PCM Tool: Privacy Requirements Specification in Agile Software Development

Mariana Peixoto[1], **Carla Silva**[1], **Ricarth Lima**[1], **João Araújo**[2], **Tony Gorschek**[3], **Jean Silva**[1]

[1]Universidade Federal de Pernambuco (UFPE), Brazil
[2]Universidade Nova de Lisboa (UNL), Portugal
[3]Blekinge Institute of Technology (BTH), Sweden

{mmp2,ctlls,rrsl,jcns}@cin.ufpe.br, p191@fct.unl.pt, tony.gorschek@bth.se

Abstract. *Recent research has pointed out that software developers face difficulties to specify requirements for privacy-sensitive systems. To help addressing this issue, this paper presents a tool, called PCM Tool, that supports the Privacy Criteria Method (PCM) - an approach designed to guide the specification of privacy requirements in agile software development.*

Link (for tool demo): *https://youtu.be/eGZiBiiMYWY*

1. Introduction

Agile Software Development (ASD) has brought benefits such as improving customer satisfaction, requirements changes at any development stage, frequent delivery of software, and close interaction with clients [Younas et al. 2017]. However, recent empirical studies have shown that requirements approaches for ASD still neglect non-functional requirements (NFRs) [Wagner et al. 2019].

Privacy has become a top concern in software development, especially due to incidents regarding unauthorized data exploration, misuse of information stored in social media websites, internet data, disclosure of personal information to third parties without users' consent and many more [Kalloniatis 2017]. In addition, research has shown that many software developers do not have sufficient knowledge and understanding about privacy, nor do they sufficiently know how to develop privacy-sensitive systems [Hadar et al. 2018]. For those reasons, Kalloniatis et al. [Kalloniatis et al. 2009] state that privacy violations can be avoided if privacy requirements are properly discovered during early phases of software development, when requirements specification occurs.

Aiming at guiding the specification of privacy requirements in ASD, an approach called Privacy Criteria Method (PCM) was defined [Peixoto et al. 2019b]. PCM was conceived based on a framework of Privacy Specification Capabilities [Peixoto and Silva 2018] and addressing automated support, understandability, team-oriented, simplicity and objectivity as essential quality factors for software requirements specifications in ASD [Medeiros et al. 2018].

In this paper, we detail the features of a tool developed to support PCM and we present the initial results of a quantitative and qualitative evaluation performed with post-graduate and undergraduate students. This paper is structured as follows. Section 2 briefly describes PCM. Section 3 presents PCM Tool features, architecture, evaluation and comparison with similar tools. Conclusions are presented in section 4.

2. Privacy Criteria Method

PCM is a method to guide software developers in specifying privacy requirements. PCM can be used in conjunction with any requirements specification technique, such as user stories that is widely used in ASD [Medeiros et al. 2018]. If the requirement to be specified involves the use, collection, retention or disclosure of personal information, it is necessary to initiate the specification with PCM.

Table 1 describes and exemplifies each attribute comprised in a specification using PCM [Peixoto et al. 2019a]. The example refers to a requirement of sharing user's personal data in a health care system. In this situation, it is necessary to ensure that the system allows sharing the user's personal information with his/her doctor. There are three actors involved: information Owner/controller (health care user); processor (system), and third party (doctor), who relate to each other. PCM contains private, public and semi-public types of personal information and its corresponding purpose of task context. For example, user's phone number is a semi-public information that is collected to be shared with the user's doctor (purpose of task context). In PCM, there are still privacy constraints given by the user privacy preferences or according to legal compliance regarding privacy.

The risk scenario is created, with the idea that vulnerability (Someone else - without permission - may access/share user's data), if exploited by a threat (Intrusion in user's life and Exposition of user's information), can generate harm (Intrusion may cause embarrassment to User and Exposure of personal information may cause problems). Then, a privacy mechanism (Provide awareness by presenting notification for the action; and Get users consent) is created to mitigate the risk scenario presented.

3. The PCM Tool

The PCM tool was developed to help the use of PCM by developers of privacy-sensitive systems. By using the PCM tool, all activities of PCM can be performed in a guided way to help avoiding the misuse of the attributes supported by PCM. The tool is available at `http://privacy-criteria.herokuapp.com/`.

3.1. Tool architecture

The tool architecture follows the structure Client/Server for Web. PCM tool was developed with Ruby on Rails technology, PostgreSQL as the database management system and Heroku as the cloud computing platform. In addition, HyperText Markup Language (HTML), Cascading Style Sheets (CSS), JavaScript and the Bootstrap framework were used to develop features for web. The tool is available at GitHub under the GNU Affero General Public License (AGPL).

3.2. Main functionalities and potential users

PCM was created to guide those software developers who are not experienced in developing privacy-sensitive systems. The tool presents documentation on how to use its functionalities, a catalog of privacy concepts, and examples of requirements specification using PCM. After creating an account, a user can create a project and start specifying privacy requirements using PCM. Each privacy specification can be recorded, edited and shared with other users, as shown in the Use Case Diagram presented in Figure 1.

Table 1: PCM Attributes [Peixoto et al. 2019a].

	Attributes	Examples
1	*ID* (unique identifier of PCM)	PCM01
	Privacy Requirement	Health Care User shares Personal Data
	Detailed description of the privacy requirement	The system must allow the option of sharing users' personal data
	Information Source (person responsible for the information)	Stakeholder (Alice)
	Priority (Low Critical; Regular; Critical; or Very Critical)	Critical
2	*Owner/Controller* is the owner of personal information	Health Care User
	Processor is the person/system that processes the personal information according to the controller instructions	System
	Third Party is a person who is authorized to access the owner/controller personal information	Doctor
3	*Trust relationship between actors* is the relationship that shows the trust between actors regarding the disclosure of personal information	Health Care User trusts System and Doctor
4	*Private Information* is the personal information that no one can access	Doctor name
	Public Information is the personal information that everyone can access	User Full Name
	Semi-Public is the personal information that can be accessed under specific conditions	Photo, Email and Phone number
5	*Purpose of task context according to usage* indicates what is the purpose of having personal information	For identification
	Purpose of task context according to usage retention indicates how long personal information will be stored	While using the system
6	*Privacy constraint according to compliance* is a limitation in accordance with a privacy policy or law	GDPR consent: Doctor may not share the data without user consent
	Privacy constraint according to user preference is a limitation indicated by the owner/controller	Partial and temporary sharing
7	*Vulnerability* is a system weakness related to personal information that can be exploited by a threat	Someone else - without permission - may access/share user's data
	Threat is a potential incident that threatens personal information by exploiting a vulnerability	Intrusion in user's life; Exposition of user's information
	Harm is the result of a privacy violation of the owner/controller personal information	Intrusion may cause embarrassment to user; Exposure may cause problems
8	*Privacy mechanism* is the privacy strategy used to mitigate the risk scenario or the privacy constraint	Awareness by presenting notification for the action and Get users consent

3.3. An Example of Use

The main goal of the PCM Tool is supporting the specification of privacy requirements with PCM. Figure 2 presents the tool's screen related to a privacy criteria specification using PCM (scenario and explanation from Section 2). Each privacy criteria specification refers to a scenario of system use, such as an user story or an use case that starts with basic information specification. The PCM tool guides users with tips of how to fill each field of the privacy criteria specification, as explained in Table 1[1].

[1] 1. Basic Information; 2. Actors; 3. Trust Relation of Actors; 4. Personal Information; 5. Purpose of Task Context; 6. Privacy Constraint; 7. Risk Scenario; 8. Privacy Mechanisms.

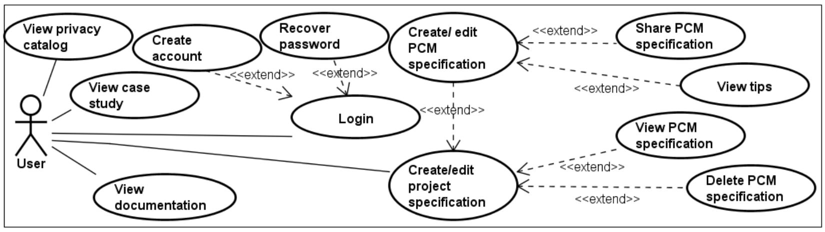


Figure 1. Use Case Diagram for PCM Tool.

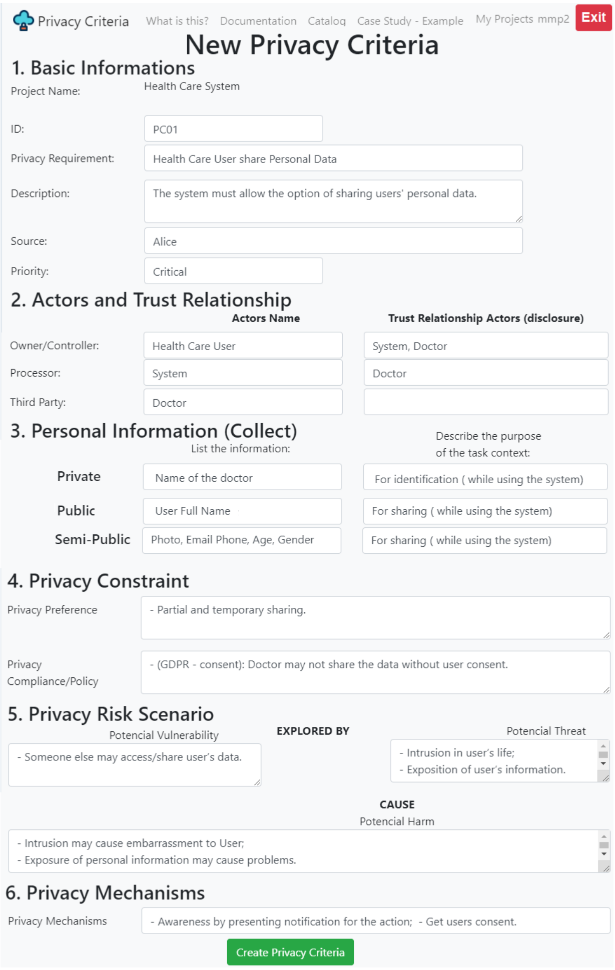
3.4. Tool evaluation

For evaluating the method and tool, we performed a controlled experiment with 34 post-graduate students of a Requirements Engineering (RE) course. These students were information technology analysts with industry experience [Peixoto et al. 2019b]. This experiment has shown that the quantity of privacy requirements specified by using PCM Tool was higher (91.86%) than the number of privacy requirements specified using User Stories and Acceptance Criteria (68.46%). Regarding quality, only specifications created using PCM Tool were evaluated by considering how Well-formed (the specification should include at least one of each PCM attribute (Table 1)), Atomic (the specification should express a requirement for exactly one feature), and Minimal (the specification should only contain PCM attributes and nothing more) each of them were [Peixoto et al. 2019b]. From 59 specifications, the results indicated an overall good quality: 44 out of 59 well-formed, 54 out of 59 atomic and 58 out of 59 minimal specifications.

Subsequently, we performed qualitative evaluations with two groups of undergraduate students of computer science courses (15 from course 1 and 11 from course 2). In this case, we asked the participants to specify a privacy-sensitive scenario using PCM Tool. Afterwards, we applied the Technology Acceptance Model (TAM) instrument that has questions about Perceived Ease of Use (PEU) (7 questions); Perceived Usefulness (PU) (6 questions); Behavioural Intention to Use (BIU) (2 questions); and Attitude Toward Usage (ATU) (3 questions) [Hart and Staveland 1988]. The results of the exploratory analysis using TAM showed that the general means and standard deviations of each scale were: PEU (course 1 - 5.07 and 1.318) and (course 2 - 4.64 and 1.856); PU (course 1 - 3.53 and 1.979) and (course 2 - 4.23 and 1.896); BIU (course 1 - 4.30 and 1.725) and (course 2 - 3.86 and 1.642); and ATU (course 1 - 5.27 and 1.095) and (course 2 - 5.06 and 1.619). Therefore, we observed in the results that ATU presented the best evaluations in both courses, showing that participants believe that using PCM is worth. Also, PEU and BIU presented the worst evaluations in course 1 and in course 2, respectively, showing that course 1 participants find the tool less easy to use, and course 2 participants have fewer plans to use PCM.

3.5. Comparison with similar tools

In the past few years, the RE community recognized the need for approaches to deal with privacy. For example, Mai et al. [Mai et al. 2018] provided a method that supports the specification of security and privacy requirements with Use Cases. Ayala-Rivera and Pasquale [Ayala-Rivera and Pasquale 2018] proposed a 6-step approach, called GuideMe, that supports elicitation of requirements that trace obligations of the General Data Protection Regulation [GDPR 2018] to the privacy controls that fulfill these obligations. Al-



New Privacy Criteria

1. Basic Informations

Project Name:	Health Care System
ID:	PC01
Privacy Requirement:	Health Care User share Personal Data
Description:	The system must allow the option of sharing users' personal data.
Source:	Alice
Priority:	Critical

2. Actors and Trust Relationship

	Actors Name	Trust Relationship Actors (disclosure)
Owner/Controller:	Health Care User	System, Doctor
Processor:	System	Doctor
Third Party:	Doctor	

3. Personal Information (Collect)

	List the information:	Describe the purpose of the task context:
Private	Name of the doctor	For identification (while using the system)
Public	User Full Name	For sharing (while using the system)
Semi-Public	Photo, Email Phone, Age, Gender	For sharing (while using the system)

4. Privacy Constraint

Privacy Preference	- Partial and temporary sharing.
Privacy Compliance/Policy	- (GDPR - consent): Doctor may not share the data without user consent.

5. Privacy Risk Scenario

Potencial Vulnerability	EXPLORED BY	Potencial Threat
- Someone else may access/share user's data.		- Intrusion in user's life; - Exposition of user's information.

CAUSE

Potencial Harm

- Intrusion may cause embarrassment to User;
- Exposure of personal information may cause problems.

6. Privacy Mechanisms

Privacy Mechanisms	- Awareness by presenting notification for the action; - Get users consent.

Figure 2. Privacy Requirements Specification using PCM Tool - an Example.[2]

though these and other approaches emerged to support privacy requirements, none of them is able to be used in the context of ASD, as well as they were not empirically evaluated.

Kalloniatis et al. [Kalloniatis et al. 2009] stated that many goal-oriented modeling languages, which have tool support, can be used to capture privacy requirements. However, in previous work we analyzed three goal-oriented modeling languages regarding their support to capture the privacy concepts present in the Privacy Specification Capabilities framework [Peixoto and Silva 2018]. Our analysis concluded that these languages are not able to model many of the privacy concerns present in the framework.

4. Conclusions and Future Work

This paper presented a tool to support PCM, a method to aid the specification of privacy requirements in ASD. Indeed, recent research has shown developers' lack of knowledge on privacy requirements and negligence in dealing with NFRs in ASD. PCM tool evaluation has shown that although using PCM assist the specification of privacy requirements, it still faces barriers for adoption, as shown in evaluations with Computer Science students.

Future work includes improving the usability of both method and tool. PCM Tool

[2] Icons made by bqlqn from www.flaticon.com, licensed by CC 3.0 BY.

needs improvements regarding scalability and other technical aspects, such as enabling reuse of artifacts among different projects and integration with agile tools. Further evaluations have to be conducted and, in particular, a survey with privacy and agile experts.

Acknowledgments

This work was financed by the Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brazil (CAPES) - Finance Code 001, and supported by the KKS foundation through the S.E.R.T. Research Profile project at SERL - Blekinge Institute of Technology.

References

Ayala-Rivera, V. and Pasquale, L. (2018). The grace period has ended: An approach to operationalize gdpr requirements. In *26th International Requirements Engineering Conference (RE)*, pages 136–146. IEEE.

GDPR (2018). General data protection regulation. `https://eugdpr.org/`.

Hadar, I., Hasson, T., Ayalon, O., Toch, E., Birnhack, M., Sherman, S., and Balissa, A. (2018). Privacy by designers: software developers' privacy mindset. *Empirical Software Engineering*, 23(1):259–289.

Hart, S. G. and Staveland, L. E. (1988). Development of nasa-tlx (task load index): Results of empirical and theoretical research. In *Advances in psychology*, volume 52, pages 139–183. Elsevier.

Kalloniatis, C. (2017). Incorporating privacy in the design of cloud-based systems: a conceptual meta-model. *Information & Computer Security*, 25(5):614–633.

Kalloniatis, C., Kavakli, E., and Gritzalis, S. (2009). Methods for designing privacy aware information systems: a review. In *13th Panhellenic Conference on Informatics (PCI)*, pages 185–194. IEEE.

Mai, P. X., Goknil, A., Shar, L. K., Pastore, F., Briand, L. C., and Shaame, S. (2018). Modeling security and privacy requirements: a use case-driven approach. *Information and Software Technology*, 100:165–182.

Medeiros, J., Vasconcelos, A., Silva, C., and Goulão, M. (2018). Quality of software requirements specification in agile projects: A cross-case analysis of six companies. *Journal of Systems and Software*, 142:171–194.

Peixoto, M. M. and Silva, C. (2018). Specifying privacy requirements with goal-oriented modeling languages. In *XXXII Brazilian Symposium on Software Engineering (SBES)*, pages 112–121. ACM.

Peixoto, M. M., Silva, C., Araújo, J., and Gorschek, T. (2019a). Supplementary Material. `https://tinyurl.com/y6hsngtz`.

Peixoto, M. M., Silva, C., Araújo, J., Gorschek, T., and Vasconcelos, A. (2019b). Submitted and under review. For a copy, ask to mmp2@cin.ufpe.br.

Wagner, S. et al. (2019). Status quo in requirements engineering: A theory and a global family of surveys. *ACM Trans. on Software Eng. and Methodology (TOSEM)*, 28(2):9.

Younas, M., Jawawi, D., Ghani, I., and Kazmi, R. (2017). Non-functional requirements elicitation guideline for agile methods. *Journal of Telecommunication, Electronic and Computer Engineering (JTEC)*, 9(3-4):137–142.