Privacy and Data Protection by Design

Jaap-Henk Hoepman
RU Nijmegen
jhh@cs.ru.nl / @xotoxot / www.xot.nl

Introduction

- **PI.lab: collaboration between**
  - Radboud University – ICIS
  - Tilburg University – TILT
  - TNO – Security; Strategy & Policy
  - SIDN
- **Myself:**
  - Scientific director PI.lab
  - Associate professor, Radboud University
  - Research: privacy & identity, applied cryptography, Internet of Things

ENISA Report

Authors:

George Danezis,
Josep Domingo – Ferrer,
Marit Hansen,
Jaap-Henk Hoepman,
Daniel Le Métayer,
Rodica Tirtea,
Stefan Schiffner

https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/privacy-and-data-protection-by-design

Privacy definitions

- **The right to be let alone**
  - [Warren & Brandeis, 1890]
- **Informational self-determination: The right to determine for yourself when, how and to what extend information about you is communicated to others**
  - [Westin, 1967]
- **The freedom from unreasonable constraints on the construction of one's identity**
  - [Agre & Rottenberg, 2001]
- **Contextual integrity: the right to prevent information to flow from one context to another**
  - [Nissenbaum, 2004]

Privacy by design

- **Protect privacy during technology development:**
  - From conception…
  - … to realisation & operation.

Through the full product development lifecycle

The ENISA report

- **Started work because concrete implementation of "Privacy by Design" unclear**
- **Report bridges gap between legal requirements and available technologies**
  - Inventory of existing approaches
  - Privacy design strategies
  - Technical building blocks (PETs)

Audience

- **Engineers:**
  - State of the art of privacy-by-design and overview of existing PETs and design approaches
- **Data protection authorities:**
  - References to current available technologies and methods
- **Regulators:**
  - Understand opportunities, challenges and limits of the privacy-by-design approach

Key findings

- **Privacy ignored in traditional engineering approaches**
  - Little awareness
  - Tools lacking
- **Thriving PET research community, but poorly connected to practice**
  - Privacy by design can be promoted through appropriate standardisation efforts
- **Enforcement of compliance with regulatory regime needs to be more effective**

Limits of privacy by design

- **Privacy properties are fragile**
  - They break when composing systems
- **Lack of privacy metrics**
- **How to balance privacy & utility**
  - Privacy or utility first?
- **Designing for privacy may increase system complexity**

Main recommendations

- **Policy makers: support the development of new incentive mechanisms for privacy-friendly services and promote them.**
- **Further investigate privacy engineering, using a multidisciplinary approach.**
- **Develop tools that enable the intuitive implementation of privacy properties.**
- **Infrastructure projects: include privacy-supporting components, such as key servers and anonymising relays.**
- **Data protection authorities: Provide independent guidance and assess modules and tools for privacy engineering.**
- **Legislators: promote privacy and data protection in norms.**
- **Standardisation bodies: Include privacy considerations in the standardisation process, and draft standards for interoperability of privacy features.**

ENISA Report Structure

- **Enigneering privacy**
- **Privacy design strategies**
- **Privacy Techniques**
- **Conclusions & Recommendations**
- **Policy context**

Privacy & Identity Lab

Engineering Privacy

Baseline

- **Principles**
  - OECD guidelines
  - Fair Information Practice Principles
  - EU Data Protection Directive 95/46/EC
- **Standards**
  - ISO/IEC 92100 Privacy Framework

Protection principles

- **Security**
  - Confidentiality
  - Integrity
  - Availability
- **Privacy**
  - Unlinkability
  - Transparency
  - Intervenability

EU legal framework

- **Lawfullness**
  - Consent, performance of contract, legal oblication, vital interest (subject/controller), public interest
- **Consent**
  - Specific, informed, explicit
- **Purpose binding**
- **Necessary and minimal**
  - Proportional, subsidiary
- **Transparancy**
- **Data subject rights**
- **Information Security**
- **Accountability**
- **Data protection by design and default**

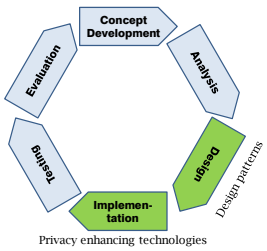
Privacy Impact Assessment

- **Steps**
  - the identification and consulting of stakeholders,
  - the identification of risks,
  - the identification of solutions and recommendations,
  - the implementation of the recommendations,
  - reviews, audits and accountability measures
- **Not as mature as security risk assessment methodologies yet**

Privacy & Identity Lab

Privacy Design Strategies

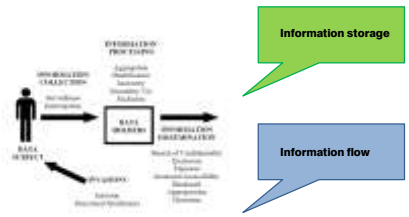
Software development cycle



Levels of abstraction

- **Design strategy**
  - "A basic method to achieve a particular design goal" – *that has certain properties that allow it to be distinguished from other basic design strategies*
- **Design pattern**
  - "Commonly recurring structure to solve a general design problem within a particular context"
- **(Privacy enhancing) technology**
  - "A coherent set of ICT measures that protects privacy" – *implemented using concrete technology*

Source #1: Solove



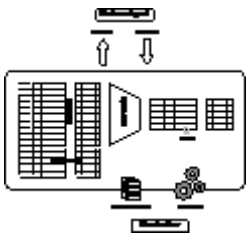
Source #2: data protection law

- **Core principles**
  - Data minimisation
  - Purpose limitation
  - Proportionality
  - Subsidiarity
  - Data subject rights: consent, (re)view
  - Adequate protection
  - (Provable) Compliance

8 privacy design strategies

- **Data oriented strategies**
  - Minimise
    - *The amount of PII should be minimal*
  - Separate
    - *Process PII in a distributed fashion*
  - Aggregate
    - *Process PII in the least possible detail*
  - Hide
    - *PII should not be stored in plain view*
- **Process oriented strategies**
  - Enforce
    - *A privacy policy should be in place and be enforced*
  - Inform
    - *Subjects should be informed when PII is processed*
  - Control
    - *Subjects should have control over when/how PII is processed*
  - Demonstrate
    - *Compliance to policies and legal requirements must be demonstrated*

Information storage system



What about design patterns?

Strategy	Patterns	Coverage
Minimise	Select before you collect, anonymisation, ….	
Separate	Distribute, sector-specific pseudonyms	
Aggregate	Data fuzzing; coarse-grained location	
Hide	Encryption, onion routing, Tor	
Enforce	Access control, privacy licenses	
Inform	P3P (?)	
Control	Informed consent (?)	
Demonstrate	Privacy management system, logging	

Privacy & Identity Lab

(Some) Privacy techniques

Secure private communication

- **Encryption**
  - Confidentiality / Integrity
- **Public Key Infrastructures**
  - Authenticity
- **Forward secrecy**
- **Coercion resistance**

Anonymous communication

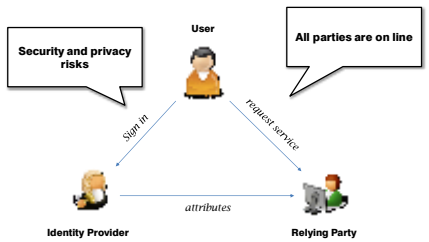
- **Proxy / VPN**
- **Onion routing**
- **Mix net**
- **DC nets**

TorProject.org

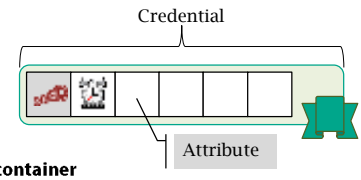
Attribute Based Credentials

IRMA

Identity management: transitional

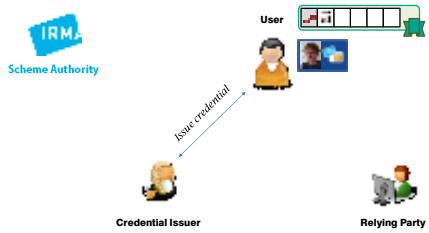


Credential

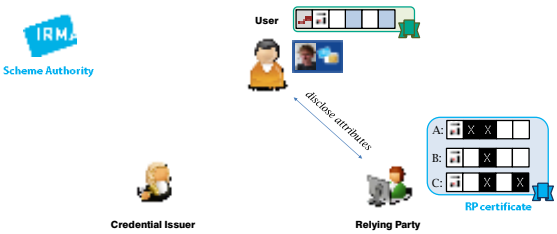


- Secure container
- Issued and signed by *credential issuer*
- Contains attributes, *selectively disclosable*

IRMA: issuing a credential



IRMA: disclosing some attributes



ABC Properties

- Unforgeable
- Unlinkable
  - Issuing with disclosing, and
  - Between two disclosures
- Revocable
- Non transferable
- (Inspectable)

Other techniques

- Statistical disclosure control
- Privacy-preserving data mining
- Private information retrieval
- Homomorphic encryption
- Secure multi-party computation

Wrapping up

- Privacy by design: a lot of talk, a lot less happening
  - Many concrete privacy enhancing technologies
  - Few concrete privacy design patterns
  - No integration into development methodologies
- Privacy:
  - a fragile property
  - hard to measure
  - hard to balance with utility
  - complex to achieve

Discussion

✉ jhh@cs.ru.nl

@xotoxot

www.cs.ru.nl/~jhh

www.xot.nl