Security, Privacy and Trust in Emerging Technologies
Project Seminar Kick-off

2015-10-20, Frankfurt, Germany

Dr. Jetzabel Serna-Olvera and MSc. Welderufael Tesfay
project.seminar@m-chair.de
Chair of Mobile Business & Multilateral Security
Goethe University Frankfurt

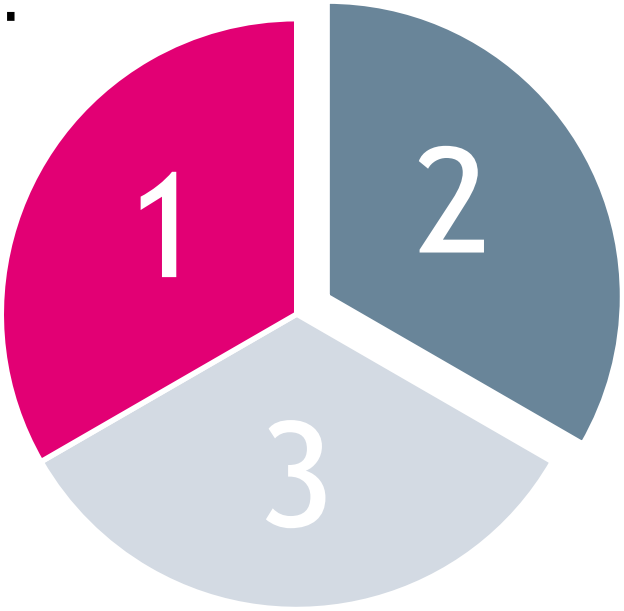
mobile business

Agenda

- Organizational information
- Introduction to the topics
- Upcoming exam (presentations)
- Questions

Organizational Information
Seminar Grade

- This project seminar consists of three administrative parts:



1) Exam (one third)
2) Report (one third)
3) 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).

Organizational Information
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 **35 pages** (including cover, table of contents, index and references)

Organizational Information 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

Organizational Information
Deadlines and Exam Info

- Exam
  - Date: 10.11.2015
  - Time: 10:00 - 12:00
  - Room: 2.202
- Submission of Structure & Draft Version
  - voluntary (but recommended)
- Submission of Seminar Paper
  - 11.01.2016, until 14:00
- Presentation of the results:
  - 25.01.2016 & 26.01.2016 09:00-18:00
  - Room : RuW 2.202

Organizational Information Contact

In case of any problems during the seminar you can contact your supervisor:

- Via Mail:
  - jetzabel.serna@m-chair.de
  - welderufael.tesfay@m-chair.de
- Via Phone:
  - Jetzabel Serna: (0)69 / 798 34667
  - Welderufael Tesfay: (0)69 / 798 34706
- For comprehensive questions please make an appointment.

mobile business

Agenda

- Organizational information
- Introduction to the topics
- Upcoming exam
- Questions

Introduction to Security

February 15, 2012, 2:14PM

Anonymous-Linked Attacks Hit US Stock Exchanges

(Distributed) „Denial of Service“-Attacks on e-auctioneers/broker/betting office

March 5, 2012, 3:40PM

Hacker Group Breaches Library of Congress Site, Publishes Passwords

Security threats and attacks

- A threat is an undesirable negative impact on your assets. A threat materializes when an attack succeeds.
- An attack is a sequence of steps until the final target is reached.
- An attacker can be passive or active
  - Passive: listens to traffic
  - Active: may modify, insert new messages, or corrupt network management information

[Go06]

Example: Risks of Unprotected Market Activities

Provider

- no payment – debtor cannot be captured
- wrong or fake orders
- copyright violations
- www attacks
- internal server intrusion
- …

Consumer

- unwanted deliveries (false, not ordered, …)
- unauthorized / unexpected direct debt of money, e.g. from a credit card account
- unwanted advertising mail (“spamming”)
- transparent consumers
- …

Security goals

- the **control of** unwanted intrusion, misuse, modification, damage or denial of a computer system, a computer network and network-accessible resources. [Ba10]

Security aspects

A very human discrepancy

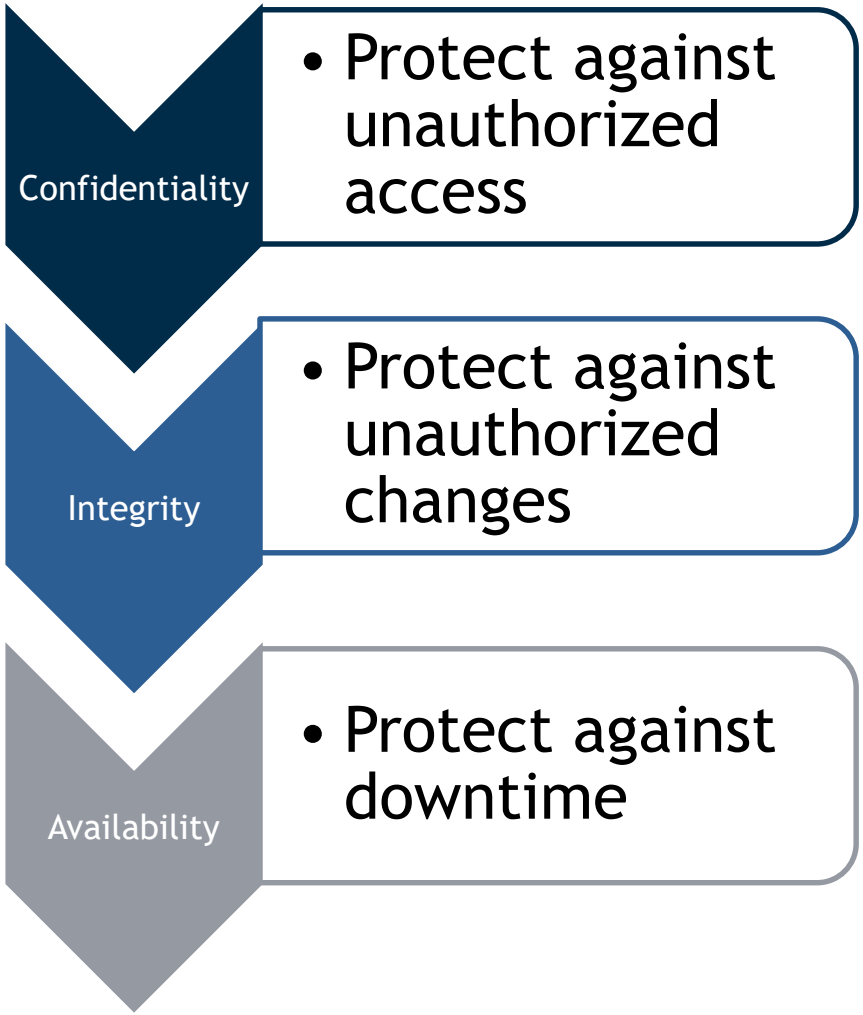
- **Privacy**
  Protect the own sphere and the own values/assets
- **Trust**
  Reliance on something

Kind of technical arrangement

- **Confidentiality**
  Information delivery just to whom it is intended
- **Integrity**
  no faking of information
- **Availability**
  no system failures / no loss of data
- **Accountability**
  actions are always accountable to responsible parties

A **combination** of technical, organizational and legal methods is necessary.

Security attributes



- Ensure the confidentiality of resources
- Protect the integrity of data
- Maintain availability of the IT resources and infrastructure
- Ensure the privacy of personally identifiable data
- Enforce access control
- Monitor IT for policy violations
- Support business tasks and the overall mission of the organization

mobile business

Authentication

- **Definition:** Authentication is the binding of an identifier to a subject.
- The authentication process consists of:
  - Obtaining authentication information from the subject
  - Analyzing the data
  - Determining if data is associated with that subject
- The computer must store some information about the subject.

Authentication Information

- The information comes from one (or more) of the following:
  - What the subject knows
    - PIN, passwords, pass-phrases, secret information
  - What the subject has
    - Keys, tokens, smart cards
  - What the subject is
    - Fingerprints, iris, retinal characteristics
  - Where the subject is
    - In front of a particular terminal, located by a particular radio receiver

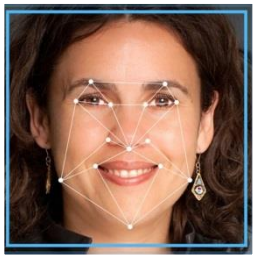
[Bi05]

What you are - Biometrics

- Identification by physical attributes is as old as humanity.
- Biometrics is the automated measurement of **biological** or **behavioural** features.
- Biometric systems provide a percentage of similarity between samples, i.e., an individual's identity is confirmed only if the resulting percentage is above a **predefined threshold.**

Physiological Biometrics

Fingerprint



Facial

DNA

Hand

Lip print

Iris & Retina

Behavioral Biometrics

Voice

Keystroke Dynamics

Signature

Gait

Biometrics Issues and Risks

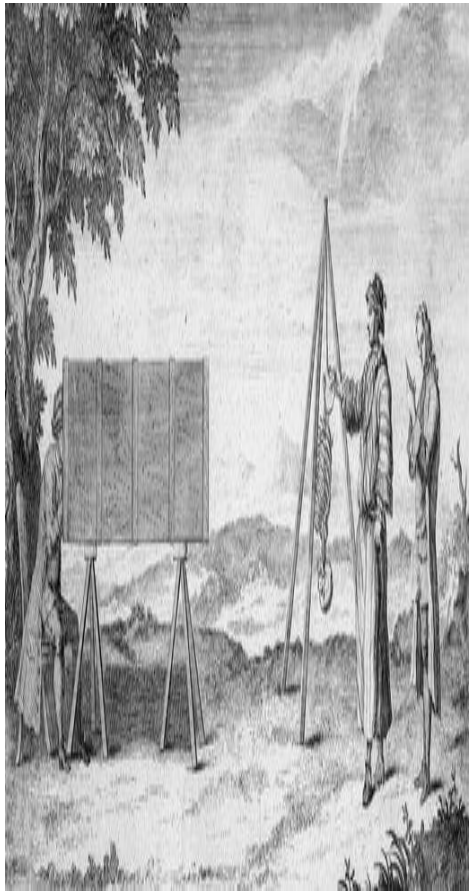
- Patterns will hardly ever match precisely.

false positives and *false negatives*

  - If data can be copied by a potential attacker, identity fraud can occur.
  - Replay attacks are possible.
  - Biometric attribute can not be **revoked** easily.

Introduction to Privacy-1

- Early day definitions:
  - "The right to be let alone" Warren and Brandeis, 1890, Harvard Law Review: "The right to privacy"
  - "A reflection of the concept of privacy at the 19th century when print media and new technological innovations like photography were responsible for the growing invasion of private information." Kolter, Jan Paul. *User-centric Privacy: A Usable and Provider-independent Privacy Infrastructure*. Vol. 41. BoD–Books on Demand, 2010.



Introduction to Privacy-2

- 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

Introduction to Privacy-3

- Contemporary
  - It is complex.
  - “the ability of the individuals to protect information about him self. "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 ”

Dimensions of Privacy Protection

- Technical privacy protection
  - Privacy-preserving authentication/authorizations
  - Minimalistic disclosure of personally identifying information (PII)
- Legal
  - Supportive legal frameworks (e.g., right to be forgotten, safe harbor)
- User awareness
  - Putting access control lists (e.g., Facebook)

TECHNICAL PRIVACY PROTECTION

Technical Privacy Protection

- Typical protection techniques are:
  - Privacy-by-Design
  - Anonymization/Pseudeonymization and identity management tools
  - Spontaneous switching between different levels of anonymity and pseudonymity depending on the context

Privacy-preserving communication systems

- The Anonymizer (www.anonymizer.com)
  - Anonymizer's personal VPN routes all users' traffic through an encrypted tunnel directly from users laptop to the anonymiser's secure and hardened servers and network, which further masks REAL IP address to ensure that users have complete and continuous anonymity for all their online activities.
- Mixmaster – Anonymous Remailer(http://mixmaster.sourceforge.net)
  - anonymous remailer which sends messages in fixed-size packets and reorders them, preventing anyone watching the messages go in and out of remailers from tracing them. It is an implementation of a Chaumian Mix network.
- Onion Routing: Tor Network(http://tor.eff.org/)
  - An advanced form of proxy routing that uses a network of nodes that constantly encrypt users data packets at every step.
- Java Anonymous Proxy (JAP) (http://anon.inf.tu-dresden.de)
  - Instead of connecting directly to a webserver, users take a detour, connecting with encryption through several intermediaries, so-called Mixes. JAP uses a predetermined sequence for the mixes.
- P3P – Platform for Privacy Preferences(www.w3.org/P3P)
  - enables Websites to express their privacy practices in a standard format that can be retrieved automatically and interpreted easily by user agents.

(For more please check Privacy Protection lecture of INKO)

Privacy-by-Design

- PbD refers to the philosophy and approach of embedding privacy into the design specifications of various technologies.
- The concept is an example of value sensitive design, i.e., to take human values into account in a well defined matter throughout the whole process

The 7 Foundational Principles of Privacy-by-Design

- **Proactive not Reactive**:- anticipates and prevents privacy invasive events before they happen
- **Privacy as the Default Setting**:- seeks to deliver the maximum degree of privacy by ensuring that personal data are automatically protected in any given IT system or business practice.
- **Privacy Embedded into Design**:- embedded into the design and architecture of IT systems and business practices. It is not bolted on as an add-on, after the fact
- **Full Functionality — Positive-Sum, not Zero-Sum**:- Privacy by Design avoids the pretense of false dichotomies, such as privacy vs. security, demonstrating that it is possible to have both.
- **End-to-End Security — Full Lifecycle Protection**:- having been embedded into the system prior to the first element of information being collected, extends securely throughout the entire lifecycle of the data involved — strong security measures are essential to privacy, from start to finish.
- **Visibility and Transparency — Keep it Open**:- seeks to assure all stakeholders that whatever the business practice or technology involved, it is in fact, operating according to the stated promises and objectives, subject to independent verification. Its component parts and operations remain visible and transparent, to users and providers alike. Remember, trust but verify.
- **Respect for User Privacy — Keep it User-Centric**:- PbD requires architects and operators to keep the interests of the individual uppermost by offering such measures as strong privacy defaults, appropriate notice, and empowering userfriendly options. Keep it user-centric.

  [Cavoukian, A. (2009).]

LEGAL PRIVACY PROTECTION

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

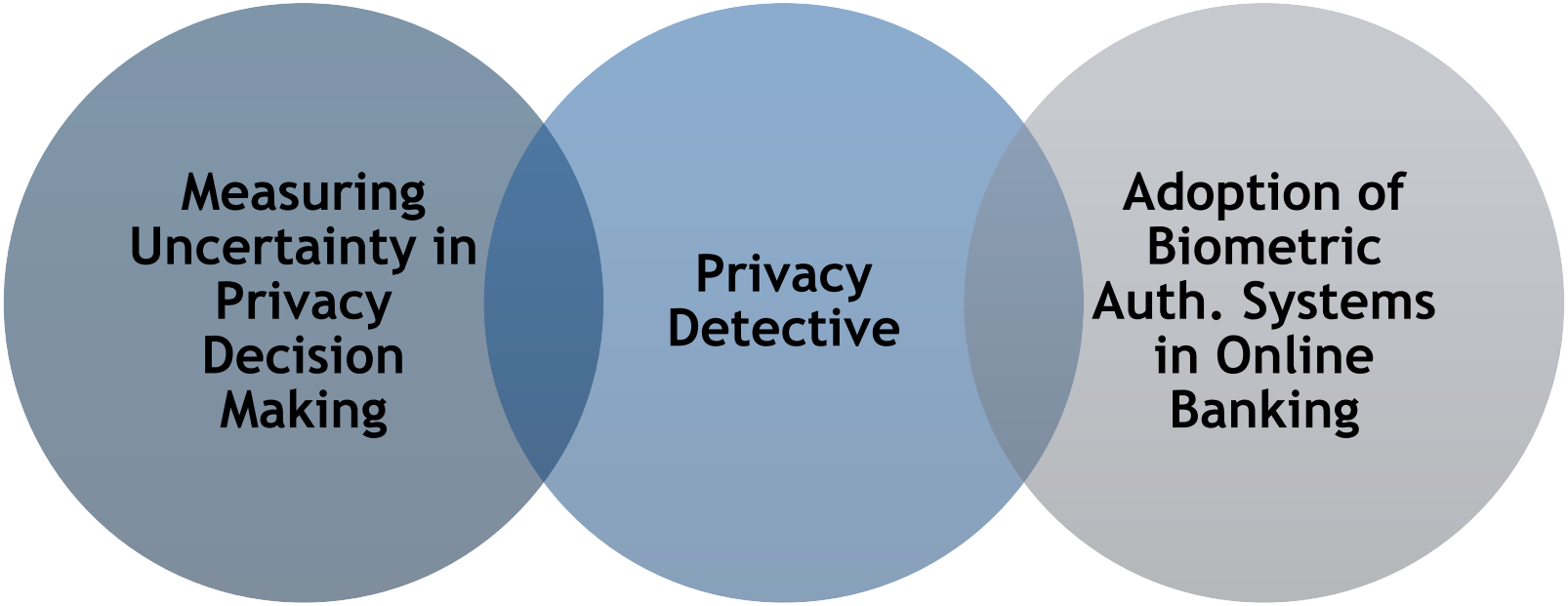
6. **Data subject's rights:** The parties involved have the right to take cognisance of and to update their data as well as the right to raise objections.
7. **Processing by a processor:** This rule states that, with the transfer of personal data to a processor, the rights of the data subject remain 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]

USER AWARENESS

User Awareness

- Privacy incidents
- Global scandals (e.g., Snowden revelations)
- Trainings and user awareness workshops
  - http://www.privacyawarenessweek.org/
- Privacy paradox
  - Users state that they are worried about their privacy, but at the same time publish detailed personal information on their profiles (Barnes, 2006).
- Uncertainty in privacy decision making, lack of quantified risk communications, etc.
- Need for supporting technologies
  - Privacy detection and advisors
  - Usable privacy-preserving technologies and consents.

Introduction to the Topics



Measuring Uncertainty in Privacy Decision Making

- Incomplete information, therefore ambiguous, risky, and uncertain.
- Complexity of situations
- Lack of context knowledge
- **Goal:** measure uncertainty using measurement constructs.

Privacy Detective

- Identity management services provide privacy-preserving mechanisms.
- Users reveal their identities in the ***content***, and ***context*** of their communications.
- Approach:
  - Coupling IdM with Machine Learning
- **Goal:** Develop a privacy detective to help users in privacy decision making.

Adoption of Biometric Authentication Systems in Online Banking

- Low adoption of biometrics in online banking systems
- Concepts: security, usability, privacy, trust, liability and data protection
- Approach: develop and evaluate a questionnaire
- **Goal:** investigate the factors influencing the adoption of biometric technologies in online banking.

Upcoming Exam

- Resources
  - this presentation + references on the seminar webpage
  - Authentication lecture based in INKO
  - Privacy protection lecture based in INKO

Deutsche Telekom Chair of Mobile Business & Multilateral Security

Asst. Prof. Dr. Jetzabel Serna, and Welderufael Tesfay, MSc.

Goethe University Frankfurt

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

WWW: www.m-chair.de