An Approach to introduce Privacy by Design in Agile App-Development
Bald 25 Milliarden Downloads aus dem App Store.

25.000.000.000
PAUSING GOOGLE PLAY

26%

WHAT PERMISSIONS DO APPS ACCESS MOST?

- Location: 42%
- Contacts: 31%
- Camera: 26%
appification

- Often developed in **short time** with **small teams**
- Apps have **limited focus**
- Have access to **personal information**
  - Sensors, messages, contacts, locations
- Apps can be developed **by non-professional developers**

(Wasserman 2010)
the MIRROR project

● Goal: Support **reflective learning at work**

Reflection: Going back to past experience and re-evaluate them to learn for future action (Boud 1985)

● „Going back“ in this project is thought of as „going back to information collected“ ... **with apps**

● **Collaborative reflection** means: share your insights and your data
apps in MIRROR

- Up to today **14 apps** are developed/in development
  - 4 targeting Android
  - 4 iOs
  - 3 exclusively Web (7 mobile/web)
  - 2 Desktop
  - 2 include wearable sensors
- Size of development teams was **2-4**
- Development time between **6 to 24 month**
example: DocTrain (1)

- An app to collect trainings a assistant physician did
- To discuss her or his learning progress with a head physician
example: DocTrain (2)

- Could be used for employee surveillance
- May contain sensitive third-party information
- Could be misused by colleagues
privacy-by-design

- Fair Information Practices (OECD 1980)
  - Individual rights, minimization, purpose, security, accountability, […]
- PbD recommendations (Cavoukian 2009)
  - Proactive, privacy as default, functionality, […]
- Data Protection Goals (Rost 2011)
  - Transparency, unlinkability, intervention, […]
Engineering privacy
(Spiekermann and Cranor 2009)

- Privacy-by-policy
- Privacy-by-architecture
engineering privacy
(Spiekermann and Cranor 2009)

• Privacy-by-policy
• Privacy-by-architecture
  → Difficult to achieve in settings with fixed technology flexible use cases
engineering privacy by design
(Gürses et. al. 2011)

- Functional **Requirements** Analysis
- Data **Minimization**
- Identifying **Attacks, Threats and Risks**
- Multilateral **Security** Analysis
engineering privacy by design
(Gürses et. al. 2011)

- Functional **Requirements** Analysis
- Data **Minimization**
- Identifying **Attacks, Threats and Risks**
- Multilateral **Security** Analysis

- Requirements are **changing**
- **Unknown** which **data** may support reflection
- Analysis are require **defined processes and time**
what the approaches have in common

- **Socio-technical** perspectives
  - policy/architecture, Multilateral Risk analysis
- Need for of **process specification**
- Set of basic **data-protection rules**
  - minimization, anonymization, encryption..
challenges for (privacy-aware) app development

- **Short development cycles** and time
  - Less structured approach
- **Small teams that do various tasks**
  - Less awareness for privacy and security
- **Multiple recipient types**
  - Difficult for policies
- **Lack of** (knowledge about) privacy problems, security-frameworks
  - Need for easy access
our approach (1)

socio-technical design

- **Participatory** design elements
  - Supported workshops between
    - Developers and users
    - Developers and organizational representatives
  - Discuss use cases and scenarios
our approach (2)

support design

- Support developers in **doing** privacy-by-design by
  - Offering questions for **simple risk assessment**
  - **7 Point Guideline** of things to consider
  - Lists of **hints and best-practices** for possible security issues from a developers perspective
our approach (3)

generic modelling for analysis

- Modelling of a **generic process** adopted to the MIRROR context
- To be adapted to **use cases** and **scenarios**
again: DocTrain

- Workshop with users and privacy officer  
  → privacy-by-policy
- Data protection by default
  - Not sharing
  - Secured app
  - Secured channels
current state and future work

• Raised **awareness for Privacy by design**
• Still needed (external) “**data protection officer**” to support
• Relevance of management awareness
• Sustain knowledge, evaluate adoption
current state and future work

- Raised **awareness for Privacy by design**
- Still needed (external) “**data protection officer**” to support
- Relevance of management awareness
- Sustain knowledge, evaluate adoption
summary

Needs of Privacy-by-design

- **Socio-technical** perspectives
- Need for of **process specification**
- Set of basic **data-protection rules**

How it was implemented

- Limited number of **workshops** and **discussions**
- **Generic process** definitions based on user stories
- **Best-practices** from developers perspective
References