Poster: A Critical Analysis of Privacy Design Strategies

Michael Colesky, Jaap-Henk Hoepman
Digital Security
Radboud University Nijmegen
Nijmegen, The Netherlands
{mrc, jhh} @cs.ru.nl

Christiaan Hillen
Valori Security
Valori
Nieuwegein, The Netherlands
christiaanhillen@valori.nl

***Abstract*—The upcoming General Data Protection Regulation is quickly becoming of great concern to organizations which process personal data of European citizens. It is however nontrivial to translate these legal requirements into privacy friendly designs. One recently proposed approach to make 'privacy by design' more practical is privacy design strategies. This paper improves the strategy definitions and suggests an additional level of abstraction between strategies and privacy patterns: 'tactics'. We have identified a collection of such tactics based on an extensive literature review, in particular a catalogue of surveyed privacy patterns. We explore the relationships between the concepts we introduce and similar concepts used in software engineering. This paper helps bridge the gap between data protection requirements set out in law, and system development practice.**

I. Introduction

An aspect of growing concern for organizations lately is the recent progress in the European General Data Protection Regulation (GDPR) [1]. As a binding legislation in the European Union, the GDPR enforces a number of restrictions on both European organizations and those subject to European data protection law, for e.g. through the expected Privacy Shield safeguards [2]. Every organization targeting EU citizens should be aware of the potential repercussions involved in mishandling personal data.

In light of this we show the exploration of privacy by design as a design philosophy which can be made to map legal requirements, particularly those of the GDPR, into software engineering. We make this more concrete through the use of privacy patterns (a kind of software design pattern), a less abstracted design medium. We connect this through privacy design strategies, which help link privacy by design to the GDPR [3].

Privacy design strategies (or just strategies) are a legislation-aware software engineering approach to privacy by design. We link these to a substantial number of privacy patterns [4] and this correlation results in the introduction of privacy design tactics (or just tactics). Our approach is comparable to that of others in the field [5] [6], but features a larger assortment of patterns.

A main focus of the paper itself, these tactics provide an additional level of abstraction between strategies and patterns. When taken as specifically 'architectural tactics', they allow for a further connection opportunity. Architectural tactics serve to achieve system quality attributes – important non-functional properties of a system (in this case, 'privacy protection') [7]. This presents a first step in exploring the relationship between software architecture and privacy engineering.

We use the term 'privacy protection', similarly to ISO 15944-8 [8], as an extension of the engineering oriented term 'privacy' to include considerations in data protection. We see this as a better alternative to using the terms interchangeably.

II. Overview

We redefine Hoepman's [3] original strategies as *distinct architectural goals in privacy by design to achieve a certain level of privacy protection*. Over a hundred privacy patterns [4] were collected and mapped to these strategies. The correlation, however, presented an opportunity for less broad variations which achieve the strategy goals – tactics. We define tactics as *approaches to privacy by design which contribute to the goal of an overarching privacy design strategy*.

There are four data oriented strategies and four policy orientated ones [3]. Each comprise of multiple tactics:

Data oriented strategies and their tactics

MINIMISE:	EXCLUDE, SELECT, STRIP, DESTROY
SEPARATE:	DISTRIBUTE, ISOLATE
HIDE:	RESTRICT, MIX, OBFUSCATE, DISSOCIATE
ABSTRACT:	SUMMARIZE, GROUP

Policy oriented strategies and their tactics

INFORM:	SUPPLY, NOTIFY, EXPLAIN
CONTROL:	CONSENT, CHOOSE, UPDATE, RETRACT
ENFORCE:	CREATE, MAINTAIN, UPHOLD
DEMONSTRATE:	AUDIT, LOG, REPORT

An example of the mapping between strategies and patterns, specifically the ENFORCE strategy, is shown in TABLE I. The patterns will not however be explored in depth, rather the focus will be on the concepts surrounding the definitions and associations.

Some of the strategies, specifically those more focused on data than policy, relate very closely to one another. This includes how ABSTRACT relates to MINIMIZE and how SEPARATE relates to HIDE. These relations can be seen through

a form of privacy protection risk management. The first pair (ABSTRACT and MINIMIZE) reduce the impact of privacy violations, through limiting usage and detail of personal information. The latter (SEPARATE and HIDE) reduce the likelihood of those violations, by preventing correlation and exposure of access, association, visibility, or understandability.

TABLE I. ENFORCE TACTICS FOR PRIVACY PATTERNS

Tactics & Patterns		Description
CREATE	Creating Privacy Policy [9]	A legal document which conveys the risks an organization's activities may pose to a person's privacy and how it endeavors to reduce them.
	Fair Information Practices [10]	The FTC's proposed principles concerning informational privacy in the US online market - less comprehensive than the EU or OECD ones.
	Respecting Social Organizations [10]	Disparity between the intimacy and trust of systems and users may cause invasions of privacy. This pattern suggests Involving users in the privacy policy creation process.
MAINTAIN	Appropriate Privacy Feedback [11]	"Appropriate feedback loops are needed to help ensure people understand what [information] is being collected and who can see [it]"
	Maintaining Privacy Policy [9]	"As services evolve so does the amount of personal information they require, [this] pattern tackles [the evolution] of privacy policies"
	Privacy Management System [3]	Personalized systems may cater to privacy preferences on a user by user basis. These preferences should be adhered to.
UPHOLD	Usage Control Infrastructure [12]	A system which supports protocol and application independent data flow tracking, sticky policies, and external policy enforcement.
	Distributed Usage Control [13]	Once access to data has been granted, control over that access may be lost. This pattern maintains rules through distributed systems.
	Sticky Policies [14]	When personal information is processed through multiple entities, they act under obligatory previous disclosed policies to prevent violations.

Between the strategies numerous examples of processing of personal data, according to those defined in the GDPR, are accounted for. These are included in their renewed definitions, but also provide an opportunity for correlation with Solove's [15] taxonomy of privacy. The relationship between strategies and Solove's taxonomy is shown in TABLE II.

TABLE II. PRIVACY AFFECTING ACTIONS IMPACTED BY STRATEGIES

Taxonomy Group		Applies to	ENFORCE	DEMONSTRATE	INFORM	CONTROL	MINIMIZE	ABSTRACT	SEPARATE	HIDE
Processing										
	Collection									
	Dissemination									
	Invasion									

We also decided to rename one of the strategies: ABSTRACT (formerly AGGREGATE). Mainly this decision is based on prominent misuse and thus negative connotation of the term 'aggregation' [8]. The new term better encapsulates the intended purpose of the strategy.

III. CONCLUSION

In our work the connection between data protection legislation and the implementation of privacy by design has been strengthened. We provided a link between known best practices (privacy patterns) and a recent implementation of privacy by design (strategies), one of the more popular privacy design philosophies. The main contribution we find is the introduction of tactics.

In doing this we brought together two opportunities for extension: further strengthening the connection between data protection and privacy engineering, and linking privacy engineering to system architecture.

The strategies are now more consistent in their definitions, and better serve their intended purpose as a bridge between domains. Both comprehensive and concise versions of their definitions are featured in the full paper, along with that of the tactics. The paper by the same title is set to appear in the International Workshop on Privacy Engineering 2016.

REFERENCES

[1] European Commission, "Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)," *COM(2012) 11 final including SEC (2012) 72 final and SEC (2012) 73 final*, vol. 2015, no. June, pp. 1–201, 2015.

[2] The European Commission, *EU Commission and United States agree on new framework for transatlantic data flows: EU-US Privacy Shield*, no. February. Strasbourg, 2016.

[3] J.-H. Hoepman, "Privacy Design Strategies," *International Federation for Information Processing*, pp. 446–459, 2014.

[4] "privacypatterns.eu - collecting patterns for better privacy." [Online]. Available: https://privacypatterns.eu/. [Accessed: 20-Oct-2015].

[5] K. Wuyts, R. Scandariato, B. De Decker, and W. Joosen, "Linking privacy solutions to developer goals," in *Proceedings - International Conference on Availability, Reliability and Security, ARES 2009*, 2009, pp. 847–852.

[6] L. Urquhart, T. Rodden, and M. Golembewski, "Playing the Legal Card : Using Ideation Cards to Raise Data Protection Issues within the Design Process," *Proc. CHI'15*, pp. 457–466, 2015.

[7] F. Bachmann, L. Bass, and M. Klein, "Deriving Architectural Tactics : A Step Toward Methodical Architectural Design," no. March, p. 6, 2003.

[8] ISO/IEC, "ISO/IEC 15944-8:2012 Information technology -- Business Operational View -- Part 8: Identification of privacy protection requirements as external constraints on business transactions," 2012.

[9] J. Porekar, A. Jerman-Blažič, and T. Klobučar, "Towards organizational privacy patterns," *Proceedings - The 2nd International Conference on the Digital Society, ICDS 2008*, 2008.

[10] H. Baraki et al., *Towards Interdisciplinary Design Patterns for Ubiquitous Computing Applications*. Kassel, Germany: Kassel University Press GmbH, 2014.

[11] G. Iachello and J. Hong, "End-User Privacy in Human-Computer Interaction," *Foundations and Trends® in Human-Computer Interaction*, vol. 1, no. 1, pp. 1–137, 2007.

[12] M. Hafiz, "A Pattern Language for Developing Privacy Enhancing Technologies," *Software - Practice and Experience*, vol. 43, pp. 769–787, 2013.

[13] F. Kelbert and A. Pretschner, "Towards a policy enforcement infrastructure for distributed usage control," *Proceedings of the 17th ACM SACMAT (Symposium on Access Control Models And Technologies)*, p. 119, 2012.

[14] S. Pearson and Y. Shen, "Context-aware privacy design pattern selection," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 6264 LNCS, pp. 69–80, 2010.

[15] D. J. Solove, "Understanding Privacy," *Harvard University Press*, 2008.