PrimeLife – Privacy and Identity Management in Europe for Life

Scramble! your social network data

Social Network Sites …

… such as Facebook, MySpace, Hi5, Netlog are a trendy, popular and useful tool for people to share information. With their fast growth they have conquered society and are increasingly incorporated into people's lives. They offer not only the possibility for users to share information with friends, family, and other contacts; their technological features also allow users to engage in new types of social interaction.

Privacy Threats

At the same time Social Network Sites pose privacy threats as users' information can be easily exposed and shared among other services, from a technological point of view. Because most Social Network Sites store their information centrally, it is hard to control who can access which information. Prying eyes range from the provider himself to more curious and/or malicious users.

Social Network providers supply users with mechanisms to enforce access control, but their model requires trusting the provider who himself might not be trustworthy. In fact, Social Network providers have access to all of the users' information, public and private, and thus can use them for several purposes. In addition, providers collect and structure users' data, which they can use or sell for economic purposes, such as targeted advertisement or behavior analysis. Also, the providers can share and leak to external viewers all users' information and traffic.

Scramble! Requirements

The concept of privacy may have different meanings depending on socio-cultural factors. Whilst the concern of ensuring a certain level of privacy is important, some control over the flow and transmitted data can also be required.

To address the privacy threat of unwanted access to pieces of content disclosed by users, they can be provided with a tool – Scramble! – that allows them to enforce access control over their published data. For each data item, a specific audience can be selected. This is referred to as audience segregation, and can be achieved by means of encryption. Simplicity of the actions and transparency of the cryptographic operations make sure that such a tool is actually usable.

Scramble! Description

Scramble! is a tool that allows not only for the definition of access control rules for audience segregation, but also for the support of their enforcement. It allows users to publish encrypted information and define the set of users that have the ability to decrypt – and therefore view – the published content.

Scramble! users:

Each Scramble! user holds a public/private key pair. The users in the system are represented by their public key, which is used to encrypt data with. These public keys are distributed through any possible means of interaction (e-mail, website, key servers, etc.).

Grouping for segregation:

Within Scramble! groups of users (public keys) can be constructed to define different contexts (friends, family, colleagues, …) in which information can live. For each piece of data the user chooses a set of contacts, constructed from groups and/or single, specific contacts who will have access to the data.

Encryption for access control:

To empower the user to determine who has access to his data, shared over Social Network Sites, Scramble! encrypts the data with a secret key, which is then encrypted with the public keys of the contacts in the intended audience. To get access to the secret key, necessary to decrypt and view the content, a user must possess a private key that corresponds to one of the public keys of the intended audience.

Transparency and easy use:

Scramble! is a Firefox extension, and is independent of the actual setup of Social Network Sites. Once set up with a user's key pair, a suitable set of users and groups, Scramble! will automatically look for content, encrypted with the public key of the user. Such information blocks are parsed, decrypted and represented in the browser without any user interaction. Generating encrypted content is done by selecting the data, clicking one button, and going through a selection dialog to construct the intended audience. Public keys are stored online in an OpenPGP key server, and can be retrieved easily. Finally, users that have no access to the encrypted data will see a suitable message (non-authorized content) while users that do not have the extension installed see a strange-looking but innocent piece of data.

Where to find Scramble!

- http://tinyurl.com/scrambleit
- http://www.primelife.eu/results/opensource/65-scramble

Scramble!

> *"Scramble your social network data!" - With Scramble! you can selectively enforce your access control preferences for your content on Social Networks like Facebook or Twitter!*

PrimeLife at a glance

Project reference:

216483

PrimeLife's objective:

Bring sustainable privacy and identity management to the web and develop tools for privacy-friendly identity management

Project duration:

March 2008 - June 2011

Partners:

15 partners from industry, academia, research centres and data protection authorities

Total cost:

About € 15.5 Million

Total EC funding:

€ 10.2 Million

Funding:

The PrimeLife project receives research funding from the European Union's 7th Framework Programme.

Contact:

Marit Hansen

t:+49-431-988-1214
f:+49-431-988-1223
primelife@datenschutzzentrum.de

Date of publication of this Primer:

January 2011

Want more info?

Various deliverables are available online:
http://www.primelife.eu/

PrimeLife