-- SOCIETIES Positions on Federated Social Networking --

Submitted by:
João Miguel Gonçalves <joao-m-goncalves@ptinovacao.pt>
Elizabeth Papadopoulou <E.Papadopoulou@hw.ac.uk>
Nick Taylor <N.K.Taylor@hw.ac.uk>
Miquel Martin <miquel.martin@neclab.eu>

== Introduction ==

SOCIETIES is an European project with a consortium of 16 partners, that started in October 2010 and will finish in March 2014. We are the largest integrated project out of the fifth call for project submissions for FP7. The project is managed by the Waterford Institute of Technology / Telecommunications Software and Systems Group (TSSG), in the person of Kevin Doolin. The full partner list is available at [1].

SOCIETIES aims to bring together social and pervasive computing into one integrating platform. The proliferation of user owned networked devices has untapped potential that can be capitalized by allowing device capabilities to be offered on the network as services, information and resources. These devices would together form a Cooperative Smart Space (CSS), a digital representation of a user or organisation, enabling the sharing of user-owned services, information and resources. CSSs constitute the users' bridge between the physical world and the digital social communities the user is a part of. A community is a collection of CSSs and/or supporting infrastructure services, who wish to collaborate for mutual agreed purpose for which the community formed. The community's digital representation is called a Community Interaction Space (CIS), through which users can access and make available services, information and resources. Figure available at [2] shows five CSSs, each of which represents an individual, that have formed themselves into four communities.

These services, information and resources would be accessible on top of a trust-enabled identity layer, designed with strong privacy concerns. An open federation of identity domains would be in place where anyone can create his domain. Each identity domain would manage its trust relationships with other domains, assuming some responsibility in the protection of its users from using unsecure or malicious services. On top of this identity web, ad-hoc trust relationships can be then formed, and access control and privacy policies should use them for maximizing automatic control of the user's digital exposition.

== The Role of Devices in Social Networking ==

The migration of social networking services from the desktop to mobile devices brought a new dynamic to the way they were used. Taking advantage of the location systems available on many smart phones was an obvious next step and, privacy issues notwithstanding, automating the process of tagging posts with location information made the process of saying where they are much easier and more attractive to the user. However, location is just one example of context data. The scope for making use of context information is much greater than this and smart phones offer sensing systems which extend well beyond GPS, such as cameras, accelerometers, etc. Furthermore, new devices are appearing all the time which measure a growing range of information about a user such as accelerometers, NFC or even blood-pressure monitors. In the future we can expect the context information which is used to personalise a user's experience and their interactions with their online acquaintances to be much richer than mere location.

The SOCIETIES project is developing a platform which will enable social network users to take advantage of the enormous variety of context sources which will be available to them in the future; not only those provided by the devices which they own and carry around with them but also those provided by other users in their vicinity and by the environments which they encounter such as smart buildings. Social media
have demonstrated very clearly that many people are prepared to sacrifice privacy for the sake of a more personalised and less cumbersome user experience. We believe it is therefore incumbent on system developers to take responsibility for the protection of users' privacy. The SOCIETIES platform will help users to personalise their privacy settings according to their context, disclosing certain information to selected groups in particular contexts but not otherwise. The use of context information to personalise a user's experience can be extended beyond the realms of social media to encompass other services which a user might come across in the smart environments which are likely to become more prevalent in the future. The SOCIETIES platform is being engineered to facilitate this as well. Context awareness to enhance user experience and the ability to make use of personalised services anywhere and at anytime are the defining characteristics of pervasive computing. The aim of the SOCIETIES project is thus to integrate social computing with pervasive computing and deliver a new form of computed mediated community which we call a pervasive community.

Such functionalities, however, are not limited to information exchange, be it directly provided by the user or sensed. A new generation of devices (among them those under the "Internet of Things" mantle) are able to provide modular services that can be shared across Social Networks, providing functionalities such as communication using physical devices around the user's environment (e.g. a rabbit-looking device [3] that reads out your friends status while wriggling its ears, a small display [4] with all you need to know or inconspicuous and hidden screens). Even if the devices are part of the environment instead of user-owned, they are also fertile ground for device actuation scenarios, such as democratically choosing the room temperature and the music at your local bar or sharing access to your WiFi hotspot. If more specific scenarios are considered, applications grow, such as allowing special care home patients to unlock the door for the medical personnel, or enabling heterogeneous rescue teams to share their already scant resources.

In our vision, a member of a pervasive community, aided by the SOCIETIES platform, will be able to extend their social network to form ad hoc communities with people and within smart spaces as they encounter them in the physical world and provide information on their physical environment, physiological and emotional state to their social network, as determined by their privacy preferences. They will also be able to augment their physical world experience by taking advantage of the interaction and communication possibilities of devices and services located in the physical environment. There is no reason why the user's device capabilities shouldn't be shared across social network members, provided that appropriate security mechanisms are built in to prevent abuse and preserve privacy. The possibilities that the use of these devices affords for recreational use, such as real world computer gaming, are perhaps easiest to imagine. However, pervasive communities also offer enormous potential for supporting the disabled or infirm in independent assisted living. Business opportunities, not least in targeted advertising, are also plentiful. Whilst it is possible for the benefits of developments such as the SOCIETIES pervasive community to be integrated with any existing social network, from the user's point of view, the restriction that they can only network with others using the same social network provider at any one time is a major obstacle. In order for pervasive communities to provide the richest user experience it is essential that social networks be federated so that anybody, no matter who their social network provider might be, can join pervasive communities with anybody else.

== Considerations from Identity Management in Social Networking ==

Boyd and Ellison [5] define social network sites as web-based services that allow individuals to
* construct a public or semi-public profile within a bounded system,
* articulate a list of other users with whom they share a connection, and
* view and traverse their list of connections and those made by others within the system.

To a very basic level, a social network is a graph of identities. However, at a point in time where social networks are attempting to become the web's identity layer, it probably is the best time to consider what identity management has to offer in a social network context. Most importantly we need to distinguish between "identity" and "identifier", because identities are much more complex than identifiers. Technically we should say that a social network is a graph of identifiers, since the remaining identity issues have different challenges also targeted in terms of access control and privacy.

These identifiers should be as strong as we want them to be, with the strongest being our name (and Facebook knows this) or national ID card number, and a weaker one being our IP address. If identifiers in a social network would be generated and issued by some trusted party, this would enable the use of pseudonyms. This trusted party is usually called Identity Provider (IdP) in identity management. Identifiers can have different scopes. An identifier may be globally valid (like your passport number) or may only be valid to one or a set of entities (your typical user account for a web site, an OAuth token, ...), or even may even only be valid for the scope of one session. Consequently, identifiers have different lifetimes and the "social connection" between two identifiers obviously is only valid while both identifiers are valid.

The use of pseudonyms in a social networking context is an important step toward a privacy-enabled social layer in the web because they allow the user to control the linkability between his interactions with different people, sites and entities. This unlinkability can obviously be attacked by requesting a number of attributes from the user, identified with a pseudonym, so that the attacker can match it against the other user's pseudonyms. Because of this, it is the responsibility of the system, maybe through the IdP, to intelligently warn about excessive disclosure. As users opt for stronger identifiers when they want people to know them and trust them, or weaker ones for more privacy, the system would be more permissive to such information requests when using stronger identifiers and less when using weaker ones - the strong identifiers inherently provide more linkability so it makes no sense to protect against attacks on it.

While identity domains manage trust relationships with other identity domains, users would also be able to establish trust relations between themselves, also if belonging to different identity domains. How this process should be related to the way connections are established in classic social networks is a matter to be discussed. Social networks generally opt for one type of connection, either directed or undirected. In SOCIETIES, because we are addressing identity at a lower level where entities relate by offering and accessing services, information and resources, we have to consider trust relationships between the providing entity and the consuming entity. They might be used on the provider side for access control and privacy enforcement, and on the consumer side for evaluating security and privacy policies.

--- Policy-based Approaches to Share Data Across Specified Audiences ---

Facet is a social networking concept [7] that we interpret in the SOCIETIES universe as the user's portrayal in a community. In SOCIETIES, users are able to present different facets of themselves in different communities and under different contexts. Multiple identities can be used to join different communities so that certain characteristics of their profile are not associated with others such as personal information and professional information. However, using different facets of the same identity, users can join different communities but filter the information and resources which they share with each of these communities. The CIS is a dynamic entity shaped from the information, services and resources shared by its members as they join and leave the
CIS. The information, services and resources can be accessed only by members of the CIS. A CIS imposes a set of terms and conditions on every CSS that joins the community. These terms and conditions are set and managed by the administrating CSS. However, in order to consume services provided by other CIS members, the participating members in the transaction have to agree to certain terms and conditions between each other. The SOCIETIES platform provides mechanisms to negotiate these terms and conditions using privacy policies to describe them and provides access control mechanisms to enforce them.

The user(s) that administer the CIS state the conditions for joining the CIS, as well as a privacy policy. This privacy policy shall be as simple as possible, since the complexity of both understanding and configuring it is one of the current problems in SNs [8]. We aim to achieve this by implementing Privacy by Design [9] and possibly by considering concepts that help to communicate the implications of policy options [10]. These privacy policies govern the use of data shared by CIS members and how these can be processed inside and outside the CIS. All members of a CIS must abide by these terms and conditions. A CIS member selects one of their identities with which they will be represented to the CIS and configures a facet of the identity to filter out any information associated with the selected identity that they are not willing to share with this specific CIS. This allows a user to join a fan club CIS with a personal identity (as opposed to a professional identity) but limit access to information associated with their personal identity using the facet which allows access only to a subset of the data associated with this identity. Users can share information, services and resources in a CIS or in the public domain. Users have complete control of what they share i.e. which resources, information and services, where they share it i.e. publicly or inside a specific CIS and when they share it i.e. under specific context conditions. This is accomplished using preferences and privacy policies. The use of preferences allows the user to define when and how specific services, resources and information can be shared with others. Preferences are also used to define the user's wishes with regard to the disclosure of personal information and the handling of this information by the requestor after disclosure. Preferences are evaluated against the current context of the user and the trustworthiness of the service provider and are used to generate a privacy policy that incorporates all the preferences of the user with regards to the requests of the service provider described in their service privacy policy. A negotiation process is performed to find an agreement about the terms and conditions of the disclosure of specific information from the user to the service provider. A successful negotiation process results in a negotiation agreement which defines the data permitted to be accessed by the service provider (such as name, postal address, e-mail address etc), the responsibilities of the service provider with regard to the handling of the data (such as storing the data in a secured storage medium and not sharing it with 3rd parties) and the rights of the user in the course of the transaction (such as the right to opt out of the service any time).

== Interest in the Workshop and External Collaboration ==

We want to capitalize on existing work, making this platform as interoperable as possible with existing (federated) social networking and open identity management projects. Proof of this is the attention we are giving to OneSocialWeb, BuddyCloud and Shibboleth, looking at their code base and considering their core enabling technologies (XMPP and SAML) for use within the project.

While the SWAT0 tests [11] and the proposals for the upcoming SWAT level 1 [12] understandably focus on the very initial use cases, we believe there is much to be gained by considering future extensions. We expect to bring a new perspective that adds value and contributes to the current ongoing work.

The contractual results of the project include a fully working open source platform with a community of 50 contributors and 1000 users by
the end of the project, so we are aiming at strong external collaboration. The project's architecture is still under development and key aspects will be decided in a meeting in 2 weeks, so this is a decisive point in the project. Any comments and suggestions will be welcomed and considered by the consortium. The architecture will be publicly available when stable, in a few months. Also, we will be creating our source code repository within the year. Anonymous read access will be possible to all the code developed in the project and we will welcome bug reports and patches provided by the community. More information will become available in the project website (http://www.ict-societies.eu/) as work progresses. Key contacts are Kevin Doolin (TSSG), project leader, and David Mckitterick (INTEL), technical leader.

Finally, SOCIETIES is coordinating the Service Front Ends Working Group [13], formed by projects working on context modelling and management, or evolution of web technologies that enable users, organized in communities, to mash-up, configure connect, and share services in a knowledge-aware manner. The projects that are collaborating under this WG are I2Web, MobiWebApp, Omelette, Serenoa, SocIoS and webinos.

-- References --


