Privacy by Socio-Technical Design

a collaborative approach for privacy friendly system design

Martin Degeling
Institute for Software Research
Carnegie Mellon University
degeling@cmu.edu

Christopher Lentzsch, Alexander Nolte, Thomas Herrmann, Kai-Uwe Loser
Institute for Applied Work Science
Ruhr-University Bochum
{lentzsch, nolte, herrmann, loser}@iaw.rub.de

***Abstract*— Lately the European data protection directive has increased the attention for privacy by design (PbD). The idea behind this system and software design approach is to not consider privacy as an add-on or legal requirement but to foster the development of privacy friendly technology right from the beginning. Current PbD approaches however mainly focus on technological aspects of privacy. They rarely consider the context in which software systems are build and used. The context however plays a vital role especially with respect to the future usage of a system in an organizational environment. We propose to use established socio-technical design approaches, in which multiple stakeholders collaborate on process models, as a basis for privacy by design. We adapt them to incorporate aspects relevant for privacy aware design and introduce a tool that can support question-based evaluation and collaborative work on processes that make use of personally identifiable information.**

Keywords—privacy by design; socio-technical sysstems

I. INTRODUCTION

During the last few years there has been a steady increase in the interest for building privacy-friendly software that ultimately led to the emergence of the research field of privacy engineering [1]. It stems from the need to build products with privacy in mind in every step of the design process. Cavoukian [2] was one of the first to summarize the privacy by design principles that emphasize user-centricity and provide indications for benefits of increased privacy and security when systems are developed transparently and proactively.

Privacy by design principles have become increasingly relevant as evident by the amount of scholarly papers published on the topic as well as by its inclusion in legislation like the new European Data Protection Directive [4]. Despite the fact that numerous privacy enhancing technologies can be used with any software there is still a lack of work on how PbD can actually be supported during software development [3]. The fact that there is limited adoption of privacy enhancing technologies by users as well as system designers begs the question why these technologies are not used to a broader extent. Gürses and Alamo [1], in line with a recent ENISA report [6], state that engineering privacy by design requires a multidisciplinary approach in which "Data protection authorities should play an important role providing independent guidance and assessing modules and tools for privacy engineering" [6, p. 4]. One way to arrive at such approaches is to foster collaboration of people from different disciplines during the design of software that includes personally identifiable information (PII).

In this paper we propose an approach that extends existing methods of socio-technical design by including privacy related aspects. Our approach combines collaborative process design workshops with a web-based system that fosters critical reflection and discussion on such designs.

II. RELATED WORK

The fuzziness of the concept "privacy" is one of the main challenges of PbD and privacy engineering [7]. There are legal, regional and cultural differences with respect to what is to be achieved by protecting privacy. This emphasizes the need of collaboration when systems are developed with privacy in mind to incorporate the different perspectives of potential users. Especially legal requirements for handling of PII, despite the fuzziness of the concept of privacy [8], have led the German discussion of *data protection goals* [9] that are thought to be workable constructs when designing process that involve PII. The data protection goals extend the widely known computer security goals (confidentiality, integrity and availability) with respect to privacy related goals such as *transparency*, *unlinkability* and the *ability to intervene* [9]. While unlinkability refers to mechanisms to enforce purpose binding, the *ability to intervene* requires data processors to prove that they can actually control and disrupt specific PII data flows, e.g. if required by the data subject. These goals were recently chosen to be the standard model for data protection audits by the German conference of data protection officials. Unlinkability for example can be achieved by minimizing the amount of data collected. The data protection goals are in line with other, less process but more technology oriented approaches like the one proposed by Gürses et al. [10]. They argue that engineering privacy by design should always be based on minimizing data since the amount and risk of PII collected within a product or process predetermines the following iterative steps of development like requirements analysis, threat modeling, security analysis and implementation. This leaves room for methods that support these iterative steps. Notario et al. [11] suggest to use cases as a methodology to elicit requirements. The value of use cases within that methodology is to bring together all stakeholders that have an interest in processing PII such as legal staff, business consultants, business analysts, data analysts and software architects. Notario et al. (ibid.) also stress the importance of models in the process of privacy engineering. Still, they miss a specific idea of how these

978-1-5090-4607-2/16 $31.00 © 2016 IEEE
DOI 10.1109/CIC.2016.75

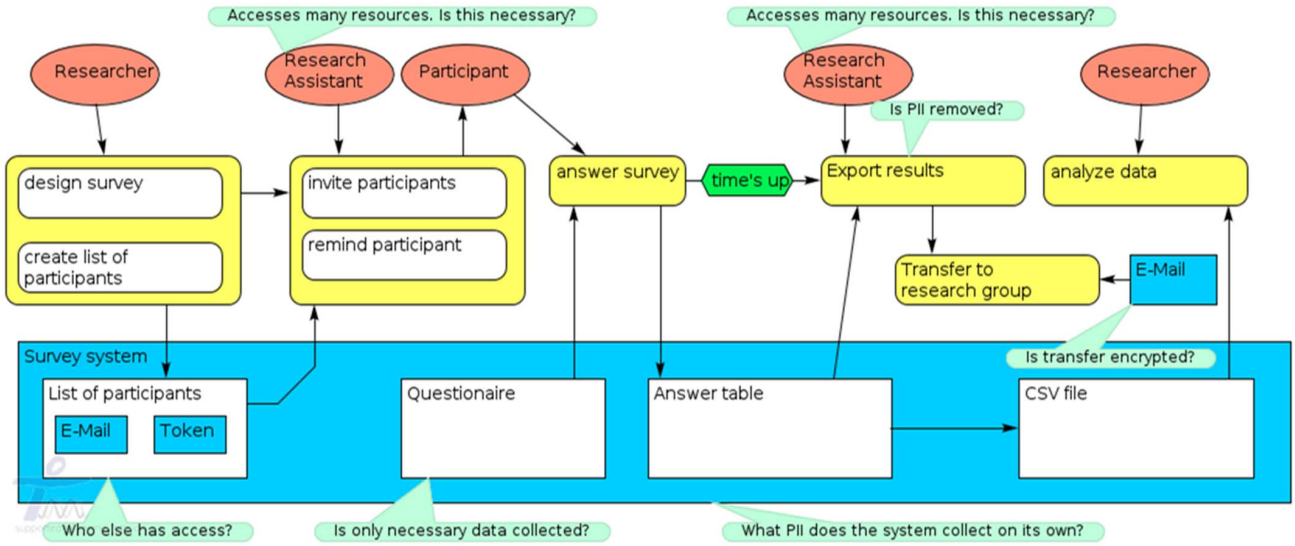

Fig. 1. *SeeMe model of the survey process with added comments regarding privacy.*

models should be developed and discussed collaboratively and how to bring all stakeholders together. The socio-technical design approach can provide a suitable solution for this gap.

Socio-technical design first became a field of interest in the early 1950s in the face of the ongoing industrialization [12]. During that time researchers realized that it is necessary to consider the social context of people in order for technology to have the desired effect. They also found that the introduction of technology inevitably has an effect on the working environment which again has an influence on how technology is used. This led to the development of a number of approaches which were subsumed under the umbrella of the term socio-technical design (STD). These approaches aim at giving "equal weight to social and technical issues when new work systems are being designed" [13].

Most STD approaches focus on workshops in which current and future users of a system alongside domain experts and software developers create a conceptualization of a future system [14]–[16]. It is common to start conceptualization by analyzing the current state of a system or process by visualizing it in graphical models. These models are then subsequently used as a basis to identify problems and discuss future designs. Arriving at a sufficient design usually requires multiple workshops as well as phases in between in which designs are reflected and tested [17]. Results from these tests then serve as an input for future workshops and future design iterations. STD can thus be perceived as a mutual adaptation process between a design and its implementation in the work place.

Privacy is a multi-facetted problem that can be leveraged with organizational as well as technical approaches. Socio-technical design can serve as a means to consider both aspects and come up with solutions that all participants agreed upon when used in the context of privacy by design. Through socio-technical design it is possible to integrate multiple stakeholders into the design process and to identify problems within processes that are potentially be overlooked otherwise because they are often considered less important [18]. Therefore, legal and privacy/security can also help to make decisions on tradeoffs that have to be made with regard to the use of privacy enhancing technologies and usability, efficiency or implementation costs.

III. Modeling an Example Process in SeeMe

Imagine the design of a survey based study by a university where participants are contacted by email and asked to use a web-based system to answer a short questionnaire. Study designs like this have to consider local privacy regulations and – depending on local practices – have to be approved by institutional review boards or data protection offices. A process model that reflects the necessary steps is shown in figure 1.

In order for a design artefact for a future system to be useful it has to cover social and technical aspects at the same time. It also has to be easily understood by those involved in the design and it has to be useful for those that later use the design to develop software based on it and conduct organizational changes in order for the software to be used effectively. The SeeMe modeling notation [19] thus can be perceived as being ideal for a task like this. It is capable of covering social and technical aspects of a process within the same visualization. SeeMe only consists of three basic elements and has been proven to be easy to understand by a large variety of stakeholders on multiple occasions. Furthermore, SeeMe also allows for explicitly displaying vagueness. This is crucial for depicting real life processes since real life phenomena sometimes cannot and should not be expressed formally. At the same time SeeMe offers all constructs necessary to depict complex decisions and can thus be used as a basis for software development.

The example process model (fig. 1) makes use of SeeMe. The process involves roles (depicted as red ellipses) like *participant*, *researcher* and *research assistant* who execute activities such as *invite participants* and *remind participants* (depicted as yellow rectangles with round corners). The process involves assistants who will send out unique links with unique tokens, e.g. encoded within the URL to the survey to a *list of participants* (an entity depicted as blue rectangle) created by the researchers. They will also remind participants if codes were not used. When the time is up the survey is closed and the assistants

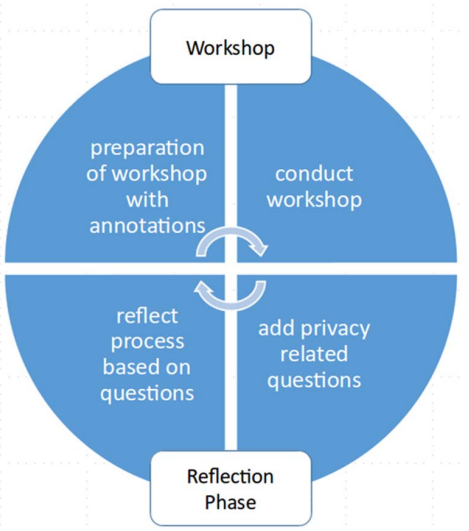

Fig. 2. Iterative process of collaborative modelling in collocated workshops and reflection phases

exports the answers from the survey systems as a CSV file and sends it to the research group via email. This rather simple process of conducting a survey can pose various privacy related issues such as protecting the identity of the participants or general questions about data handling within research groups.

Additional stakeholders that we omit in this example are third parties like the company providing the survey system or researchers from other institutions that would also like to work with the raw data.

IV. Privacy by Socio Technical Design: A Mixed Collaboration Approach

As described above models can take a central role in privacy by socio-technical design. In order to arrive at a privacy friendly system and corresponding organizational process those models have to be embedded in an approach that covers both aspects. Therefore, we propose an approach that intertwines phases of collaborative work in workshops with phases of asynchronous collaboration and reflection (see fig. 2). This approach is based on a well-established method that has been used in various socio-technical design projects [17], [20]–[23]. It is based on the development of graphical process models in workshops. After a workshop privacy experts review these models and add privacy related questions. The models are then distributed among workshop participants and other interested stakeholders who are asked to answer those questions by adding annotations. Those annotations subsequently serve as a basis for the next workshop during which they are discussed. In what follows we will describe this approach in detail.

A. Collaborative modeling workshops

The purpose of the creating process models in workshops is to be able to reflect multiple perspectives and aspects of real work environments. However, those conducting the work or in our case a survey study, are not always capable of analyzing their work environment. Although, for example, all researchers are trained to reflect on their practices and create survey with respect to participants' privacy, day to day practices often look different and when tasks are carried under time pressure or by non-experienced assistants deviations from trained process occur. Therefore, to reflect the actual process in a process model they have to be supported by experts which serve as facilitators of a workshop. These facilitators guide workshops by asking participants how participants conduct their work and what they do at a certain point in time. The contributions by the participants are integrated into a graphical process model. This model subsequently serves as a basis for discussion on potential improvements as well as on how the future system has to be designed to suit the work environment of current and future users. In order to arrive at a suitable design, the facilitator usually asks the users a set of predefined questions such as: "Where do you see issues with the current process?" or "What support do you need in order to fulfill your tasks?".

Altering this approach in order to fit the context of privacy by design mainly requires three alterations to the initial design:

1. The involvement of privacy experts as participants
2. A focus on potentially privacy relevant aspects of work processes
3. The inclusion of questions regarding privacy into the design phase

The first two aspects can be considered to be inevitably intertwined since it can be expected that regular users of a system will not be capable of identifying parts of a work process that are potentially relevant for privacy on their own. The second and third aspect also implicitly include the requirement for facilitators and privacy experts to collaborate more closely not only during workshops but also during its preparation.

B. The SeeMe web editor for collaborative modeling

Designing a suitable socio-technical system cannot solely happen within modeling workshops. Due to the fact that social and technical aspects mutually influence each other it is not possible to analyze all potential effects of technology on a social system and vice versa. It is thus crucial to apply an evolutionary approach in which designs are created, tested and refined. In order to support this approach we propose a web-based editor as a means to access process models that have been created during workshops and to discuss these models using annotations. The SeeMe web editor is designed to offer easy access to models without the need of special tooling or sophisticated knowledge of models and modeling notation. Models are kept in sync among all collaborators and the individual work areas of other modelers are visualized.

The SeeMe web editor thus allows for participants of workshops to reflect upon the design when it is put into practice and leave comments on models. These comments can then subsequently be used in future workshops to discuss potential problems and to alter the design accordingly. In addition, the web editor supports a question based re-evaluation of a process that can be asked questions related to the data protection goals or common privacy patterns [24]. This enables non-privacy experts to evaluate common privacy practices and optimize a process before details are discussed with privacy experts in a consecutive workshop.

Referring to the example in fig. 1 common questions about data encryption can be guided by questions created by a PbD/plugin. Researchers can then reflect on these questions and propose changes, like e-mail encryption or transportation of data on encrypted device.

While this can help to avoid common privacy and security pitfalls a privacy expert who prepares and facilitates a second workshop can address more complex questions like the design of the survey or how to create and maintain token distribution systems where only a trusted third party is able to de-anonymize participants instead of delegating it to assistants.

Due to the participative process of model creation and elicitation we can expect an increased buy-in to the process created. As more participation leads to a higher acceptance of the process [25] and higher involvement motivates implementation of otherwise disregarded features [18].

V. Conclusion and Future work

In this paper we described how privacy by design can be incorporated in established, collaborative methods for designing socio-technical systems. We suggest that privacy experts should take part in workshops were processes are modelled and propose a question-based evaluation of processes to enable non-privacy experts to avoid common privacy and security issues.

In our future work we aim at evaluating past workshops to sharpen the methodology so that it can be applied to the design of privacy sensitive socio-technical systems. After including common privacy patterns into PbD plugins of the SeeMe web editor we also aim at evaluating our approach in workshops with the data protection office of a university that handles cases like described above.

References

[1] S. Gürses and J. M. del Alamo, "Privacy Engineering: Shaping an Emerging Field of Research and Practice," *IEEE Secur. Priv.*, vol. 14, no. 2, pp. 40–46, Mar. 2016.

[2] A. Cavoukian, "Privacy by Design - The 7 Foundational Principles," 2009.

[3] S. Spiekermann, "The challenges of privacy by design," *Commun. ACM*, vol. 55, no. 7, p. 38, Jul. 2012.

[4] European Parliament, *General Data Protection Regulation*. 2016.

[5] S. Gürses and J. M. del Alamo, "Privacy Engineering: Shaping an Emerging Field of Research and Practice," *IEEE Secur. Priv.*, vol. 14, no. 2, pp. 40–46, Mar. 2016.

[6] J. Domingo-Ferrer, M. Hansen, J.-H. Hoepman, D. Le Métayer, R. Tirtea, S. Schiffner, G. Danezis, European Union, and European Network and Information Security Agency, *Privacy and data protection by design - from policy to engineering*. Heraklion: ENISA, 2014.

[7] S. Spiekermann, "The challenges of privacy by design," *Commun. ACM*, vol. 55, no. 7, p. 38, Jul. 2012.

[8] P. M. Schwartz and D. J. Solove, "The PII Problem: Privacy and a New Concept of Personally Identifiable Information," *N. Y. Univ. Law Rev.*, vol. 86, p. 1814, 2011.

[9] M. Rost and K. Bock, "Privacy by design and the new protection goals," European Privacy Seal, 2011.

[10] F. S. Gürses, C. Troncoso, and C. Diaz, "Engineering Privacy by Design," *Comput. Priv. Data Prot.*, 2011.

[11] N. Notario, A. Crespo, Y.-S. Martin, J. M. Del Alamo, D. Le Metayer, T. Antignac, A. Kung, I. Kroener, and D. Wright, "PRIPARE: Integrating Privacy Best Practices into a Privacy Engineering Methodology," in *2015 IEEE Security and Privacy Workshops (SPW)*, 2015, pp. 151–158.

[12] E. Trist and K. Bamforth, "Some social and psychological consequences of the Longwall method," *Hum. Relat.*, vol. 4, no. 3, pp. 3–38, 1951.

[13] E. Mumford, "A Socio-Technical Approach to Systems Design," *Requir. Eng.*, vol. 5, pp. 125–133, 2000.

[14] T. Herrmann, "Systems Design with the Socio-Technical Walkthrough," in *Handbook of Research on Socio-Technical Design and Social Networking Systems*, B. Whitworth and A. de Moor, Eds. IGI Global, 2009.

[15] F. Kensing, J. Simonsen, and K. Bodker, "MUST: A Method for Participatory Design," *Hum.-Comput. Interact.*, vol. 13, no. 2, pp. 167–198, 1998.

[16] K. Bødker, F. Kensing, and J. Simonsen, *Participatory IT Design: Designing for Business and Workplace Realities*. 2009.

[17] A. Nolte and T. Herrmann, "Facilitating Participation of Stakeholders during Process Analysis and Design," in *Proceedings of the 12th International Conference on the Design of Cooperative Systems*, Trento, Italy, 2016.

[18] K.-U. Loser and M. Degeling, "Security and Privacy as Hygiene Factors of Developer Behavior in Small and Agile Teams," presented at the 11th Human Choice and Computers International Conference, Turku, Finland, 2014.

[19] T. Herrmann, "SeeMe in a nutshell.," *Available Online*, 2006.

[20] K.-U. Loser, A. Nolte, M. Prilla, R. Skrotzki, and T. Herrmann, "A Drifting Ambient Assisted Living Project," in *Phenomenology, Organizational Politics and IT Design: The Social Study of Information Systems*, 2012.

[21] T. Herrmann, G. Kunau, K.-U. Loser, and N. Menold, "Sociotechnical Walkthrough: Designing Technology along Work Processes," in *Artful Integration: Interweaving Media, Materials and Practices. Proceedings of the eighth Participatory Design Conference 2004, Toronto, Ontario, Canada, July 27 - 31*, 2004, vol. 1, pp. 132–141.

[22] T. Herrmann, K.-U. Loser, and K. Moysich, "Intertwining Training and Participatory Design for the Development of Groupware Applications," in *In: Proceedings of PDC 2000, CPSR, Palo Alto.*, 2000, pp. 106–115.

[23] T. Herrmann, M. Prilla, and A. Nolte, "Socio-technical Process Design—The Case of Coordinated Service Delivery for Elderly People," in *Blurring the Boundaries Through Digital Innovation*, F. D'Ascenzo, M. Magni, A. Lazazzara, and S. Za, Eds. Springer International Publishing, 2016, pp. 217–229.

[24] J. Kahrmann and I. Schiering, "Patterns in Privacy - A Pattern-Based Approach for Assessments," in *Privacy and Identity Management for the Future Internet in the Age of Globalisation*, J. Camenisch, S. Fischer-Hübner, and M. Hansen, Eds. Springer International Publishing, 2014, pp. 153–166.

[25] [M. den Hengst and G. J. D. de Vreede, "Collaborative business engineering: a decade of lessons from the field," *J. Manag. Inf. Syst.*, vol. 20, no. 4, pp. 85–114, 2004.