Digital Single Market

Projects news and results02/11/2011

Scientists teach discretion to gossipy web

Internet surfers are obliged to reveal more and more personal data to get the best out of the latest web services and sites. How this information is then used or shared is a big question hanging over the Future Internet. Now EU-funded scientists have developed technology for both end-users and businesses that could teach the web some discretion and revolutionise online privacy and identity management along the way.

[1]

Privacy and security issues go hand-in-hand and serious data breaches are on the rise. In April this year, a leading consumer electronics manufacturer suffered a massive breach which led to the theft of over 100 million user account files. The files contained names, addresses and credit card data.

In the US, a well-known hospital posted data for 20,000 emergency room patients on its publicly accessible website, while in the UK newspaper reporters hacked the mobile phones of the Royal Family, UK celebrities and the victims of high profile crimes.

Unsurprisingly concerns about private data and identity (ID) theft are growing in this uncertain online environment.

'People want to protect their privacy and retain control over personal information, whatever their activities,' explains Dieter Sommer, coordinator of the 'Privacy and identity management in Europe for life' [2] (PrimeLife) project. 'But information technologies hardly consider those requirements, thereby putting the privacy of the citizen at risk.'

That has always been the case with various traditional services over the web, but now the increasingly collaborative character of the internet means that users contribute more and more personal information, notes Mr Sommer. 'Individuals contribute throughout their life, leaving a life-long trail of personal data.'

This data trail raises significant challenges that PrimeLife sought to address. The three-year project gathered together 14 of the continent's leading companies and research institutions involved in the privacy field and a US-based partner.

PrimeLife follows on from the work of the project 'Privacy and identity management in Europe' [3] (PRIME). 'Prime focused on data minimisation, so that the minimum absolute required data was exchanged to complete transactions,' explains Mr Sommer. 'In PrimeLife we developed a much broader perspective. One aspect ... was to take the work of the PRIME project forward, but we tackled a number of other topics too.'

The PrimeLife vision is to provide privacy, trust and ID management through tools such as browser plug-ins, social networks and encryption, but that is a huge challenge. People exchange 'Personally identifiable information' (PII) far more often, whether it is signing up for services like news bulletins or road toll payments, engaging in social networks, or through eGovernment and eCommerce.

And the information society landscape is constantly changing, with new business models and new service delivery platforms multiplying the instances of information exchange. It is almost impossible for users to keep track of what information goes where. PrimeLife launched a series of research strands to assess the nature of the problem, develop robust solutions and formalise concrete methods for deploying these new technologies.

The first activity looked at what life-long privacy means, developing and evaluating user scenarios. With use cases established, the project started to develop mechanisms in another strand of research. A key activity looked at policies, arguably one of the most effective ways to give people control of their privacy. A policy could demand, for example, that personal data used for a service must not be used for direct marketing, or can only be used by specified parties.

Confusion and clunkiness

Usability was another PrimeLife focus. Users rarely read the small print and the current confusion and clunkiness surrounding privacy interfaces and control is one of the main reasons why users often remain unprotected.

PrimeLife also researched and developed infrastructures, such as policy-driven privacy protection in services and secure mobile devices, and they looked at economic considerations as part of this aspect of their research.

Throughout their work, the project team pursued a parallel activity for all their research that they called 'Privacy Live'. Privacy Live was an on-going effort to get their research out to the wider community working in privacy issues through standards work, dissemination, cooperation and the release of open source software.

Major outputs included tools for privacy made available to social network communities, and some highly successful basic research in credential systems, cryptography in general, and other key areas of privacy. Allied to this were a substantial number of open source tools designed to handle all aspects of the privacy problem.

For example, PrimeLife developed its own social network, called Clique, that lets users keep control of their privacy through audience segregation - one audience might be friends, another could be colleagues - thereby automatically limiting information like a user name or profile photo to designated audiences.

The project also developed Scramble, a web browser plug-in which lets users encrypt their data so they can enforce access control on social networking sites. Another interesting technology is Identity Mixer, which lets users authenticate themselves without revealing their identity - users can prove they are trustworthy without revealing who they are. It would mean that consumer websites, for instance, would not need all the sensitive data that they have today in order to provide services, eliminating the risk of data loss.

The policy work, too, could revolutionise privacy for complex 'composed services'. For example, when a discount coupon service combines with a retailer to target special offers, identity or location information might be exchanged. But PrimeLife's approach would allow a user to control which information is going to which of those services. That is just one very simple example, but the tools developed by PrimeLife could handle immensely complex service composition as well.

PrimeLife tools could also make advanced privacy services available to companies. For example, when a biotech company does research based on information from a third-party DNA database, it wants to access the information but it does not want the service provider to know or record what information it accessed as this may be linked to confidential research or patient information.

To do this right now, companies must lease a local copy of the entire database, which is not only expensive but also problematic from a security perspective due to the value of the database asset. Using advanced cryptographic technology developed by PrimeLife, however, biotech clients could access the database and pay for the service but preserve anonymity about who they are or what they studied. Results like this only touch on PrimeLife's output.

Coordinated by IBM Research in Zurich, Switzerland, PrimeLife also consisted of Germany's SAP, Microsoft Innovation Centre, Technische Universität Dresden, Unabhängiges Landeszentrum für Datenschutz, Giesecke & Devrient, and Goethe Universität Frankfurt, Karlstads Universitet in Sweden, Universita degli Studi di Milano, and Universita degli Studi di Bergamo in Italy, Tilburg University in the Netherlands, Katholieke Universiteit Leuven in Belgium, Austria's Centre for Usability Research & Engineering and Brown University in the US.

Significantly, the World Wide Web Consortium (WC3), the leading standards body for web technologies, also participated in the project through its European site located in France.

PrimeLife completed the EU-funded aspect of the research in June 2011, and many of the consortium members are continuing this work in one form or another. A new project, https://abc4trust.eu/ (ABC4Trust), pilots the two major anonymous credential systems currently available, one of them being IBM's Identity Mixer technology that has been researched in PrimeLife.

Another project, FIware [4], a European platform for the Future Internet, will integrate credential technology as part of the security within the platform. Altogether, PrimeLife has made major advances and developed technologies that could soon be deployed to better protect users' privacy on the internet.

PrimeLife received EUR 10.2 million (of EUR 14.93 million total budget) in EU funding under the Seventh Framework Programme, sub-programme 'Secure, dependable and trusted infrastructures'.

- Privacy and identity management in Europe for life project [2]
- PrimeLife project data record on CORDIS [5]
- Prime project data record on CORDIS [3]
- ABC4Trust - Attribute-based credentials for trust [6]
- FIware - Future Internet core platform [4]

- Putting privacy at the heart of biometric systems [7]
- A matter of trust: privacy and security issues in the Information Age [8]
- Me and my files [9]
- What is the identity of identity in the digital age? [10]
- Electronic ID becoming a reality in the EU [11]

- Country: SWITZERLAND
- Information Source: Dieter Sommer, PrimeLife project coordinator
- Date: 2011-11-02
- Offer ID: 7208

Share this page

Links
[1] https://ec.europa.eu/digital-single-market/sites/digital-agenda/files/newsroom/offer_id_7208_3250.jpg
[2] http://www.primelife.eu/
[3] http://cordis.europa.eu/fetch?CALLER=PROJ_ICT&ACTION=D&RCN=71383
[4] http://www.fi-ware.eu/
[5] http://cordis.europa.eu/fetch?CALLER=PROJ_ICT&ACTION=D&RCN=85453
[6] http://abc4trust.eu/
[7] http://cordis.europa.eu/fetch?CALLER=OFFR_TM_EN&ACTION=D&RCN=6916
[8] http://cordis.europa.eu/ictresults/index.cfm?section=news&tpl=article&BrowsingType=Features&ID=70244
[9] http://cordis.europa.eu/ictresults/index.cfm?section=news&tpl=article&BrowsingType=Features&ID=91255
[10] http://cordis.europa.eu/ictresults/index.cfm?section=news&tpl=article&BrowsingType=Features&ID=91163
[11] http://cordis.europa.eu/fetch?CALLER=EN_NEWS&ACTION=D&RCN=33736