Introduction

- Pl.lab collaboration between
  - Radboud University – ICIS
  - Tilburg University – TILT
  - TNO – Security; Strategy & Policy
  - SIDN

- Myself:
  - Scientific director Pl.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


Privacy definitions

- The right to be let alone
  - [Warren & Brandeis, 1890]
- Informational self-determination: The right to determine for yourself how and to what extend information about you is communicated to others
  - [Desta, 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.

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)
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

- 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

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

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
- Engineering privacy
- Privacy design strategies
- Privacy Techniques
- Conclusions & Recommendations
- Policy context
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

- **Lawfulness**
  - Consent, performance of contract, legal obligation, vital interest (subject/controller), public interest

- **Consent**
  - Specific, informed, explicit

- **Purpose binding**

- **Necessary and minimal**
  - Proportional, subsidiary

- **Transparency**
  - 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 Design Strategies

Software development cycle

- Concept Development
- Development
- Testing
- Implementation
- Analysis

Privacy enhancing technologies
A basic method to achieve a particular design goal — that has certain properties that allow it to be distinguished from other basic design strategies.

Commonly recurring structure to solve a general design problem within a particular context.

A coherent set of ICT measures that protects privacy — implemented using concrete technology.

Information storage

Information flow

Core principles

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

Minimise

Separate
Aggregate
Hide

Enforce
Inform
Control
Demonstrate

8 privacy design strategies

Data oriented strategies

Process oriented strategies

Data subject rights

Adequate protection
(Provable) Compliance
Strategy | Patterns | Coverage
---|---|---
Minimise | Select before you collect, anonymisation,... | Green
Separate | Distribute, sector-specific pseudonyms | Green
Aggregate | Data forcing, coarse-granularity | Yellow
Hide | Encryption, onion routing, Tor | Red
Enforce | Access control, privacy licenses | Red
Inform | P3P (?) | Red
Control | Internal consent (?) | Red
Demonstrate | Privacy management system, logging | Red

(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

Attribute Based Credentials

Identity management: transitional

Security and privacy risks

User

All parties are on line

Identity Provider

attributes

Relying Party

The user of IRMA: 09/02/2015

09/02/2015
Credential

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

IRMA: issuing a credential

- User
- Credential issuer
- Relying party

IRMA: disclosing some attributes

- User
- Credential issuer
- Relying party

ABC Properties

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

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