Privacy in E-learning

Hauptseminar “E-Learning” – Sommersemester 2008

Simon Mansfeld
LFE Medieninformatik
23.07.08

Ludwig
Maximilians-
Universität
München
LMU

Outline

- Privacy (What? Why?)
- Framework for Privacy-Preserving E-learning
  - Privacy Requirements
  - Grading of Privacy Sensation
- Privacy-Preserving Solutions
  - Mix Networks and Secure Channels
  - Policies
  - Anonymous Credentials
- Pros and Cons of these Systems
- Balancing Act Between Anonymity and Identification

1. Privacy
What Is Privacy?

- *"Privacy can be described as a learner's ability to maintain* a '**personal space**' *within which the learner can* ***control*** *the conditions under which* ***personal information*** *is* ***shared*** *with others."*

  (El-Khatib et. al)

→ Freedom to choose what others may see

→ True nature undetectable

1. Privacy
Why Is Privacy Necessary?

- Competitive reasons
  - Advantage on the market
  - Electors interest
  - …
- Personal reasons
  - Protection against the tutor
  - Hiding demographic information (age, race, gender, …)
  - …

1. Privacy E-commerce Not Suitable

- Other electronic applications (e. g. e-commerce) fulfill privacy requirements

- Not suitable
  - Main problem: kind of transaction
    - Transactions between client and system are independent
    - E-learning: interactive, interwined
  - History
    - Not necessary for e-commerce
    - E-learning: important showing qualifications (e. g.)

1. Privacy
Current Standards

Problems

- Missing specification of models and technologies (IEEE P1484)
- No details implemented (IMS CLC)
- Less regard on privacy and security (ARIADNE)

2. Privacy-Preserving E-learning Three Privacy Requirements (1/2)

- Data integrity
- Confidentiality
- Access control

- Data integrity
  - Deletion or modification while transmitting process must not be possible
  - Important: Learner commits answer of an exam

2. Privacy-Preserving E-learning Three Privacy Requirements (2/2)

- Confidentiality
  - Private information only seen by persons learners want to

    (e. g. test scores = appropriated tutor)
  - Important: Personal and competitive reasons
  - Two stages:
    - While transmission (→ encryption)
    - Storage
- Access control
  - Restricted access to personal data
  - Important: Problem if super-users (“admins”) exist

2. Privacy-Preserving E-learning Grading Of Privacy Sensation

- *"Different learners have different privacy requirements"* (Aïmeur et al., 2008)

- Possible points of interest from a privacy point of view
  - Identity: All information make it know who the user physically is
  - Demographic profile: Age, gender, race, …
  - Learning profile: Learners qualification and learning style
  - Course history: List of graduated courses and current courses

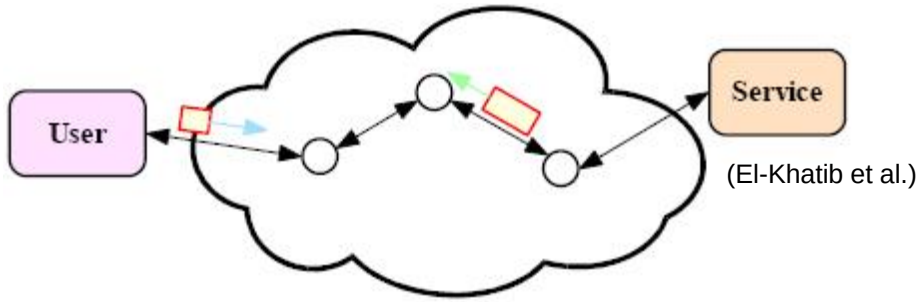
2. Privacy-Preserving E-learning Grading Of Privacy Sensation

- Possible grading:
  - No privacy → full privacy: Does not care about / wants privacy
    → All profiles secret
  - No tracking → strong tracking: Not even know the user is a visitor
    → All activities related to a certain user

- Individual must have possibility to decide
  - Advantages of e-learning systems vs. telling personal information
  - Different persons have different privacy sensations
  - For different applications exist different privacy sensations

3. Privacy-Preserving Solutions Mix Networks

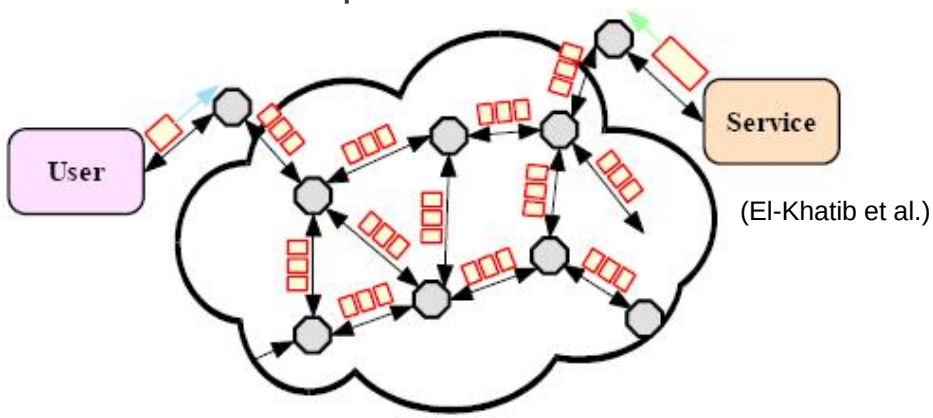
- Secure Channel



(El-Khatib et al.)

  - Only channel between user and service encrypted
  - Traffic analyze and time detect possible!

- Mix Network

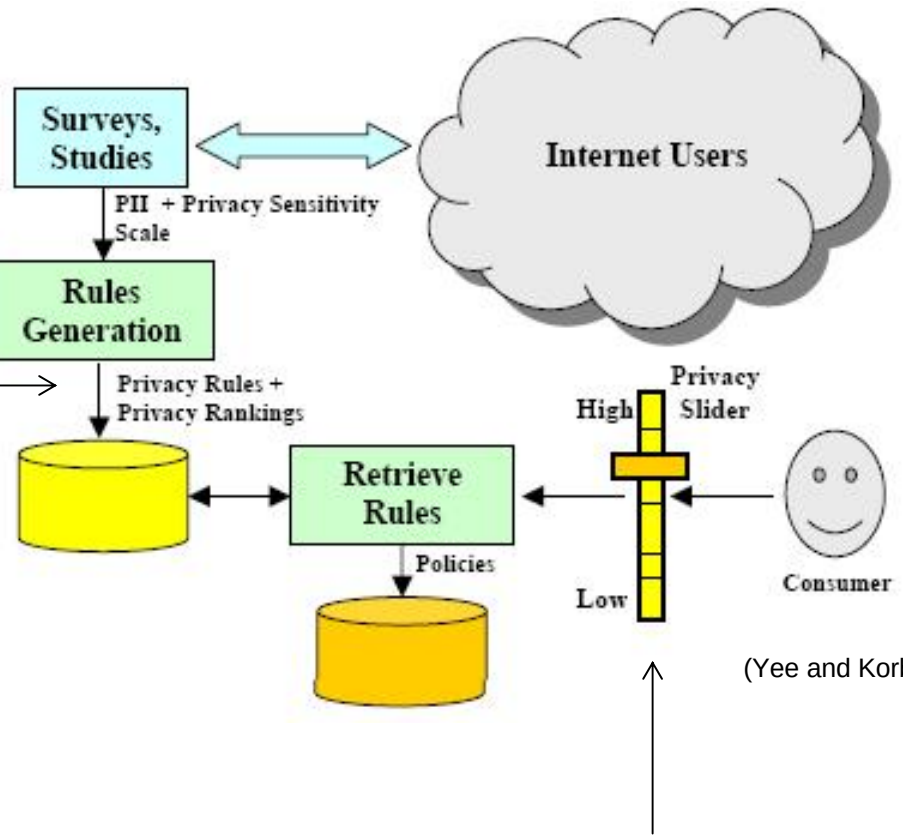


(El-Khatib et al.)

  - Date and traffic from different users mixed at each node
  - Difficult to determine origin, destination and nature of the message

3. Privacy-Preserving Solutions Policies

- Provider gets sensitivity of privacy from a survey
- Corresponding to a providers privacy policy (specify what PII is required) the provider constructs and ranks the privacy rules
- Set of consumer privacy rules, ranked by PII sensitivity for different providers
- Privacy rules are expressed in an machine-readable language (e. g. APPEL)
- Consumer obtain online from policy



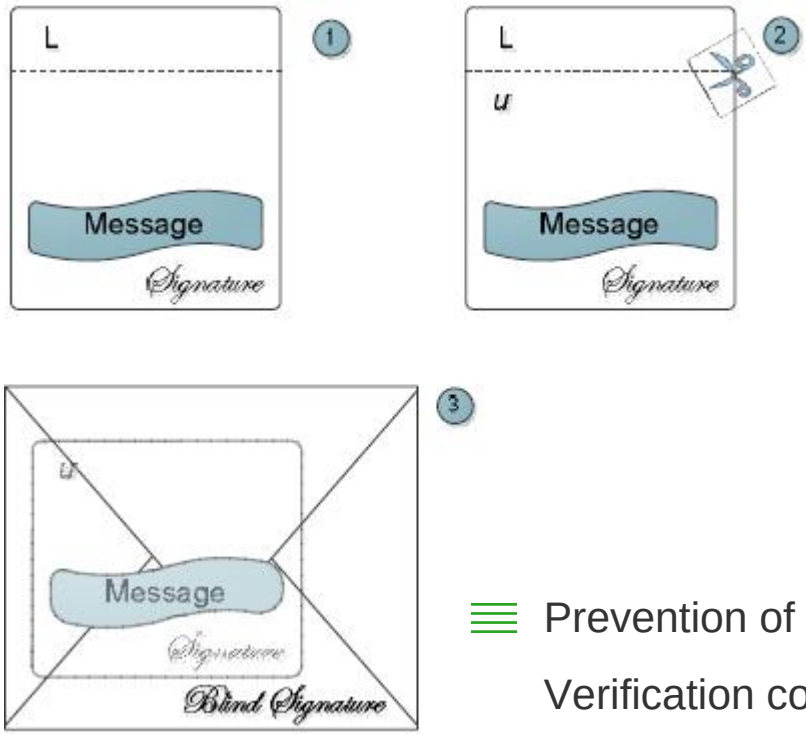
(Yee and Korba)

provider the privacy rules, they specify by using the slider

- Adapt rules for different services

3. Privacy-Preserving Solutions Anonymous Credentials for ES

- Ensuring that users have certain qualifications without leaving traces to detect their real identity



(Aïmeur et al.)

- Example: Anonymous Learner Credential
  - Goal: Prove to an external entity (EE) that the user was enrolled in an e-learning system (ES)
  - Learner (known as L) creates a pseudonym *u* in the EE
  - Request of L to digitally sign m (content of registration certificate) (1)
  - ES signs m and sends it back to L (2)
  - L asks the ES for a blind signature of m (3)
  - The ES blindly sings m
- Prevention of sharing credentials:

  Verification contains an entry (learner's pseudonym) in the Revocation of Anonymous Credential List (RACL).

4. Pros and Cons

Ludwig Maximilians Universität München

- Mix networks
  - [+] time analyze, origin and destination hard to determine
  - [–] increasing of costs (overhead), data transmission time (delay)

- Policies
  - [+] create own privacy rules, warning if there is a mismatch
  - [–] no guarantee that the web site acts like it claims to do

---

- Anonymous Credentials
  - [+] association between acquired certifications and learners’ pseudonyms
  - [–] users' trust relies on the authenticity of the public key

5. Balancing Act
Anonymity ⇔ Identification

- Balancing Act
  - Adaptable to learning style
  - Mobile and individual useable
  - Test situations: Ensure that users are who they claim to be

➔ The more adapted the more personal data are important

➔ For test situation, the users' identities must be known