Identity Management in Social Networks

Miguel-Ángel Monjas, David Suárez
{miguel-angel.monjas, david.suarez.fuentes}@ericsson.com
Technology and Innovation Unit, Madrid R&D Center
Ericsson[1]

Position Paper for W3C Workshop on the Future of Social Networking

As the user takes a more active role in the production of contents and even services, and becomes a "prosumer", this situation leads to a somehow chaotic scenario where a same user is present in an uncountable number of different platforms, taking best-of-breed for any aspect of his/her social interaction or simply following the hype or, better, joining their friends, activating his/her presence in the social networks where most of their friends are already present. This situation creates an increasingly inconvenient and uncomfortable situation where users not only own different accounts, each one with a specific set of credentials, but also an increasing amount of personal information scattered through several sites, each with different data usage policies and privacy protection conditions.

Ericsson believes that the user experience in social networks must be improved following some basic principles:

- Enhancing the user **security** without compromising the usability. In that sense, the take-off of the mobile Internet, with users always carrying a personal device (in a way that only was equaled previously by keys or watches), the mobile phone, equipped with an xSIM card, leads to a natural consequence: taking advantage of authentication mechanisms supported by the xSIM card, such as two-factor authentication with SMS interaction with the user or 3GPP GAA/GBA mechanisms. An interesting development is that with new mobile technologies such as 3G or LTE, SIM cards are propagating to laptops. Therefore, the number of SIM-equipped devices the users own increases, thus opening the way to implementing security functionalities based on such kind of authentication techniques, some of them also allowing key distribution. Additionally, user location can be used as an extra authentication factor when considering user security technologies based on the SIM card.

[1] This work has been partially supported by CDTI, Ministry of Science and Innovation of Spain, as part of the SEGUR@ project (https://www.cenitsegura.es/), within the CENIT program, with reference CENIT-2007 2004.

- Giving the user the tools for appropriately handling his/her **data**. The user should be able not only of transferring his/her data between social network sites (something that emerging specification such as DataPortability are aiming to) but also to set the sharing and privacy conditions of his/her data, generated content and applications, networks of friends and professional contacts, and even delete them, as fine-grained as wished. As such, the user should be given tools to effectively control his "identity map" regardless of the place where any piece of it is actually stored. Such requirements may only be met if the user is been given sort of virtual single access point(s) to his/her identity map, not only in social network sites but also in network providers (operators), ISPs, payment providers, GAMEYs and any other site where a digital fingerprint of the user is present. The user should be as well able to trace the use of its identity information, both in terms of knowing "who" uses them and "how" it is being used.

- Enhancing the user experience through a better understanding of the user needs, likings and behavior. The user profile can be enriched by adding **inferred** attributes like the user's communities, explicit or implicit, she/he belongs to or the features or such communities. It leads to unquestionable benefits to the user (not only as a means to help the user to choice among the increasing offer of services and contents, but also as automated personalization, security or usability recommendations). That inferred **user knowledge** can be automatically created and updated by using **machine learning** techniques. Ericsson wishes to promote the standardization of the exchange format for social network information, beyond current de facto standards, thus covering that kind of inferred information.

Ericsson sees a positive industry trend and therefore actively participates in the development of so-called federated identity systems (such as openID and DataPortability in the social area, SAML and LAP ID-WSF in the enterprise area, GSMA Access API in the telco area) as identity provider entities able to federate different online actors that can render many of the intended benefits already mentioned. This Identity Provider concept could be seen as an extension of the **broker** concept that Ericsson is actively playing already in the telco market: an entity that handles m to n relationships thus hiding the complexity of such relationships to its clients, showing only a single entity instead of n.

Such "identity" brokers, providing services directly to users, and behaving as a broker towards social network sites, networks operators and whatever other entity hosting user information may help to fulfill the aforementioned requirements. These entities should provide as many as needed of the following features:

- **xSIM-based authentication** regardless of the network operator giving service to the user. For instance, 3GPP GAA/GBA and SMS-based OTP. Such authentication mechanisms should be available to any site by means of different protocols such as openID, SAML and so on.
- Other **strong authentication** mechanisms not under the control of network operators. For instance WPKI and electronic (smart card-based) identity documents.
- **User location** regardless of the network operator giving service to the user. User location should be also available as an enhancement of user authentication (thus allowing that authentication is only valid if the user being authenticated is in a given location or nearby). The emerging GSMA Access API by GSM Association should be used in the relationship with network operators.

- **Anonymous assertions** about location or any kind of demographic information (such as gender or age). For instance, it would enable anonymous access to social network sites but only when fulfilling certain conditions (an obvious use case can be child protection). The source of this information may be a network operator or a digital certificate used in electronic identity documents. Liberty Alliance ID-WSF and Windows CardSpace/Higgins might be suitable specifications for the handling of such information.
- Distribution of user information obtained with machine learning techniques both in the Identity Broker and in other entities connected to it between the different actors, meeting user privacy settings.
- Ability to **infer the user's implicit social networks** automatically by analyzing the user's communication patterns.
- The means to enhance the user profile by adding inferred **user knowledge** extracted from the usage of network and services.
- Providing **virtual single access points to user data**, to the user convenience, providing the means for setting privacy restrictions in the sites where the information is available, cancelling user information, handling address books and so on, regardless of where the information is stored.
- Ability to **trace the use of identity information** across service providers, so determining who / to do what (or said to) with identity information.