

An Approach to introduce Privacy by Design in Agile App-Development

Martin Degeling, martin.degeling@rub.de
Kai-Uwe Loser, kai-uwe.loser@rub.de

Bald 25 Milliarden Downloads
aus dem App Store.

25.000.000.000



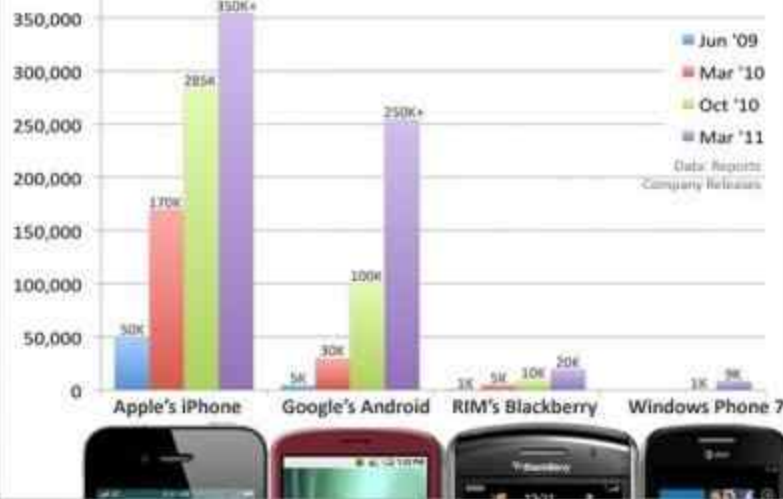
Appsfire
@appsfire



Breaking: today will mark the day the App store has seen 1 million apps ever created since launch (iOS)

Silicon Alley Insider Chart of the Day

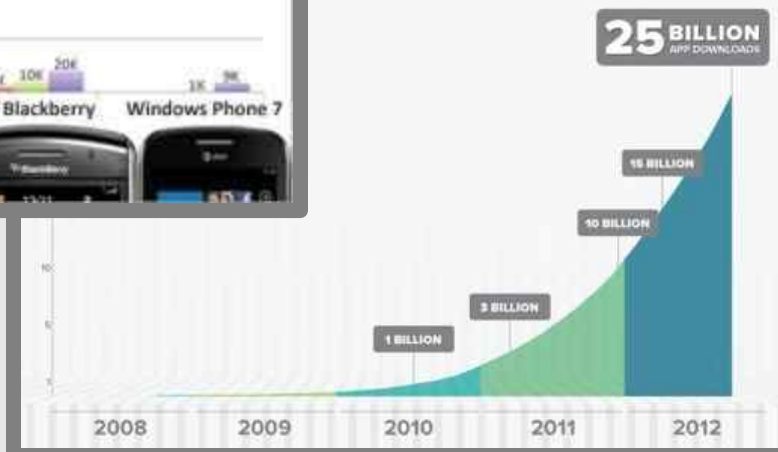
Number Of Apps Available At Smartphones' Apps Stores



weeten ★ Favorisieren

lesen Tweet integrieren

Play APP INSTALLS



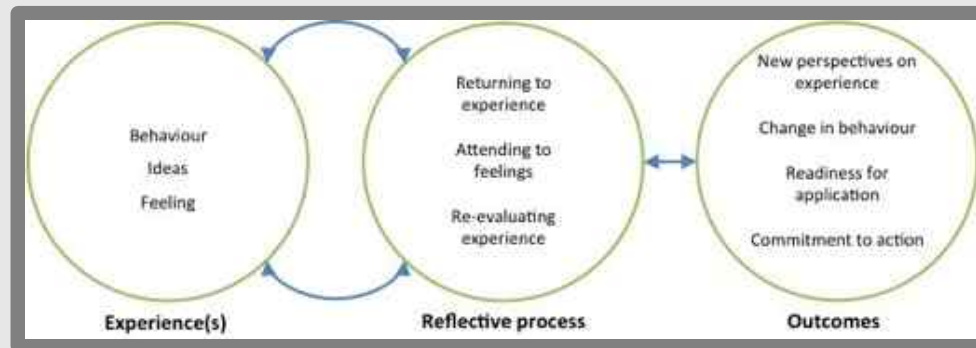


appification

- 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**

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



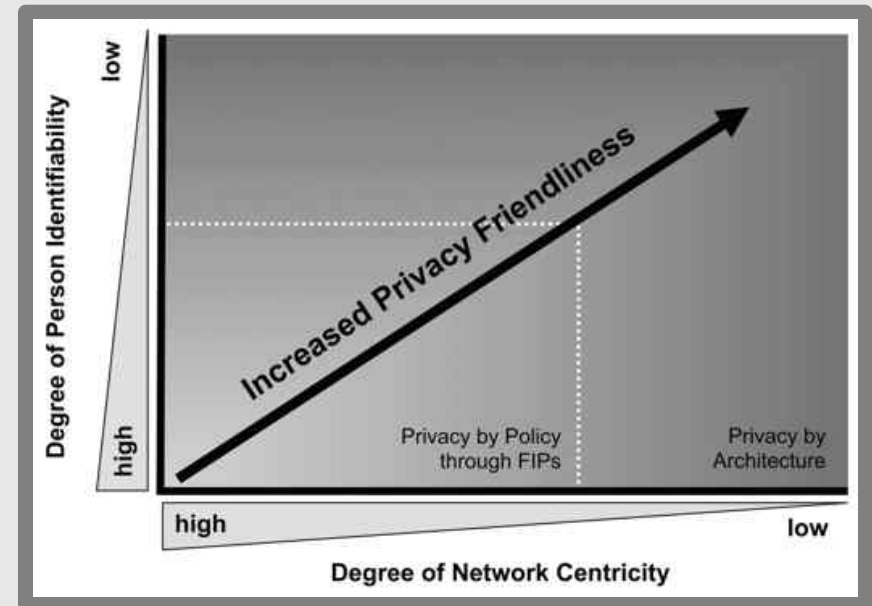
privacy-by-design

- 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**

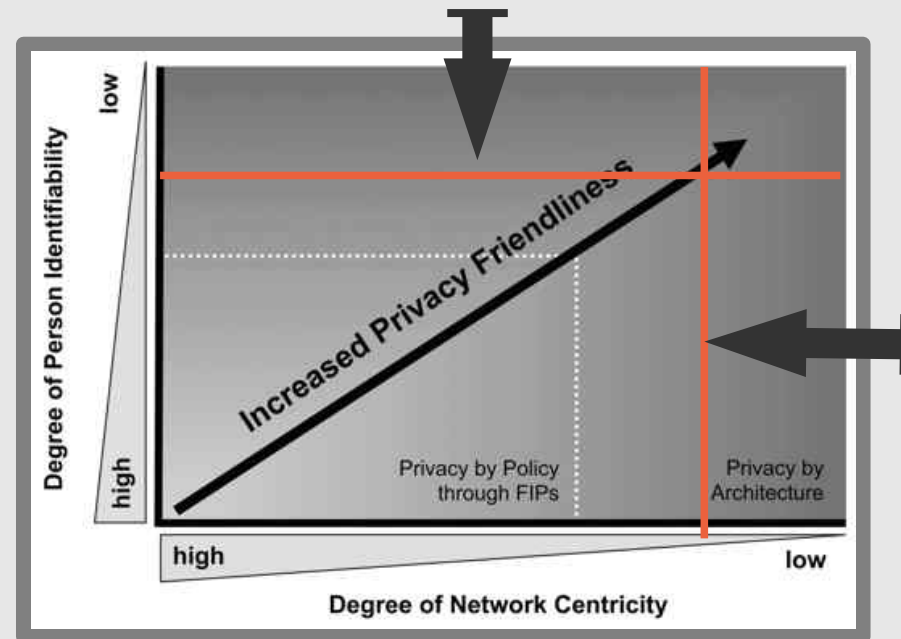


engineering privacy

(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**
 - Diffult 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

MIRROR

PRIVACY DEV CHEATSHEET

SUMMARY

This guideline is a short introduction into privacy-aware development of MIRROR applications. The aim is to build apps that respect the privacy and informational self-determination of the users and to meet basic security requirements of organizations.

RISK ASSESSMENT

1. What affects the privacy of the users? What are possible issues about collection and sharing? What could happen with the data in the worst case?
2. What influences privacy of third parties?
 - a) Those within the organization like colleagues etc.
 - b) Those that are service users of the organization like customers, patients or relatives. This is not only a privacy issue but the data is of high value for the organization since they are (legally) responsible for that data
3. What are possible attacks and threats?
 - from within the organization e.g. someone who wants to harm one of the data-owners (mad colleagues, unfair bosses)
 - from outside the organization e.g. steal and/or disclose information; manipulate information; harm one of the roles

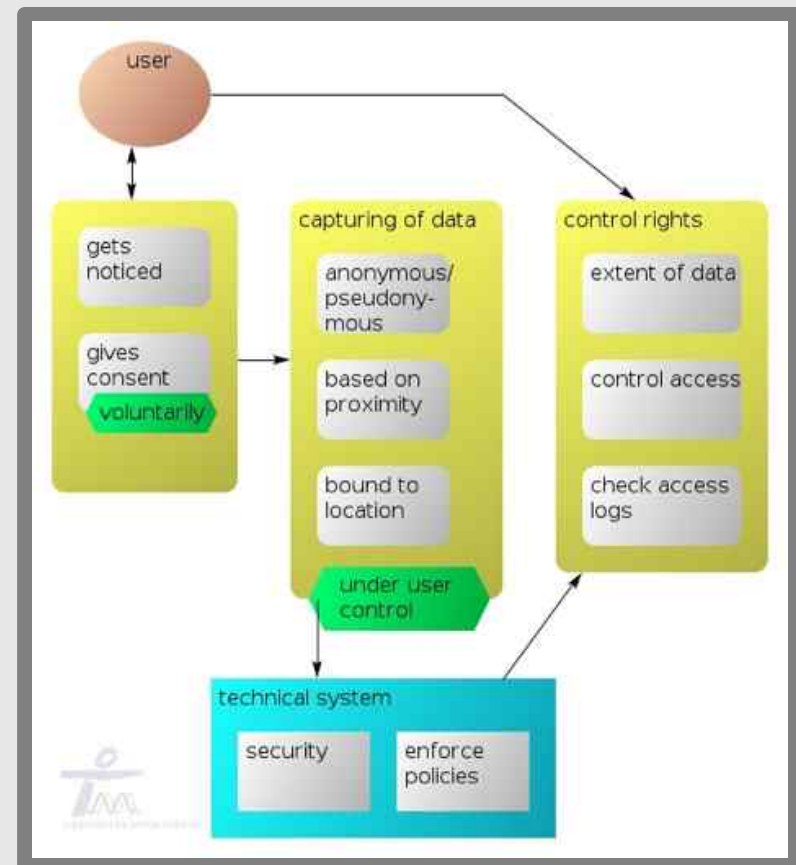
GUIDELINES

1. **Data Minimization:** Every data-item that describes something about a user or a third

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

- D. Boud, Reflection: turning experience into learning. Routledge, 1985.
- A. Cavoukian, „Privacy by Design - The 7 Foundational Principles“, 2009.
- F. S. Gürses, C. Troncoso, und C. Diaz, „Engineering Privacy by Design“, Computers, Privacy & Data Protection, 2011.
- M. Langheinrich, „Privacy by Design — Principles of Privacy-Aware Ubiquitous Systems“, in Ubicomp 2001: Ubiquitous Computing, Bd. 2201/2001, Springer Berlin / Heidelberg, 2001, p. 273–291.
- Organisation for Economic Co-operation and Development (OECD), „Guidelines on the Protection of Privacy and Transborder Flows of Personal Data“. [[Online](#)]. [Accessed: 28-June-2012].
- T. Probst, „Generische Schutzmaßnahmen für Datenschutz-Schutzziele“, Datenschutz und Datensicherheit - DuD, Bd. 36, No. 6, p. 439–444, Juni 2012.
- S. Spiekermann und L. F. Cranor, „Engineering Privacy“, IEEE Transactions on Software Engineering, Bd. 35, No. 1, p. 67–82, Jan. 2009.
- M. Rost und K. Bock, „Privacy By Design und die Neuen Schutzziele“, Datenschutz und Datensicherheit, Bd. 35, No. 1, p. 30–35, Jan. 2011.
- T. Wasserman, „Software Engineering Issues for Mobile Application Development“, FoSER 2010, 2010.