Trust and Privacy Management in MobiLife - on the Difficulty of Giving Control to the User

Markus Miettinen
Nokia Research Center
P.O.Box 407, FI-00045 NOKIA GROUP
Itämerenkatu 11-13, FI-00180, Helsinki, Finland

May 16, 2007

1 The MobiLife Project

The integrated project MobiLife was part of the European Union's Information Society Technologies arm of the sixth framework programme for research[mob07]. The project's goal was to bring advances in mobile applications and services within the reach of users in their everyday life by innovating and deploying new applications and services based on the evolving capabilities of the 3G systems and beyond.

The project was run by a consortium of 22 partners from nine different countries in Europe. The consortium partners included several telecommunications device vendors, network operators, universities and research institutes.

In this talk, we present the privacy and trust framework which was developed for the MobiLife application architecture and discuss some of the findings that were identified during the course of the project. We also present some of the privacy management-related research problems remaining and provide useful pointers to the results of the project [Kle07].

2 The MobiLife Privacy and Trust Framework

The basic notion adopted in the privacy and trust work of the project was that the user must be in control of all privacy decisions related to her data. This means that in order for the user to build a sense of trust to the system she must have the certainty that none of her private data are released to unauthorised parties without the user's consent. In the MobiLife framework this means that all access to user data are controlled by using user-specified privacy policies, which mandate what user data items may be shared with whom and under which conditions.

The privacy control on user data is realised by the use of so-called Trust Engines. Trust Engines are access control components, which have two roles in the MobiLife framework. On one hand the Trust Engines may act as privacy decision points (PDPs), i.e. components which the user can use to specify, store and modify her privacy preferences in the system. The privacy policies specified by the user are then replicated to other Trust Engines in the system, which hold custody of data items beloning to

the user. These Trust Engines act as privacy enforcement points (PEPs) evaluating access requests to user data which are located on their local data repositories, so-called Context Providers (CPs).

We will also discuss, how the notion of trust is handled in the MobiLife framework. The basic idea from which trust is derived in the MobiLife framework is the concept of a so-called Trust Seed. The Trust Seed is a unique cryptographic key, which uniquely identifies a MobiLife system comprising of a user and her devices. The key is created and associated with the user when a MobiLife system is bootstrapped and it acts as a seed on which all user trust is built. The Trust Seed is used to derive secondary cryptographic keys and it can be used to verify the identity and authenticity of privacy policies specified.

3 Visualisation of User Choices

During the course of the project also issues regarding the usability of the privacy management functionalities were addressed. It turned out that solving the somewhat contradictory goals of providing full and fine-grained control of privacy decisions to the user while at the same time making the system easy and convenient to use is a very challenging task. This is due to the fact that full control of privacy preferences inherently introduces also a considerable amount of complexity to the system which is not easy to communicate to the user in an understandable manner.

One example of a management challenge is the handling of privacy preferences for groups of users. Groups can be used to reduce the number of individual security associations that have to be managed but on the other hand they introduce the need for managing the membership of individual users. It is also not a straightforward task to model real-world trust relationships of persons through groups in a way that is flexible but does not introduce too much group management overhead.

In addition to the above-mentioned problems, the challenges represented by the typically small sizes of mobile devices' user interfaces makes solving the privacy management problem even more demanding. We will, however, give an overview on the approaches taken in the project to address the problem of user control through the use of different visualisation solutions and discuss problems that still remain to be solved.

References

[Kle07] Mika Klemettinen, editor. *Enabling Technologies for Mobile Services: the MobiLife Book*. ISBN 978-0-470-51290-6. Wiley, September 2007. To appear. See e.g. `http://eu.wiley.com/WileyCDA/WileyTitle/productCd-0470512903.html`.

[mob07] Mobilife website. `http://www.ist-mobilife.org/`, 2007. [last accessed 10 May 2007].