Location Privacy by Design
- Technology & Business Incentives

Dr. Lothar Fritsch

Norsk Regnesentral
Norwegian Computing Center

Oslo

Internetdargana, Stockholm, 26-27.10.2010
**Privacy-enhancing technology**

**Plats:** Kongresshall C  
**Datum:** 2010-10-26  
**Tid:** 11:00-12:30

In this seminar, the concept of Privacy-enhancing Technologies (PETs) will be presented and examples for basic PET (Mix-nets, anonymous credentials, privacy policies, privacy-enhanced access control, transparency tools) will be given. We will show how, within the scope of the EU PRIME and PrimeLife projects, state of the art and novel PETs have been integrated into a privacy-enhancing identity management architecture, which allows end users to gain better control over their personal spheres.

**Talare:**  
Simone Fischer Hübner, Forskare Läs mer  
Hans Hedbom Läs mer  
Lothar Fritsch, Research Scientist Läs mer
Contents

► Location Privacy
  ▪ Concepts
  ▪ Technology

► Privacy by Design
  ▪ Planning vs. Patching
  ▪ Design Process

► Business Incentives for Privacy
  ▪ Customer damage is business damage
  ▪ Businesses want privacy, too!
Simple change of pseudonym?
Use of Anonymizers / MIXing / TOR?

[1]
Cloaking in Time and Space

[1]
MIX zoning of users
Dummy Users as Camouflage
Two particular solutions

► PRIME LBS prototype for T-Mobile [2]
  ▪ Using a 3rd-party service to separate location data from identity data
  ▪ Creation of 3rd-party LBS supplier IDs
  ▪ Management of user location policies at the location source

► ”Oblivious maps” – anonymous access to mapping [3]
  ▪ Based on ”oblivious transfer” algorithm
  ▪ Basically bundels many user’s access to a mapping service into a batch
  ▪ Cryptographic properties ensure that the mapping server can’t profile users
PRIME: Real-World Reseller Business

- Large number of connected partners
- Content & application providers
- Aggregators / Reseller
  - Brunet (SMS)
  - C3S (SMS)
  - T-Motion (WAP, SMS)
  - Jamba (WAP)
  - ??
  - ??

Individual enabling products / services
- Enabling Product
- Location
- Enabling Product
PRIME: Requirements

► Enable established business models on a secure, privacy-friendly architecture
► Ensure efficiency & economy of the solution
► Enable users to manage policies & their ‘online’ identities for each service provider and for each usage cycle
► No processing of localizations violates a user’s consent
► Hide service usage patterns from observers & infrastructure providers
► Confidentiality of communication content against observers & infrastructure
PRIME: LBS privacy architecture

LBS Client

U
LBS_C
IDM

LBS Server

L
LBS_S
IDM

sub-profile, payment matching result

Location Matcher

I
LM
IDM

request location, payment location of U

Location Source

O
LS
IDM

Identity Management System

Policy negotiation, consent personal settings, payment notification

Policy negotiation consent
Oblivious Maps

► Based on "tiling" of the map structure
► Bundling of requests to tiles through cryptographic methods
► Mapping server always sends a batch of tiles to a number of users through an "Oblivious transfer" protocol that hides tile receivers
Contents

► Location Privacy
  ▪ Concepts
  ▪ Technology

► Privacy by Design
  ▪ Planning vs. Patching
  ▪ Design Process

► Business Incentives for Privacy
  ▪ Customer damage is business damage
  ▪ Businesses want privacy, too!
Cost of software maintenance:
- cheapest early in development
- Privacy & Identity Management are expensive to change!

Privacy by Design provides cheaper results
Privacy by Design

1. Identification of Stakeholders
   - What is the IS about?
   - What is the business purpose?
   - Who is involved?
   - What are the roles?
   - How is the interaction taking place?

2. Requirements Using Boundary Object
   - What is the common vocabulary?
   - Where is the equilibrium of interests and concepts?
   - What are contradictions or conflicts?

3. Hi-Level Specification
   - What is the IS main function?
   - Which transactions are performed?
   - What data is processed?
   - What do the workflows look like?
   - Does it keep the budget?

4. Multilateral Security Analysis
   - How are each stakeholder’s interests considered?
   - What measures are necessary to enforce them?
   - Are there conflicts?

5. Security Detail Specification
   - What does the overall security architecture look like?
   - Which security primitives and policies are needed?
   - What security management measures are necessary?
Find a stakeholder consensus!
Contents

► Location Privacy
  ▪ Concepts
  ▪ Technology

► Privacy by Design
  ▪ Planning vs. Patching
  ▪ Design Process

► Business Incentives for Privacy
  ▪ Customer damage is business damage
  ▪ Businesses want privacy, too!
Privacy Protection in IT

Privacy Protection

Collect, Store, Process, Transfer, Delete

Flow of Personal Data

Identify, Authenticate, Link person, give right express ownership

Identity Management
Privacy
Relevance

- Reputation
- Branding loss
- Customer loss
- Competitive loss
- Business loss
Privacy Relevance

Legal Compliance

Fines

Exclusion from tender

Legal processing

Reputation

Branding loss

Customer loss

Competitive loss

Business loss

[6]
Privacy Relevance

- Management Cost
- TCO
- Risk Management
- Training
- Legal Compliance
- Fines
- Exclusion from tender
- Legal processing
- Business loss
- Customer loss
- Competitive loss
- Branding loss
- Reputations
- Customer loss
- Business loss
Duality of Privacy Risks

Personal Information Problem

System

Business risks
- Reputation
  - loss of image
  - loss of branding
  - loss of trust
  - higher expense in marketing
- Compliance
  - fines
  - loss of license
  - prosecution
  - exclusion from govmt. business
  - higher legal expense
- Lost Opportunity
  - Exclusion from international opportunities
  - Lose customers - to competition
  - Not get new customers
  - Higher cost of acquisition

User risks
- Self-Determination
  - loss of reputation
  - loss of diversity
  - SPAM and price discrimination
  - higher efforts to keep control
- Intransparency
  - confusion on what others know
  - uncertain future dangers of loss
  - loss of trust
dossier society
- Health & Freedom
  - personal dangers
  - totalitarianism
  - stalking
  - intrusion

Lost Opportunity
- Exclusion from international opportunities
- Not get new customers
- Higher cost of acquisition

Compliance
- Exclusion from international opportunities
- Prosecution
- Exclusion from govmt. business
- Higher legal expense

Self-Determination
- Loss of reputation
- Loss of diversity
- SPAM and price discrimination
- Higher efforts to keep control

Intransparency
- Confusion on what others know
- Uncertain future dangers of loss
- Loss of trust
dossier society

Health & Freedom
- Personal dangers
- Totalitarianism
- Stalking
- Intrusion

[6]
Businesses need privacy, too.

► Or... bad things might happen anytime soon...
The Boycott Phone

Boycott FLATFISK ASA!

Boycott all farmed salmon!

Get 2 for the price of 1 at FJORDFISK!

3G data connection

Web community

Supermarket cart

[5]
RFID future uses – the two-edged sword

Imagine a world where...

- A vendor’s trash (packages, products) will be tracked around the globe, even 20 years after production, until it turns up on a polluted site in Africa – and on some NGO’s agenda;

- The city trash removal facilities read RFIDs on package waste to bill the producers for the trash processed;

- Corporate tax & toll is adjusted based on scanners at borders, ware houses and waste dumps.

- Does the ”kill” function kill TID tag serial numbers?
Privacy by Design Instruments

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Legal frame</td>
<td>Threats to privacy</td>
<td>Catalog of protection</td>
<td>Model of cost, Effectiveness</td>
<td>Business process model</td>
</tr>
<tr>
<td>Technical frame</td>
<td>Threat impact model</td>
<td>PET catalog</td>
<td>and efficiency of privacy training</td>
<td>Life cycle</td>
</tr>
<tr>
<td>User requirements</td>
<td>Impact analysis</td>
<td>Insurance coverage</td>
<td>Abstraction of PET into function,</td>
<td>Best practices</td>
</tr>
<tr>
<td>Business Models</td>
<td></td>
<td>Hope &amp; Pray</td>
<td>price and QoS</td>
<td>Assurance</td>
</tr>
</tbody>
</table>

What is the system about?  
Where are the problems?  
What can be done?  
What can we afford?  
How will it be put in place?
Further reading


Contact

Lothar Fritschi

forsker · research scientist
DART · department of applied research in information technology

dir. phone: (+47) 22 85 26 03
mob. phone: (+47) 968 85 758
Lothar.Fritschi@nr.no

Norsk Regnesentral · Norwegian Computing Center
Gaustadalléen 23, P.O. Box 114, Blindern
NO-0314 Oslo, Norway
www.nr.no · nr@nr.no

phone: (+47) 22 85 25 00
fax: (+47) 22 69 76 60