of these activities would affect various aspects of the agile process such as sprint velocity, confidence in the security of the product, adoption of security practices into the software development life-cycle, etc. We would also ask their opinions on what more could be done to increase security and robustness of the software product.

The third quarter of the year will be occupied in analyzing the interview responses and forming the results. The recording or the transcripts of the interviews would be thoroughly analyzed by performing qualitative analysis. This would give us more insight into how the practitioners of agile perceive the inclusion of security practices into the software development process. And finally based on upon the results a conclusion would be drawn summarizing the whole project.

The fourth quarter would focus on writing our project as a research paper and getting it published in a reputed journal or conference. Our findings would have to be communicated in a clear and concise way, so that the practitioners of agile could use them to their own good.

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] 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.

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

[5] 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.

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