Privacy and Trust
Frameworks/Systems

Presented by Zalia Shams
PRIME - Privacy and Identity Management for Europe

- Primarily a research project.
- Aimed to develop a working prototype of a Privacy-enhancing Identity Management System.
- www.prime-project.eu
Trust In PRIME (2005)

Christer Andersson*,
Jan Camenisch‡,
Stephen Crane§,
Simone Fischer-Hübner*,
Ronald Leenes†,
Siani Pearson§,
John Sören Pettersson* and
Dieter Sommer‡

* Karlstad University
‡IBM Zurich Research Laboratory,
§Hewlett-Packard Laboratories,
†Tilburg University
Where Identity Information is Stored?

A complete picture of someone’s movements, transactions, whereabouts and relationships can be found from the trail left from interaction with websites!!!
A Typical e-Shopping Scenario
PRIME Solution

- Credit Card Payment
- Browsing
- Advice, Purchase
- Direct Payment
- Direct Delivery
- Anonymous Delivery
- Pick up point/Delivery Service

Customer → Bank → Merchant

Usable Security – CS 6204 – Fall, 2009 – Dennis Kafura – Virginia Tech
Contribution

- Introduces the PRIME technical architecture.
- Discusses end user’s trust influencing factors
  - Socio-psychological factors
  - HCI aspects
- Describes necessity of
  - HCI research,
  - User studies and
  - Socio-psychological research in system design.
Design Principles

- Start from maximum privacy (anonymity).
- State explicit privacy rules.
- Privacy rules must be enforced, not just stated.
- System should be transparent (data track).
PRIME Architecture

User Side:
- Stores users’ personal data and credentials in repository
- Protects these by software layer.

Services Side:
- Interacts with users.
- Provide evidence of its trustworthiness.
- Protects user’s data once released.

Fig. 1: PRIME Architecture Overview.
PRIME Architecture

**User Side:**
- Stores users’ personal data and credentials in repository
- Protects these by software layer.

**Services Side:**
- Interacts with users.
- Provide evidence of its trustworthiness.
- Protects user’s data once released.

Fig. 1: PRIME Architecture Overview.
PRIME Architecture

**User Side:**
- Stores users’ personal data and credentials in repository
- Protects these by software layer.

**Services Side:**
- Interacts with users.
- Provides evidence of its trustworthiness.
- Protects user’s data once released.

Applications access prime functionality by middleware components.
Components and Mechanisms

Combining Accountability and Privacy (Access Control):
- User side checks evidence of service provider’s trustworthiness (e.g. privacy seal)
- Services side checks proof of individual attributes denoted as Anonymous Credentials

Enforcing Privacy Policy (Before and After):
- Both sides checks compliance on policy and obligation of data handling by Automated Trust and Policy Negotiation.
- A component on service side enforces agreed obligations (e.g. limited time data retention). This is Obligation Management.

Transparency:
- User can track their data that are released to services side.

Trusted User Interface: Prime console is used as front-end.
A Typical Interaction

- **User's identity control component**
  - Protected resource access request
  - Confirmation data request (e.g. age)
  - Trust data (e.g. privacy seal) requested
  - Trust + Policy compliance data submitted

- **Front end access control component**
  - Actual release of data
  - Access is granted

- **Trust and policy negotiation component**
  - User Console
  - Obligation Management
## Socio-Psychological Factors

<table>
<thead>
<tr>
<th>Trust Layers</th>
<th>Influence</th>
</tr>
</thead>
</table>
| Socio-cultural   | ▪ Relates to trust in Society.  
                  ▪ Strongly associate with known people, likely to have low trust in online stores.                                              |
| Institutional    | ▪ Relates to trust in institution.  
                  ▪ Legal and technological safeguards enhances peoples’ trust.                                                                          |
| Service area     | ▪ Concerns trust in a particular sector of economic activity (e.g. Medical profession > banking sector > internet service provider).         |
| Application layer| ▪ Concerns trust in a particular service provider.  
                  ▪ Irregular events creates distrust.                                                                                                  |
| Media layer      | ▪ Relates to communication channel.  
                  ▪ Visible icons like lock sign in pages can increase trust.                                                                                  |
Usability Tests and Problems found

- A series of usability tests were performed for an e-shopping scenario using interactive mock-ups.

- Results:
  1. Many users did not trust the claim that system will protect their data and privacy.
  2. “Internet is insecure anyway”.
  3. “I did not agree my mental picture that I can buy a book anonymously”.
  4. Users had difficulties to
    - mentally differentiate server and user side identity managements.
    - understand that PRIME console is within users’ control and protects their identities.
Possible Solutions for Enhancing Trust

- "Institutional Trust" has to put into PRIME from external sources. (e.g. consumers’ organizations recommend PRIME).
- Trustworthiness of the service provider must be conveyed to user.
- Data blocking, rectifying or deleting facilities need to be added.
- Help functions for legal issues need to be added.
- User side and services side Identity Management Middleware functionalities should be clearly distinguishable by UI.
Conclusions

- Powerful trust and privacy-enhancing technical mechanisms are developed in PRIME.
- Social factor and usability research have to accompany the development to enhance trust in users’.
Discussions

- Do you think anonymous credentials support unlinkability/privacy appropriately? Is so why? If not, why?
- The paper mentioned—“… buying anonymously via Internet did not fit to a user’s mental picture… it is clear that providing anonymous shopping will wake awake an interest in the privacy technology”. How this conflict can be resolved?
- Do you think PRIME is transparent enough? If not, what can be done to increase transparency?
- Up to what extent PRIME middleware should enforce service provider and third party’s back-end? (e.g. only give a message that you should delete x customers’ data
  or,
  Check back-end database and delete the data itself.)