Privacy in Smartphone Ecosystems
Project Seminar Kick-off

October 25, 2016

Dr. Jetzabel Serna & MSc. Majid Hatamian

project.seminar@m-chair.de

Chair of Mobile Business & Multilateral Security

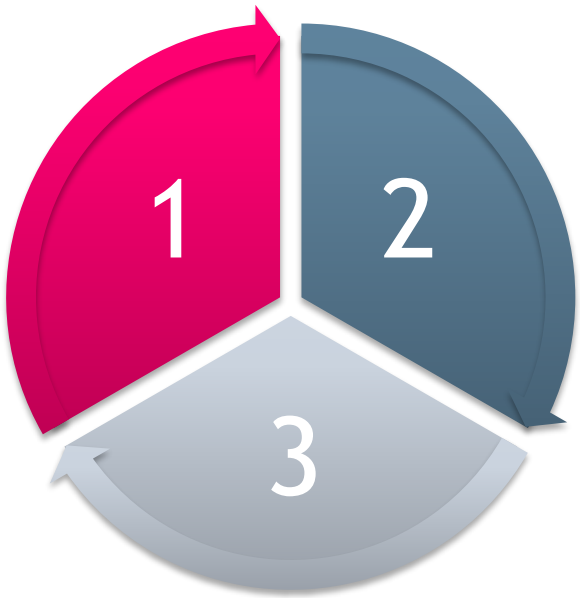
Goethe University Frankfurt

Agenda

- Organizational information
- Introduction to Privacy and Data Protection
- Privacy in Smartphone Ecosystems
- Questions

Seminar grade

- This project seminar consists of three administrative parts:



- Exam (one third)
- Report (one third)
- Presentation (one third)

- Participation in all parts is **required** for the successful completion of the seminar. The work is evaluated on individual basis (not in groups).

Formal requirements

- For the paper, the formal requirements of the chair apply.
  - Word-template available at
    - www.m-chair.de → Teaching
  - Number of pages required:
    - At least **50 pages,** recommended **70 pages** (including cover, table of contents, index and references)

Submission

- The seminar papers **must** be submitted in printed form to the secretariat of the chair or directly to the supervisor **in duplicate**.

- Furthermore, the seminar papers must be submitted in **electronic form** in the following formats:
  - MS-Word or OpenOffice
  - Adobe PDF

  via E-Mail to: project.seminar@m-chair.de

Important dates

- **Exam**
  - Date: 10.01.2017
  - Time: 10:00 - 12:00
  - Room: RuW 2.202
- Submission of Seminar Paper
  - 23.01.2017
- Presentation of the results:
  - January 31 & February 01 10:00-18:00
  - Room : RuW 2.202

Contact

In case of any questions or problems arise during the seminar you can contact:

- Via Mail:
  - project.seminar@m-chair.de
  - Jetzabel.serna@m-chair.de
  - Majid.hatamian@m-chair.de

- Via Phone:
  - Jetzabel Serna: (0)69 / 798 34667
  - Majid Hatamian: (0)69 / 798 34662
- For comprehensive questions please make an appointment at least one week in advance.

mobile business

Privacy & Data Protection

Upcoming Exam

Data Protection and Privacy

- Both terms are related but not synonymous and *have many definitions*.
- 2 popular ones:
  - Data protection is the protection from harmful and unsolicited usage of data linked to the personal sphere of a person.
  - Privacy is the right to be left alone, e.g. to be unwatched or anonymous [WaBr1890]
- **More work needed on a complete understanding of privacy**

Introduction I

- Early day definitions: "The right to be let alone" Warren and Brandeis, 1890, Harvard Law Review: "The right to privacy" [WaBr1890]
- Beginning of information age: "The claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others." Westin, 1967.

- Westin's index
  - Privacy fundamentalists
  - Privacy pragmatists
  - Privacy unconcerned

Source: https://pixabay.com/es/de-distancia-junction-direcci%C3%B3n-1020088/

Introduction II

- Contemporary: **It is complex**
  - "The ability of the individual to protect information about himself" Goldberg et. al 1997

- Personal information: "Any information relating to an identified or identifiable natural person (data subject); an identifiable person is one who can be identified directly or indirectly "

Source: https://pixabay.com/es/icono-la-cabeza-ver-el-perfil-1247948/

Privacyinternational.org

- https://www.youtube.com/watch?v=zsboDBMq6vo

Dimensions of Privacy Protection

- Legal aspects of privacy
  - Supportive legal frameworks (e.g., right to be forgotten, safe harbor/privacy shield)
- Technical aspects of privacy
  - Privacy engineering, and PETs
- User aspects of privacy
  - User awareness, and usability

Source: https://pixabay.com/es/cl%C3%A1usula-correo-electr%C3%B3nico-en-1462968/

Source: https://pixabay.com/es/sistema-red-noticias-conexi%C3%B3n-954972/

Legal aspects of privacy

- EU Privacy Law (Privacy directive …)
- eIDAS Regulation
- General Data Protection Regulation

Source: https://pixabay.com/es/contrato-consulta-pluma-firma-1332817/

9 Principles of EU Privacy Law I

1. **Intention and notification:** The processing of personal data must be reported in advance to a Data Protection Authority.
2. **Transparency:** The person involved must be able to see who is processing her data for what purpose.
3. **Finality principle:** Personal data may only be collected and processed for specific, explicit and legitimate purposes.
4. **Legitimate grounds of processing:** The processing of personal data must be based on a foundation referred to in legislation, such as permission, agreement, and such.
5. **Quality:** Personal data must be as correct and as accurate as possible.

[BlaBorOlk2003]

9 Principles of EU Privacy Law II

6. **Data subject's rights:** The parties involved have the right to take cognisance of and to update their data as well as the right to raise objections.
7. **Processing by a processor:** This rule states that, with the transfer of personal data to a processor, the rights of the data subject remain unaffected and that all restrictions equally apply to the processor.
8. **Security:** A controller must take all meaningful and possible measures for guarding the personal data.
9. **Transfer of personal data outside the EU:** The traffic of personal data is permitted only if that country offers adequate protection. [BlaBorOlk2003]

Protection of Personal Data

http://ec.europa.eu/justice/data-protection/index_en.htm

[EC-Prot-2014]

General Data Protection Regulation

- The European Commission says that the recently approved regulation “puts the citizens back in control of their data, notably through”:
  - A right to be forgotten - Users will have the right to demand that data about them be deleted if there are no "legitimate grounds" for it to be kept.
  - Data minisation: adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
  - Privacy by design and by default – privacy friendly default settings to be the norm.
  - Transparency - processed lawfully, fairly and in a transparent manner in relation to the data subject.
  - Purpose limitation - collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
  - Accuracy - every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay
  - Storage limitation - kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;
  - Security (integrity and confidentiality)

[EC2014]

eIDAS Regulation

- REGULATION on electronic identification and trust services for electronic transactions in the internet market.
- One of the objectives is to remove existing barriers to the cross-border use of electronic identification means used in the Member States to authenticate, for at least public services.
- Authentication for an online service should concern processing of only those identification data that are adequate, relevant and not excessive to grant access to that service online.

[Electronic identification and trust services (eIDAS): regulatory environment and beyond, ec.europa.eu]

Law Alone is not Sufficient

- Data protection / Privacy law alone not sufficient
  - Not all processing can be controlled (e.g. every network node).
  - Deliberate breaking and bending of law (different legislations on the internet)
  - Economic pressure can force customers to give consent to almost any kind of ‘privacy’ policy (e.g. selling privacy for “peanuts”).

[Reagle1998, SelfReg1999, Bell2001, Hoofnagle2005]

⇨ Technical Privacy Protection

Technical Aspects of Privacy

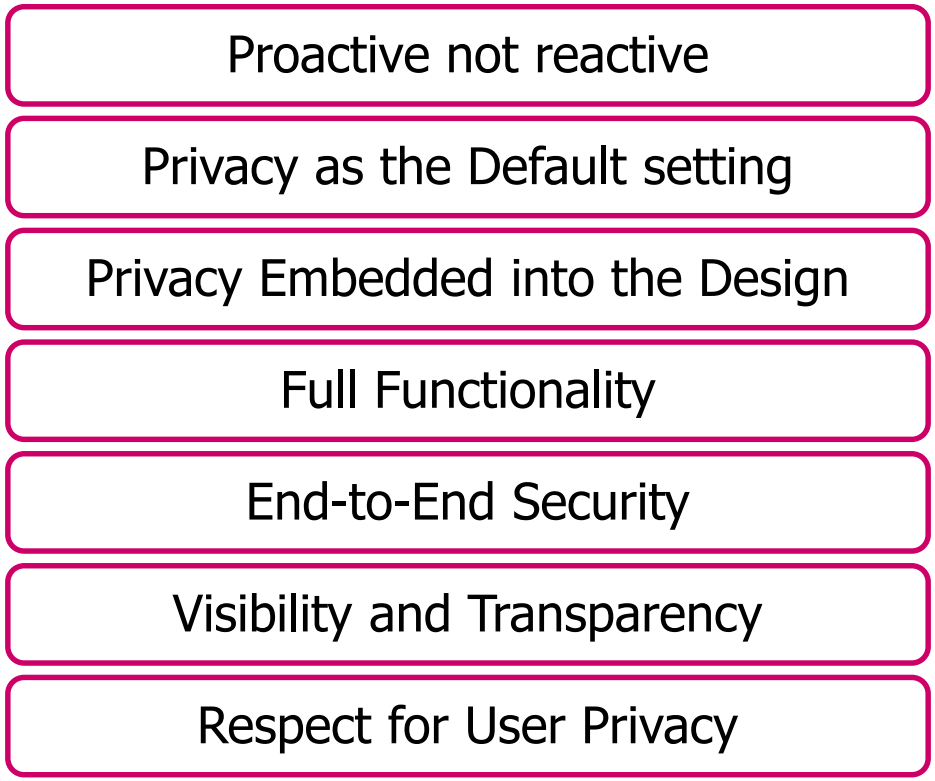
- Privacy by Design
- Privacy Engineering
- Privacy enhancing technologies

Source: https://pixabay.com/es/humanos-siluetas-redes-internet-1157116/

Privacy-by-design I

PbD: refers to the notion of embedding privacy directly into the design of ITs and systems

- There are 7 foundational principles:



[Cavoukian2010]

Privacy-by-design II

- Adoption
  - 2010: The International Conference of Data Protection and Privacy Commissioners unanimously endorsed PbD.
  - 2012: The Federal Trade Commission (FTC) in the US, proposed a framework for business and policymakers with PbD as a core value.
  - 2014: The European Commission announced that: 'Privacy by Design' and 'privacy by default' will become essential principles in EU data protection rules.

[CPDP2014]

Privacy-by-design III

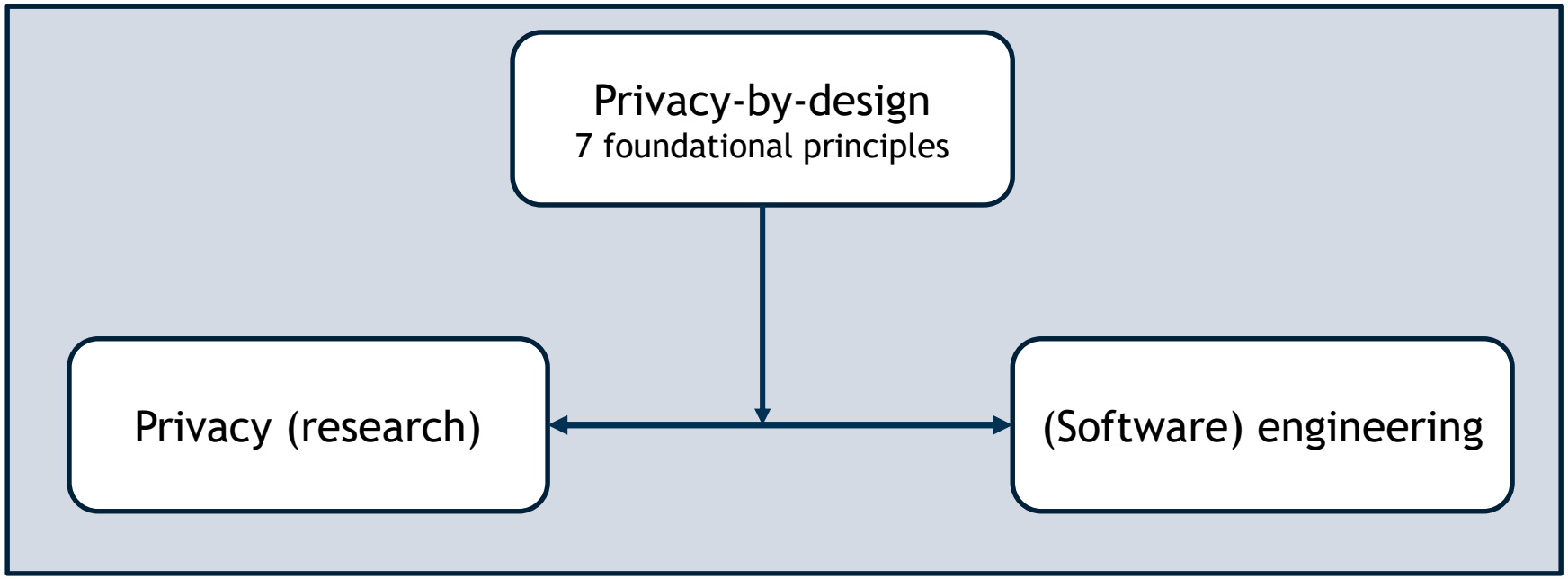
- There are 8 privacy-by-design strategies:

Minimization
Hiding
Separation
Aggregation
Information
Controlling
Enforcement
Demonstration

[D' Acquisto2015]

Privacy engineering I

- It aims to fill the gap between research and practice (between privacy and software engineering)



[Gürses2016]

Privacy engineering II

- Field of research and practice that **designs**, **implements**, **adapts**, and **evaluates** methods, techniques, and tools:
  - methods are approaches for systematically capturing and addressing privacy issues
  - techniques are procedures, possibly with a prescribed language, to accomplish privacy-engineering tasks or activities
  - tools are means that support privacy engineers during part of a privacy engineering process

[Gürses2016]

Privacy enhancing technologies

- Privacy Enhancing Technologies (PETs)
  - It refers to the category of technologies that minimise the processing of personal data
- Examples
  - Automatic anonymisation (e.g. Anonymizer, iPrivacy)
  - Encryption tools (e.g. SSL)
  - Policy Tools (e.g., P3P, TRUSTe)

[Danezis2014]

User Aspects of Privacy

- User awareness

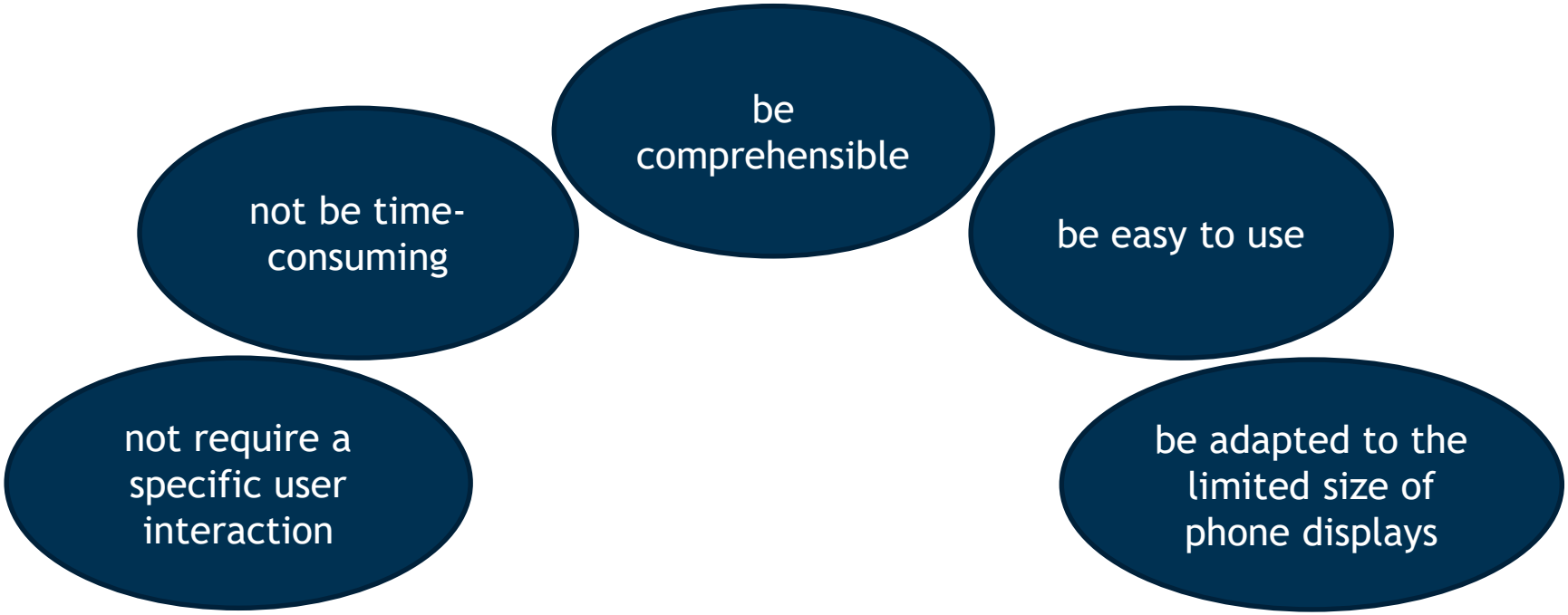
Source: https://pixabay.com/es/signo-de-interrogaci%C3%B3n-pregunta-mark-1722862/
https://pixabay.com/es/advertencia-signo-de-exclamaci%C3%B3n-34621/

- Usability

Source: https://pixabay.com/es/equipo-parry-juntos-s%C3%ADmbolos-403505/

User awareness

- User awareness (transparency)
- Solution should:

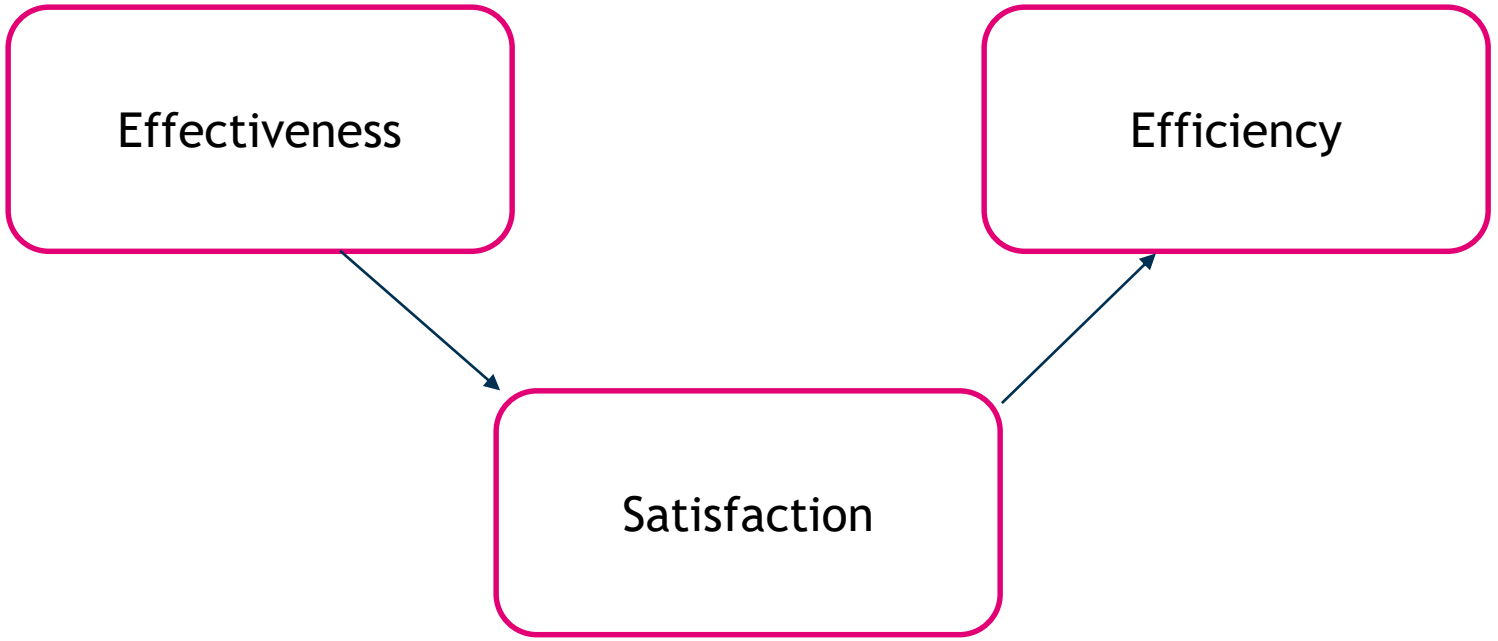


[Danezis2014]

Usability

"Can I do what I want to do?"

"Do I feel secure and comfortable while using the system? "



"Does the system accomplish my tasks quickly? "

[National Academy2010]

Upcoming Exam

- Resources
  - This presentation
  - References on this presentation

mobile business

Privacy in Smartphone Ecosystems

Seminar projects

Motivation/Problem Statement

- Smartphones applications collect lots of information from sensors, etc.
- Users are often unaware of what information is being collected, how often, for which purpose?
- Neither applications nor marketplaces provide an appropriate level of transparency.
- Current privacy risk information does not inform users about individual privacy risks of apps in an appropriate manner.

Objective & Expected results

- **Increase user privacy awareness & enhance privacy protection in smartphone ecosystems.**
  - Analyze data flows and data types in order to better understand the privacy threats of mobile apps.
  - Analyze crowdsource comments reporting issues about privacy to measure the privacy invasiveness of an app
  - Develop privacy indicators to support effective risk communication.

mobile business

Transparency of smartphone apps

Topic 1

What is transparency?

- Important privacy principle
- Right of individuals to be informed about
  - how and by whom their personal data have been processed?
- In order to provide real transparency
  - users need to have access to the types of information collected by an app and the context in which it is collected, used, stored and shared.

mobile business

HCI techniques

- Human-computer interaction (HCI) aims to
  - create interactive products that are easy and enjoyable to use.
- It is highly challenging for designers to create apps which are usable and affordable to such a heterogeneous set of users.

mobile business

Usability

- Mobile app ecosystems have been exposing a growing number of APIs through their apps
- Many of these APIs involve accessing sensitive functionality and/or user data.
  - Android for instance allows developers to select from over 130 possible permissions.
- There is an important tension between usability and privacy

mobile business

Expected results

- A literature review of HCI techniques, methods and tools to enhance transparency will be performed.
- Selected techniques will be analyzed and compared in terms of usability and usefulness.

mobile business

Assessing privacy of smartphone apps through crowdsource comments

Topic 2

Crowdsource comments

- User comments serves as a valuable source of information for evaluating a mobile app, for both new users and developers.
- For the purpose of evaluation on the security/privacy aspects of an app, user comments are not always directly useful.

Privacy risk score

- We still need a criterion which enables us to:
  - estimate how much an app could be a threat for the users' privacy?
- Privacy risk score is a metric which is:
  - obtained regarding the crowdsource-comments analysis

Expected results

- An extensive literature review
- implementation of a prototype using (e.g. using machine learning techniques) to identify the context and usage of the application as well as privacy related comments and ultimately provide a privacy risk score.

mobile business

Assessing privacy of smartphone apps through the analysis of data flows

Topic 3

mobile business

Data flows

- Every app has access to different kinds of data (data flow):
  - Location, SMS, Contacts, etc.
- Every app has a specific functionality, thus
  - it requires to just have access to a certain number of information flows which are related to its functionality

mobile business

Privacy risk score

- Important question:
  - Which apps have access to the data which do not pertain to their functionality?
- Measuring a privacy risk score according to analysis of permissions which are being used by installed apps.

Expected results

- An in-depth literature review to analyze and investigate which characteristics make an application a potential danger with regard to user's security and privacy.
- A technical/mathematical approach to provide a privacy score that will take into consideration the behavior of the application with regard to
  - access permissions,
  - data flows, and
  - frequency of access and context/usage of the application

mobile business

Privacy risk indicators for smartphone apps

Topic 4

What are the problems with indicators?

- The main problems:
  - Ambiguity
  - Lengthful
  - Unattractive

Psychological aspects of privacy

- What will happen?
  - poor awareness or lack of knowledge of how to go about protecting privacy
  - unthinking installation of untrustworthy apps
- A potential reason is:
  - Psychological aspect

Psychological aspects of privacy

- What are the challenges?
- Why do the developers pay a limited attention to the psychological aspects of privacy in smartphone apps?
- Why the privacy indicators are most of the times ambiguous?

- How the developers can make the indicators more attractive for the users?
- Which psychological factors are important to the users to pay sufficient attention to the privacy indicators?

Expected results

- An extensive literature review
- Classification of the crucial psychological factors which have been ignored by the developers in designing of privacy indicators.
- A case study should be performed (between 10 to 20 participants) to assess and measure the classification of the psychological factors in terms of usability and usefulness in order to determine whether they are important to the real users or not.

Questions

Source: Pixabay released under Creative Commons CC0:
https://pixabay.com/es/pregunta-imagen-plaza-556104/

References

- [Cavoukian2010]: Privacy by Design The 7 Foundational Principles Implementation and Mapping of Fair Information Practices, 2010.
- [D' Acquisto2015]: Privacy by design in big data: An overview of privacy enhancing technologies in the era of big data analytics.
- [Gürses2016]: Privacy Engineering: Shaping an Emerging Field of Research and Practice IEEE Security and Privacy, 14:2, pp. 40-46, 2016.
- [NIST2014]: NIST Privacy Engineering Objectives and Risk Model Discussion Draft. Introduction, 2014.
- [Danezis2014]: Privacy and Data Protection by Design – from policy to engineering, 2014.
- [National Academy2010]: Toward Better Usability, Security, and Privacy of Information Technology: Report of a Workshop
- [Europe2006] European Parliament and the Council: Directive 2006/24/EC of the European Parliament and if the council; www.ispai.ie/DR%20as%20published%20OJ%2013-04-06.pdf
- [EC2014] Progress on EU data protection reform now irreversible following European Parliament vote. Accessed at http://europa.eu/rapid/press-release_MEMO-14-186_en.htm on 12.11.2014.
- [EC-Prot-2014] European Commission: Protection of personal data: http://ec.europa.eu/justice/data-protection/index_en.htm
- [WaBr1890] Samuel D. Warren, Louis D. Brandeis: The Right to Privacy, Harvard Law Review; Vol. IV; December 15, 1890, No. 5; http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html

Deutsche Telekom Chair of Mobile Business & Multilateral Security

Jetzabel Serna, PhD, and Majid Hatamian, MSc.
Goethe University Frankfurt
E-Mail: project.seminar@m-chair.de
WWW: www.m-chair.de