Secure Agile Software Development Process

APPENDIX I

January 2022

Abdulhamid Aliyu Ardo, Julian Bass & Tarek Gaber

SECURE AGILE SOFTWARE DEVELOPMENT PROCESS

Interview Guide

Introduction

The aim of this research is to build a secure agile software development process model by integrating security practices. The study will explore the current state of agile security practices adopted by practitioners. The study will further explore how security influences the development of high-quality agile software.

I would like to ask you some questions about your experience of security engineering practices while using agile software development methods. Additionally, I would like to know your perception of security integration into normal agile processes. I will be interviewing a cross section of practitioners ranging from technical (software developers, security specialists, systems analyst, business analyst) to non-technical (decision maker/managers, project managers) to understand different business context.

Security Engineering while Using Agile Methods

1. Please can you describe your job role?
    a. How important is cybersecurity to your role?
    b. What project(s) are you working on currently that involves security tasks?
    c. Have you ever had any incidence of security breach from within/outside your organization?
2. Please describe how security issues influence the way you manage projects?
3. When you are planning a new software project, how do you take into account security features?
4. Please describe how you do security requirements gathering?
    a. (Probing) How are security requirements discussed and disseminated within your organization?
    b. How is security involved at the requirements gathering stage?
    c. Who else is involved in the security conversation at the requirements gathering stage for a new feature?
5. How do you consider security issues during the design stage of software development? (Probing) – Software, Hardware, Network, Storage?
6. Please describe what informs the company's decisions when selecting or developing appropriate secure software design methods, tools, and techniques?

a. (Probing) Do you have an organizational security policy, standard or guideline for software design and software architectures?
b. How do you ensure adherence to security technical strategies in software design?

7. Please describe the collaboration practices that you use in your organization to handle security?
    a. (Probing) Who is responsible for handling security audits in your current company?
8. Please describe the software security testing methods adopted in your organization?
    a. (Probing) How do you manage security vulnerability testing activities within your organization?
    b. Does your organization use security tools for the following;
        i. Vulnerability checks
        ii. Software testing
9. How do you do security risk assessment?
    a. Does your company use any security risk assessment framework?
    b. How do you ensure technologies are securely used?
10. How do you build security into deployment processes?
    a. (Probing) How does security impacts the CI/CD pipeline processes?
    b. Do Security Deployment tools fit into your deployment processes?
11. Would you say your organization has a security culture?
    a. (Probing) Please can you describe how the security culture is built or developed in your organization?
12. How do you ensure adherence to secure software regulatory policies?
    a. What security measures and checks are put in place by government to ensure companies are adhering to security policies?
13. (Open-Ended) Does your company face any security resource constraints during software development?
    a. How do you deal with budgetary constraints in the face of technological requirements?
    b. How often do you give security trainings to your staff?
    c. If you are to advice the government, what other areas of cybersecurity do you think needs urgent attention?

Closing Question

1. Is there anything else you think is relevant that has been missed?

Personal Details

1. What is your name?
2. What is your educational level and professional background?
3. What is your current job title?
4. How many people are in the current projects you are handling?
5. How long have you been working at the current company?
6. How long have you been working in the software industry?

Practice-Based Model Validation - Focus Group Interview Questions

1.Does the model represent the security practices you are using during agile software development?

[Probing] (a.) If yes, what other practices do you use that is not included in the model?

(b.) If no, what practices are you using to create secure agile software?

2.Do you think the model looked logical and understandable?

3.Is there anything you think I should have added in my model?

4.Is there anything you think shouldn’t have been added onto the model?

TABLE I: Participants' description

Company	Business Sector	Size	Interviewee Job Titles	Software Development Experience (Years)	Cybersecurity Experience (Years)
Company A	Cybersecurity Solutions	Large	Cybersecurity Analyst	11	5
Company B	Educational Software Solutions	SME	Product Manager	13	4
			Chief Technology Officer	24	11
			Senior Software Engineer	9	3
			Back-End Developer	9	3
			Product Manager	11	3
			Project Manager	16	2
			DevOps Engineer	9	3
Company C	Healthcare Services Company	SME	Software Developer	4	-
Company D	Financial Services	Large	Senior Software Engineer	17	4
Company E	IT Consulting	SME	Security Consultant	11	2
			Manager, IT Security	26	8
Company F	IT Service Management Company	Large	Security Technical Program Manager	9	6
Company G	Telecommunications Company	Large	VP, Operational Security	27	18
Company H	Manufacturing	Large	Manager, IT Security & Operational Risk	17	8
Company I	Customer Relationship Management	Large	Full-Stack Software Developer	8	-
Company J	Digital Forensics Services	SME	Security Consultant	12	8
Company K	Financial Solutions & Services	SME	Senior DevOps Engineer	11	6

			Frontline Manager	11	2
Company L	IT Services & Consulting	SME	Software Developer	6	-
Company M	Digital Services	SME	Security Team Lead	10	2
Company N	IT Services & Consulting	SME	Quality Assurance Analyst	8	5
Company O	Healthcare Services Company	SME	Front-End Developer	9	2

TABLE II: Security Practices

Security Practices		Quotes
Planning	Baseline security standards	"There is what we call HIPAA compliance security standards in the healthcare industry which me and others in my team that are involved in the security site of things have a good understanding of and ensure compliance always" (Front-End Developer, Company O).
	Industry regulatory standards	"We keep tap with periodic reviews to ISO standards like ISO 27001, ISO 9001 and PCI DSS or others and it's always easy for security team members to understand them since they are mostly little updates here and there to what we already know…" (Senior DevOps Engineer, Company K).
Requirements	Define evil user stories	"I would liaise with the business to determine what they want out of the project first and then it would be dependent on it that threat scenarios of attacking the system can be determined" (Cybersecurity Analyst, Company A).
	Brainstorm security features feasibility	"We work as a team to deliver the product as different security features are defined for different users like administrator, manager, and the others…" (IT Security Manager, Company E).
	Security backlog	"The security experts come up with a list of work items that are security related which needs to be considered as part of the system functionality which they discuss with the CTO and agree before we begin development…" (Software Developer, Company C).
	Misuse case estimation	"…while defining evil scenarios and tasks, we scope out how much time, … so we estimate on every single evil behaviour the amount of time that it takes us to handle the scenario during our development..." (Cybersecurity Analyst, Company A).
	Security metrics reporting	"All stakeholders meet like weekly to see where we are failing… in terms of like

		misconfigurations, vulnerability, and patch management. So, … there is a lot of visibility into security issues…" (IT Service Management, Company F).
	Threat modelling session	"We look at every possible way security issues like spoofing, tempering, repudiation, information disclosure and the likes can affect our system and we address them." (Manager, IT Security & Operational Risk, Company H).
	Security risk assessment	"The ISO 27001 risk management checklist is implemented in my company and out of that risk assessment process, our annual audit timetable is presented." (Manager, IT Security & Operational Risk, Company H)
	Evaluate security frameworks	"In adhering to secure-by-design principles of software engineering, we compare different peer-reviewed frameworks… we review how actively maintained it is, how many times it has been breached and how quick was it to be fixed?" (Cybersecurity Analyst, Company A).
	Architectural design review	"…we look at the security requirements and then we look at the architectural designs that are available… maybe a website that has to do with payments, we go for MV-6 and for real-time system we adopt event driven architectural design…" (Security Team Lead, Company M).
Implementation	Demoing security features	"…In the process of our development, we carry our clients along so whatever security feature we add we show them to get their feedback since we want to build what they are happy to use…" (Project Manager, Company B).
	Secure coding template	"There is a secure coding … documentation that defines coding best practice for development of software in my organization… It guides us securing our code and implement security in the design…" (Manager, IT Security & Operational Risk, Company H).
	Secure code review session	"From writing code to reviewing the code, we have peer review session where people look at it from security perspective, to deal with the

		vulnerabilities…" (Senior Software Engineer, Company D).
Testing	Security test plan	"… we have a QA team that are responsible for designing the blueprint to be used for all testing activities in a project. The document is written with inputs from QA team members and is periodically updated…" (Frontline Manager, Company K).
	Security regression tests	"…we have different tests that as part of quality assurance to ensure it does not break anything, to ensure there is what we call continuous integration. It does not mean if you build a new feature, it should break what is existing…" (Chief Technology Officer, Company B).
	Penetration testing	"I go beyond the mere code scans and conduct pen test because scanners may not give you the result of all vulnerabilities" (Security Technical Program Manager, Company F).
Deployment	Security retrospective	"…we do hold meetings to reflect on security mechanisms implemented and discuss ways of improvement by constantly addressing the security flaws…" (Chief Technology Officer, Company B).
	Secure CI/CD pipeline review	"…The DevOps team and the security specialist usually work to design a secured CI/CD pipeline and so on... Other security issues are sometimes discussed in the meeting…" (Senior Software Engineer, Company B).
	Secure audit plan	"…We rely on industry best practice, CIS benchmark which tells you about the benchmark for software development and secure coding and the rest to design our audit plan which is based on highest risk areas…" ((Manager, IT Security & Operational Risk, Company H).
	Security patching	"Part of our company security policy document are guidelines on security patch management to handle the ever-changing security vulnerabilities during software development." (VP, Operational Security, Company G)