Marit Hansen heads the Privacy Enhancing Technologies (PETs) Division at Unabhängiges Landeszentrum für Datenschutz in Germany. She discusses the methods of bolstering both security and privacy online used in the PRIME project (Privacy and Identity Management for Europe)

Me, Myself and I! Manage your IDs safely

Managing our personal identity

has become a serious issue as we enter our credentials online and into various databases, to be made available for reference by organisations.

Managing the amount of information you want to disclose to one party is something that has become increasingly important in terms of personal security, partly because organisations are now highly networked when it comes to information. We disclose scraps of our ID to different organisations with the belief that small amounts of information cannot reveal enough about us to impact on us in a negative way but when using the internet extensively we can give away lots more information about ourselves than we may care to admit.

It is possible to build a complete picture of someone's movements, transactions, whereabouts and relationships from the trail left from interaction with websites.

It's because of this that we have to plan to guard against identity abuse.

How did John get burgled?

Let's look at a real-life example of how this sort of identity trail can make an innocent individual (in this case a man called John) the victim of a serious crime:

Returning from vacation, John finds his house burgled. Who could have known that he was not at home for some days? Together with a trustworthy consultant, he reconstructs his online tracks from the time before the burglary. Linking the data John has disclosed in different situations, it becomes clear how the facts necessary for the burglary could have been gathered.

This story is told in the PRIME introductory movie which illustrates crucial privacy issues on the internet and shows two basic rules explaining how people can protect themselves in the online world:

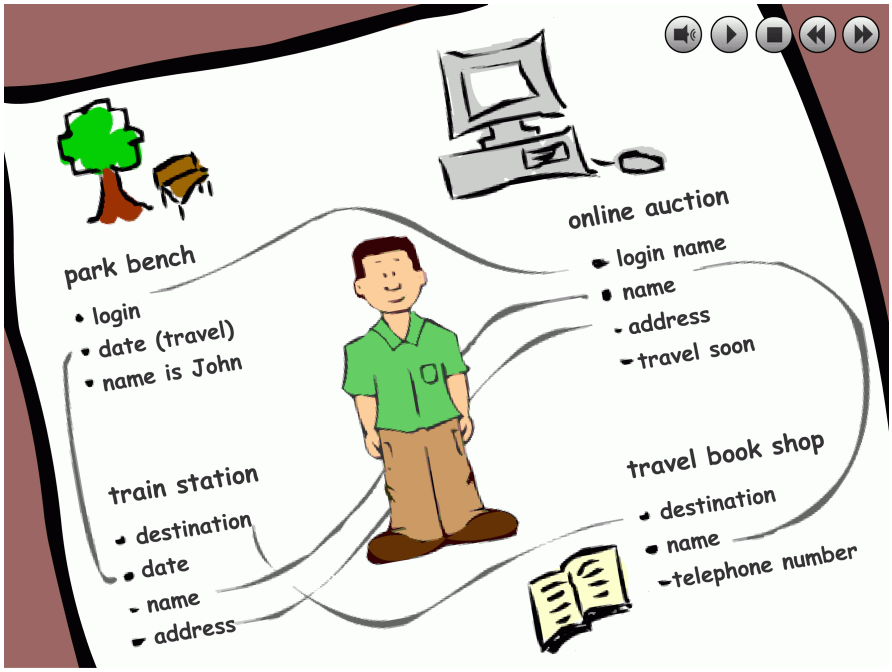
1. Separating contexts so that observers cannot accumulate sensitive data

2. Being cautious when personal data are requested and keeping track of information disclosure

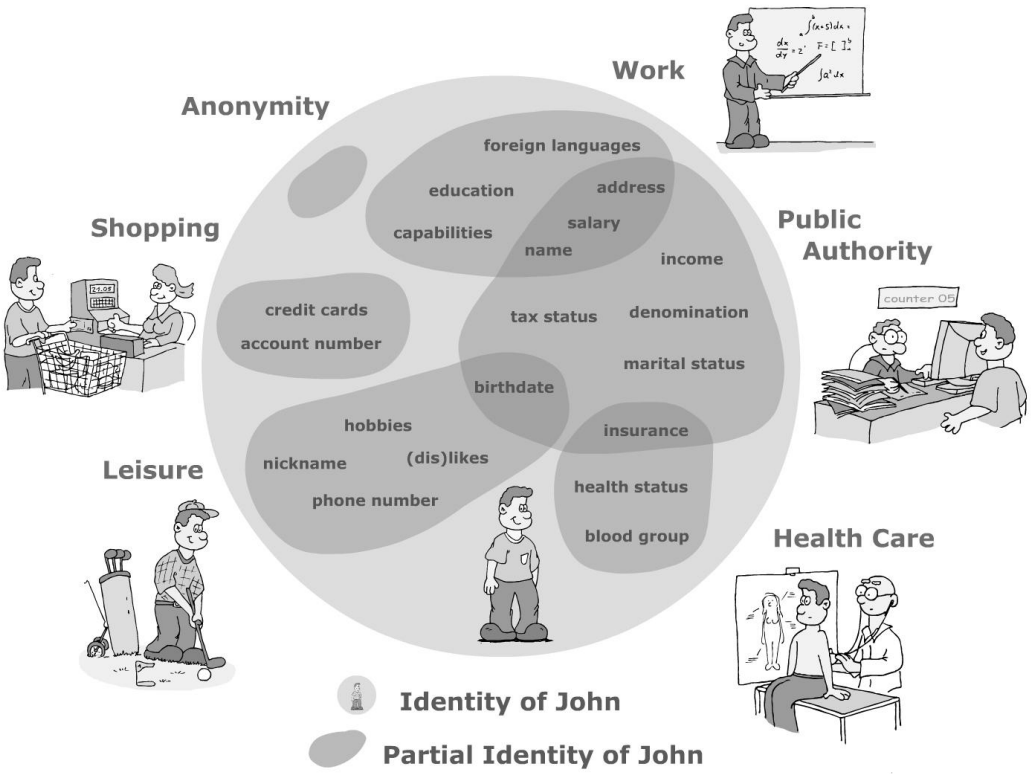
These rules are the main features of the concepts and prototypes developed within the PRIME project. Since 2004, 20 partners from industry, academia and data protection have been working in the four year PRIME project on privacy and identity management. PRIME aims to demonstrate viable solutions to privacy enhancing identity management by delivering a reference framework, requirements, an architecture, design guidelines, protocols and prototype implementations that are evaluated from a multidisciplinary perspective.

People are used to intuitively deciding what to tell whom according to the specific situation – this is already a form of identity management. For example data required in professional life are different from what is needed in private life, and in a book store other data are relevant than in the sports club. Nobody gets to know the complete identity of a person – instead, only specific partial identities can be perceived.

The identity of a person comprises many partial identities of which each represents



Linking John's data



An individual's partial identities

the person in a specific context or role. Identity management means choosing and developing appropriate partial identities with respect to the current application needs. User-controlled identity management systems enable the users to handle the plurality of their accounts and passwords.

The guiding principle is to put individuals in control of their personal data, based on three main components:

Pseudonyms and private credentials – combining accountability and privacy

Not always the real name of the user is required. Instead, different pseudonyms could be used to prevent undesired context-spanning linkage and profiling by other parties. Organisations can support this by clever design of their workflows, separating different tasks – and the corresponding databases – from each other.

As a specialty, PRIME's approach uses 'private credentials' which enable proving one's authorisation (e.g., to be over 18 years old) without revealing information that may identify the individual. These private credentials are derived from certificates issued on different pseudonyms of the same person. Multiple private credentials can be created from a single certificate that are neither linkable to each other nor to the issuance interaction in which the master certificate was obtained. Private credentials provide accountability while protecting the anonymity of the user as long as there is no misuse – in this case the user's anonymity can be revoked.

Enforcing privacy policies – both before and after

For organisations, showing a privacy policy on a website is nothing new. But providing privacy policies which are really understood by users and at the same time serve as rules for the automated data processing within the organisation is a challenge tackled by the PRIME project. Its work encompasses both 'before' and 'after': the provision of privacy policies before a transaction takes place, e.g., in a stage when the user has to give consent to data processing, and after the transaction when the policy still sticks to the data disclosed. These 'sticky policies' enforce the rules how the data may be processed even after they have been disclosed and thereby have left the user's area.

The 'Data Track' – transparency of prior transactions

The important question should be 'What do others know about me?' Knowing the reality of this is the prerequisite for the so-called 'informational self-determination'. The 'Data Track' is a history function of all online transactions. In principle it stores

The Commission considers that PETs should be developed and more widely used, in particular where personal data is processed through ICT networks.

PRIME's toolbox containing privacy components and building blocks

when which personal data have been disclosed to whom – and under which conditions. This comprises also the privacy policy of services requesting data. Thus, the 'Data Track' does not only provide transparency for users, but also enables them to ask data controllers later on whether they really treated the data as promised.
In addition, the 'Data Track' helps to use or re-use the appropriate accounts – pseudonymous and passwords – in different contexts, keeping them apart unless otherwise desired.

PRIME toolbox

These overarching concepts and the details of the PRIME toolbox, i.e., single components and building blocks to be used for user-controlled identity management, are explained in the PRIME tutorials and the project's White Paper. Everybody is invited to use them for their own projects.
Compliance to European law is the premise of all PRIME results. The project's concept is in the spirit of the European Commission promoting Privacy Enhancing Technologies (PETs), stating that PRIME is an example of significant IST research projects in this field. The Commission considers that PETs should be developed and more widely used, particularly where personal data goes through ICT networks. The Commission believes wider use of PETs would improve the protection of privacy as well as help fulfil data protection regulations. The use of PETs would complement existing legal framework and enforcement mechanisms.
As a matter of course, PETs – and user-controlled identity management systems such as envisioned in PRIME – need socio-economic backing. Hence, PRIME explores socio-economic incentives, elaborates acceptance factors and investigates potential business models for various players including new services relevant to user-controlled identity management. These players could be identity providers, brokers specialised on fair value exchange, or information services to give feedback to users on trust issues like personal data being handled by dubious controllers.
Furthermore, PRIME partners are active in standardisation concerning identity management, e.g., in ISO, W3C and ITU-T, so that upcoming standards are compliant to privacy enhancing concepts of user-controlled identity management. ★

At a Glance

Project Reference: IST-507591

PRIME's Objective:
PRIME is developing a working prototype of a privacy enhancing Identity Management System. Novel solutions for managing identities will be demonstrated

Project Duration: March 2004-February 2008

Partners: 20 partners from industry, academia, research centres and data protection authorities

Costs: About €13 mn, thereof €10 mn funded

Funding: The PRIME project receives research funding from the European Union's Sixth Framework Programme and the Swiss Federal Office for Education and Science

Contact: Marit Hansen
t: +49-431-988-1214
f: +49-431-988-1223
www.datenschutzzentrum.de

Want More Info?:
The PRIME movie, tutorials, White Paper and various deliverables are available online:
www.prime-project.eu

Marit Hansen

Head of PETs Division
Unabhängiges Landeszentrum für Datenschutz

Marit Hansen received her diploma in 1995 and has since worked extensively on multi-lateral security and privacy. She is actively involved in several European projects on user-controlled identity management and eID systems.

PRIME