"A Critical Analysis of Privacy Design Strategies"

Michael Colesky (jhh; mrc@cs.ru.nl)
Jaap-Henk Hoepman
Christiaan Hillen (christiaanhillen@valori.nl)

Radboud University

VALORI

Our Goals

1: Translate data protection legislation into **architectural goals** which system engineers can understand

2: Make these goals **achievable** to help them **actually happen**

State of the Art

making Privacy by Design more concrete
like Cavoukian;

Thought organization tool like
Wuyts, Scandariato, De Decker, & Joosen;
Urquhart, Rodden, & Golembewski

using Privacy Patterns like
Doty & Gupta; Bier & Krempel;
Hafiz; and Hoepman

using Hoepman's strategies
in particular

Privacy, Patterns & Strategy

data protection laws protect privacy
privacy design strategies translate these laws
privacy patterns implement data protection

Engineers use 'privacy', the EU uses 'data protection'
We (and ISO 15944-8) bridge the two as **'privacy protection'**

Satisfying Our Goals

1: strategies (translate)

distinct architectural goals in privacy by design, facilitating privacy protection

2: patterns (achieve)

best practice solutions to recurring problems, tested by time and public scrutiny

(translation to achievability)

Mapping Strategies to Patterns

in our collection of **privacy patterns**,
opportunity for **another level of abstraction**
resulted in **privacy design tactics:**

approaches to privacy by design which contribute to the goals of overarching strategies

this links to 'tactics' from the software architecture domain
– where privacy is a system quality attribute

Software Architecture

the highest level of abstraction, consisting of **structures** which include **elements**, their **properties**, and their **relationships**

(like security and privacy)
Quality Attributes
important non-functional **properties** of a system

not **whether** the system functions, but
how well it functions

our architectural tactics enhance privacy protection
They are grouped by strategies

The Privacy Design Strategies
definition e.g.

HIDE

preventing exposure as much as possible by mixing, obfuscating, dissociating, or restricting access to any storage, sharing, or operation on personal data, within the constraints of the agreed upon purposes

(and their mapped privacy patterns)

Some of the HIDE Strategy's Tactics

MIX processing personal data randomly within a large enough group to reduce correlation

Constant Length Padding; Delayed Routing/Random Wait; Guarantee Anonymous Access when Un-authenticated; Oblivious Transfer; Random Exit; Link Padding

DISSOCIATE removing the correlation between different pieces of personal data

Anonymity Set/Probable Suspect/Mix Networks; Batched Routing; Chaining; K-anonymity; Layered Encryption/Onion Routing; Morphed Representation/Werewolf/Gate of Heaven/Dr. Jekyll and Mr. Hyde/Amoeboid Shape/Psuedo Identities/Identity Separation; Cover Traffic/Use of Dummies

Shorter Strategy Definitions

the 'concise' definitions follow some rules

e.g. HIDE preventing exposure of access, association, visibility, and understandability of personal information to reduce the likelihood of privacy violations

- personal information concerns all kinds of processing
  (collecting, recording, use etc.)
- provide as much protection as possible
- purposes must have freely given, specific informed consent
  (or be required by indicated legitimate grounds)

Kinds of Processing from the GDPR examples

Solove's Taxonomy		GDPR Processing Examples
Processing	Operate	Adaptation/Alteration/Retrieval/Consultation/ Use/Alignment/Combination
	Store	Organization/Structuring/Storage
	Retain	opposite to (Erasure/Destruction)
Collection	Collect	Collection/Recording
Dissemination	Share	Transmission/Dissemination/Making Available/opposite to (Restriction/Blocking)
Invasion	Change	(Adaptation/Alteration/Use/Alignment/Combination)
	Breach	(Retrieval/Consultation)

Conclusions

We introduced tactics between our amended strategies and cataloged patterns

goals

allowing us to connect requirements to design & implementation
(and system architecture)

this presents a more accessible medium for stakeholders and engineers

to **achieve** privacy

Thank you for your time

feel free to ask any questions,

or make any comments or criticism

References

L. Bass, P. Clements, and R. Kazman, Software Architecture in Practice, 3rd ed. Addison-Wesley Professional, 2012.

C. Bier and E. Krempel, "Common Privacy Patterns in Video Surveillance and Smart Energy," in ICCCT-2012, 2012, pp. 610–615.

A. Cavoukian, "Operationalizing Privacy by Design : A Guide to Implementing Strong Privacy Practices," pp. 1–72, 2012.

A. Cavoukian, "Privacy by Design The 7 Foundational Principles Implementation and Mapping of Fair Information Practices," Information and Privacy Commissioner of Ontario, Canada, 2009.

Committee on Civil Liberties Justice and Home Affairs, "Draft Report on the proposal for a regulation of the European Parliament and of the Council on the protection of individual with regard to the processing of personal data and on the free movement of such data," 2014.

European Commission, EU Commission and United States agree on new framework for transatlantic data flows: EU-US Privacy Shield, February. Strasbourg, 2016.

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, June, pp. 1–201, 2015.

European Parliament and Council of European Union, "Directive 95/46/EC of the European Parliament and of the Council," Official Journal of the European Communities, vol. 281, no. 31, pp. 31–50, 1995.

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

J.-H. Hoepman, "Privacy Design Strategies," IFIP SEC 2014, pp. 446–459, 2014.

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.

ISO/IEC, "ISO/IEC 29100:2011 Information technology -- Security techniques -- Privacy Framework," 2011.

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

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.

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.