Concepts of Privacy-Enhancing Identity Management for Privacy-Enhancing Security Technologies

PRISE Conference
“Towards privacy enhancing security technologies – the next steps”
April 28-29, 2008 in Vienna

Marit Hansen
Unabhängiges Landeszentrum für Datenschutz
Schleswig-Holstein
Overview

- **Enhancing user-centric identity management:**
  PRIME – Privacy and Identity Management for Europe
  - Objective
  - Building blocks
    - “Various Pseudonyms and Private Credentials”
    - “Anonymous Communication”
    - “Transparency Functionality”

- **How to use components of privacy-enhancing identity management in security technologies?**
Vision of PRIME
– Privacy and Identity Management for Europe

In the Information Society, users can act and interact in a safe and secure way while retaining control of their private sphere.
Example: Anonymous Wine Shop

Proof (age > 20), enc_k(name, address)

“Anonymous user”
Proof of age > 20 AND
Encryption of name & addr with K

“Registered user”
Cryptographic pseudonym

User

Wine Shop

enc_k(name, address)

Shipping Company

K (public key)
Building Block “Various Pseudonyms and Private Credentials”

Anonymity & strong authentication at the same time
What’s the Problem?

Driver's License

Insurance

Dangerous Cars

Slide: PRIME Project / Jan Camenisch
The Solution: Private Credentials

Driver's License

Insurance

Dangerous Cars

ULD-i

Slide: PRIME Project / Jan Camenisch
The Solution: Private Credentials

Slide: PRIME Project / Jan Camenisch
Drivers' License
Insurance
cars
Roles
"Attributed based access control"
Policies towards users
Enforcement of policies
Change of business processes
Privacy policy
Data minimization
Easy management of partial identities
Usable interfaces
Anonymous Communication Infrastructure
Interested in sender of Anonymous Communication Infrastructure (1/3)

Judge

Law Enforcement Agency

Anonymizers in same jurisdiction

“Suspicious”

Messages

Slide: AN.ON Project / Stefan Köpsell – www.anon-online.de
Anonymous Communication Infrastructure (2/3)

- Users
  - IP=a
  - IP=b
  - IP=c

- Anonymizers in same jurisdiction

- Judge
  - Court Order

- Law Enforcement Agency
  - Surveillance Request
  - Interested in sender of "Suspicious"

- Messages

Slide: AN.ON Project / Stefan Köpsell – www.anon-online.de
Anonymous Communication Infrastructure (3/3)

Monitoring of specific single cases instead of full surveillance

Surveillance Request

Judge

Law Enforcement Agency

Interested in sender of "Suspicious"

IP=a

IP=b

IP=c

Anonymizers in same jurisdiction

Users

Messages

Slide: AN.ON Project / Stefan Köpsell – www.anon-online.de
Building Block “Transparency Functionality”

Giving information in an understandable way & empowering users to act accordingly
Overview: Transparency Functionality

• Objective: empower users to understand and act

• Examples in privacy-enhancing identity management:
  – Showing privacy policies: conditions of data processing
  – Trustworthiness of transaction partners
  – History function
  – Support of exercising privacy rights
  – Security feed
  – Tutorials, demonstrations and simulations
  – Server-side: full audit trail
Understandable Privacy Policies

- **Jurisdiction:**
  Differences in law (data protection & law enforcement)
- **Transparency on data processing**

| Extract of Iconset for Data-Privacy Declarations v0.1 (Mehldau 2007) |
|---|---|
| **How is my Data handled?** | **For how long?** |
| - deleted | - end of usage / logout |
| - saved | - end of contract |
| - anonymized | - timestamp / hours |
| - encrypted | - days |
| - published | - |
| - passed on | - |

<table>
<thead>
<tr>
<th>Extract of Creative Commons-like Icons (Rundle 2006)</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Money icon" /> You agree not to trade or sell this data.</td>
</tr>
<tr>
<td><img src="image" alt="Information icon" /> You agree to make available to me the data that you have on me without my having to pay for it/at a minimal charge.</td>
</tr>
<tr>
<td><img src="image" alt="Pencil icon" /> You allow me to address inaccuracies in the data and request its removal.</td>
</tr>
<tr>
<td><img src="image" alt="Lock icon" /> You agree to take reasonable steps to keep my data secure.</td>
</tr>
<tr>
<td><img src="image" alt="Filing Cabinet icon" /> You agree to arrange with X organization to help resolve any disputes we have over your treatment of this data. [The seal / name of the entity follows.]</td>
</tr>
</tbody>
</table>
Online Help Functions

- Support for exercising one’s privacy rights, i.e.,
  - to request ...
    - … access to personal data
    - … rectification of inaccurate personal data
    - … erasure of illegally stored data
  - to give or withdraw consent
  - to ask for further information on data processing

- Challenge: exercising rights under pseudonym
Security Feed

- Demand of Security Breach Notification Acts
- Information on security & privacy incidents and threats
- Implemented as RSS feed

The provider CVE reports a vulnerability about the communication partner http://www.DoubleClack.com with category 'Other Errors' and with high priority.

Identity Theft
On 20th July 2006 hackers may have accessed all customer data from transactions in 2006. Unauthorized use cannot be excluded. More information at: http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2004-4

Assumed detection date: 07/20/2006 12:30
Assumed used date: 07/20/2006 12:00
Publication date: 07/20/2006 13:00
Privacy-Enhancing Identity Management Concepts for Privacy-Enhancing Security Technologies?
<table>
<thead>
<tr>
<th>Transparency functionality</th>
<th>Objective in Privacy- Enhancing IDM</th>
<th>Security functionality</th>
</tr>
</thead>
<tbody>
<tr>
<td>Various pseudonyms and private credentials</td>
<td>Protection against unauthorized linkage</td>
<td></td>
</tr>
<tr>
<td>Anonymous communication infrastructure</td>
<td>Protection against unauthorized identification</td>
<td></td>
</tr>
<tr>
<td>Policies</td>
<td>Make clear conditions for data processing</td>
<td></td>
</tr>
<tr>
<td>Support to exercise privacy rights</td>
<td>Empower users, establish contacts to DPA / consumer protection</td>
<td></td>
</tr>
<tr>
<td>Security feed</td>
<td>Inform people concerned on breaches</td>
<td></td>
</tr>
<tr>
<td>Server-side: full audit trail</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Transparency functionality</td>
<td>Objective in Privacy-Enhancing IDM</td>
<td>Security functionality</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-----------------------------------</td>
<td>-----------------------</td>
</tr>
<tr>
<td>Various pseudonyms and private credentials</td>
<td>Protection against unauthorized linkage</td>
<td>Prevent misuse, enable authorized singularized linkage</td>
</tr>
<tr>
<td>Anonymous communication infrastructure</td>
<td>Protection against unauthorized identification</td>
<td></td>
</tr>
<tr>
<td>Policies</td>
<td>Make clear conditions for data processing</td>
<td></td>
</tr>
<tr>
<td>Support to exercise privacy rights</td>
<td>Empower users, establish contacts to DPA / consumer protection</td>
<td></td>
</tr>
<tr>
<td>Security feed</td>
<td>Inform people concerned on breaches</td>
<td></td>
</tr>
<tr>
<td>Server-side: full audit trail</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Transparency functionality</td>
<td>Objective in Privacy-Enhancing IDM</td>
<td>Security functionality</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-----------------------------------</td>
<td>------------------------</td>
</tr>
<tr>
<td>Various pseudonyms and private credentials</td>
<td>Protection against unauthorized linkage</td>
<td>Prevent misuse, enable authorized singularized linkage</td>
</tr>
<tr>
<td>Anonymous communication infrastructure</td>
<td>Protection against unauthorized identification</td>
<td>Enable authorized singularized identification</td>
</tr>
<tr>
<td>Policies</td>
<td>Make clear conditions for data processing</td>
<td></td>
</tr>
<tr>
<td>Support to exercise privacy rights</td>
<td>Empower users, establish contacts to DPA / consumer protection</td>
<td></td>
</tr>
<tr>
<td>Security feed</td>
<td>Inform people concerned on breaches</td>
<td></td>
</tr>
<tr>
<td>Server-side: full audit trail</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Transparency functionality</td>
<td>Objective in Privacy-Enhancing IDM</td>
<td>Security functionality</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-----------------------------------</td>
<td>------------------------</td>
</tr>
<tr>
<td>Various pseudonyms and private credentials</td>
<td>Protection against unauthorized linkage</td>
<td>Prevent misuse, enable authorized singularized linkage</td>
</tr>
<tr>
<td>Anonymous communication infrastructure</td>
<td>Protection against unauthorized identification</td>
<td>Enable authorized singularized identification</td>
</tr>
<tr>
<td>Policies</td>
<td>Make clear conditions for data processing</td>
<td>Ditto; e.g., information on jurisdiction</td>
</tr>
<tr>
<td>Support to exercise privacy rights</td>
<td>Empower users, establish contacts to DPA / consumer protection</td>
<td></td>
</tr>
<tr>
<td>Security feed</td>
<td>Inform people concerned on breaches</td>
<td></td>
</tr>
<tr>
<td>Server-side: full audit trail</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Transparency functionality</td>
<td>Objective in Privacy-Enhancing IDM</td>
<td>Security functionality</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-----------------------------------</td>
<td>------------------------</td>
</tr>
<tr>
<td>Various pseudonyms and private credentials</td>
<td>Protection against unauthorized linkage</td>
<td>Prevent misuse, enable authorized singularized linkage</td>
</tr>
<tr>
<td>Anonymous communication infrastructure</td>
<td>Protection against unauthorized identification</td>
<td>Enable authorized singularized identification</td>
</tr>
<tr>
<td>Policies</td>
<td>Make clear conditions for data processing</td>
<td>Ditto; e.g., information on jurisdiction</td>
</tr>
<tr>
<td>Support to exercise privacy rights</td>
<td>Empower users, establish contacts to DPA / consumer protection</td>
<td>Extension to “security bodies” possible: defined processes for access, better acceptance</td>
</tr>
<tr>
<td>Security feed</td>
<td>Inform people concerned on breaches</td>
<td></td>
</tr>
<tr>
<td>Server-side: full audit trail</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Transparency functionality</td>
<td>Objective in Privacy-Enhancing IDM</td>
<td>Security functionality</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-----------------------------------</td>
<td>------------------------</td>
</tr>
<tr>
<td>Various pseudonyms and private credentials</td>
<td>Protection against unauthorized linkage</td>
<td>Prevent misuse, enable authorized singularized linkage</td>
</tr>
<tr>
<td>Anonymous communication infrastructure</td>
<td>Protection against unauthorized identification</td>
<td>Enable authorized singularized identification</td>
</tr>
<tr>
<td>Policies</td>
<td>Make clear conditions for data processing</td>
<td>Ditto; e.g., information on jurisdiction</td>
</tr>
<tr>
<td>Support to exercise privacy rights</td>
<td>Empower users, establish contacts to DPA / consumer protection</td>
<td>Extension to “security bodies” possible: defined processes for access, better acceptance</td>
</tr>
<tr>
<td>Security feed</td>
<td>Inform people concerned on breaches</td>
<td>Use channel for communication to users after surveillance</td>
</tr>
<tr>
<td>Server-side: full audit trail</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Transparency functionality</td>
<td>Objective in Privacy-Enhancing IDM</td>
<td>Security functionality</td>
</tr>
<tr>
<td>----------------------------</td>
<td>-----------------------------------</td>
<td>------------------------</td>
</tr>
<tr>
<td>Various pseudonyms and private credentials</td>
<td>Protection against unauthorized linkage</td>
<td>Prevent misuse, enable authorized singularized linkage</td>
</tr>
<tr>
<td>Anonymous communication infrastructure</td>
<td>Protection against unauthorized identification</td>
<td>Enable authorized singularized identification</td>
</tr>
<tr>
<td>Policies</td>
<td>Make clear conditions for data processing</td>
<td>Ditto; e.g., information on jurisdiction</td>
</tr>
<tr>
<td>Support to exercise privacy rights</td>
<td>Empower users, establish contacts to DPA / consumer protection</td>
<td>Extension to “security bodies” possible: defined processes for access, better acceptance</td>
</tr>
<tr>
<td>Security feed</td>
<td>Inform people concerned on breaches</td>
<td>Use channel for communication to users after surveillance</td>
</tr>
<tr>
<td>Server-side: full audit trail</td>
<td>Auditability, transparency on data quality, possibility to find errors and correct them</td>
<td></td>
</tr>
</tbody>
</table>
Melange of security objectives

- Prevention of misuse beforehand
  - Better authentication against identity theft
  - Know the degree of accuracy & completeness of data and their sources

- Protection of non-criminals (also against espionage)
  AND catching criminals
  - Support self-protection
  - Avoid mass surveillance
  - Keep data in own jurisdiction

- Acceptance of society
  - Beware of criminalizing privacy-aware behavior
  - Provide transparency and checkability of law enforcement whenever possible

For individuals
For employees
For companies

PRIVACY ≦ TRADE SECRETS
What privacy-enhancing identity management cannot prevent

• Monitoring of people outside the scope of identity management
  – Biometric sensors
  – Video surveillance
  – RFID

• Collecting data voluntarily disclosed by users

• Non-favorable policies
  – But it can make them transparent

• Security breaches
  – But it can interpret information on security breaches
Further information on PRIME

Closing Event:
21 July, 2008 in Leuven, Belgium

https://www.prime-project.eu/

Holistic approach:
• Legal, social & economic framework
• Architecture
• Prototype implementation of architecture & user interface
• Application demonstrators (Collaborative eLearning, LBS)
• Tutorials (general public, end-users, experts)
• Research in all areas
Launched in March 2008: PrimeLife!

10 Million € FP7 Project
Duration: March 2008 – Feb 2011

Objectives:

• Fundamentally understanding privacy-enhancing identity management “for life”
• Bringing privacy to the future web
• Making tools for privacy-enhancing identity management widely available – privacy live!

http://www.primelife.eu/