Enabling Trust and Privacy on the Social Web

W3C Workshop on the Future of Social Networking, 15-16 January 2009, Barcelona

Alexandre Passant [1], Philipp Kärger [2], Michael Hausenblas [1], Daniel Olmedilla [3], Axel Polleres [1], Stefan Decker [1]

[1] Digital Enterprise Research Institute, National University of Ireland, Galway, Galway, Ireland

[2] L3S Research Center, Hannover, Germany

[3] Telefonica R&D, Madrid, Spain

Motivation

Based on our recent observations at the 7th International Semantic Web Conference and some related workshops as the "Social Data on The Web" one [1], as well as other frequent discussion threads on the Web, trust and privacy on the Social Web remains a hot, yet unresolved topic. Indeed, while Web 2.0 helped people to easily produce data, it lead to various issues regarding how to protect and trust this data, especially when it comes to personal data. On the one hand, we are wondering how to protect our private information online, above all when this information is re-used at our disadvantage. On the other hand, information should not only be protected when being published by its owners, but tools should also help users to assess trustworthiness of third-party information online. According to our recent research works, both from a theoretical and practical point of view, we think that Semantic Web technologies can provide at least partial solutions to enable a 'trust and privacy layer' on top of the Social Web. Hence, this position paper will present our work on the topic, that is in our opinion, also particularly relevant to the mobile Web community, according to the advances of ubiquitous Social Networking with, e.g., microblogging from mobile devices.

Challenges

Sharing information with trusted and intended parties

People tend to publish personal information on the Web, be it pictures (e.g., on popular sites like Flickr, Facebook, etc.), thoughts (blogs), videos (e.g., YouTube), or even complete profiles comprising date of birth, postal address, phone number, etc. on personal homepages or social network applications (e.g., Linkedin or Xing). Yet, there is no simple way to restrict access to some content to only a set of trusted parties or to decide who is allowed to access some part of a profile. Some sites, such as for instance Flickr, allow to define people as friends or family members to restrict access, but then there is no more fine-grained data management. Thus, if both collegues and close friends are in the same "friends" group, there is no way to restrict access to a subgroup for a particular picture. Another complex problem regarding online pictures is the issue of co-depiction. For instance, on Facebook pictures can be put on the Web, while the affected person learns about it in retrospect. By the social connections of depicted and tagged people though, co-depicted non-tagged people are almost as easy to find. Still, pictures become available immediately on one's own public space although they are not necessarily intended to be public.

Another relevant trend is the use of microblogging websites, such as Twitter, that provide a straightforward and ubiquitous way to create lifestreams from many different devices. Yet,

there is no policy to whom this information is delivered and there is a need for fine-grained privacy settings, for instance allowing to disclose one's geographic location only to family members. Blogging about meetings is another big issue in terms of not only privacy-loss but also violation of corporate policies: more and more, people are writing posts that tell about them participating in an important meeting, other people attending the same meeting, etc. Competitors can freely read and exploit this information. The search query for "meeting" posts on Twitter reveals that there are more than 10 posts every two minutes telling about attending a meeting, some of them being internal corporate meetings. Another example regarding the need of fine-grained access rights is user profiles management. For instance, on Blogger users can only share their personal information completely or not at all, but cannot decide who can access e.g. their birth dates.

Retrieving trusted information and avoiding social software annoyance

While the previous point focused on publishing private information, similar issues arise when consuming information. The general question is hence "How trustworthy is what we find on the Web?". When browsing a web page, current browsers provide means to protect users from phishing, but still there are no means to assess if a web page contains information of someone you should trust or not. This information might either be computed based on the social network relations (both explicit and implicit ones: explicit might be an intentional addition to a friend-list, while implicit might be entailed by common and repetitive exchange of messages), based on some of your interests, or based on a negotiated trust level.

Another related issue is social information overload, or social software annoyance. Web 2.0 eased the process of information publishing to an extent that overwhelms its consumers. Filtering options are mostly restricted to very simple means. For instance users may specify to be updated with the state of the art on a particular topic by subscribing to various RSS feeds (such as del.icio.us and technorati). However, popular feeds may become hard to keep track with because they still provide a tremendous amount of information in short time which is too difficult to manage. Similarly, many social media services and applications provide alert functionality, getting informed each time a friends does or writes something which leads to further "social information overload". However, in most cases information can be of particular relevance if provided by someone trusted on a particular topic. Topicwise filtering may significantly improve the current all-or-nothing approaches. For instance, Alice may like to get microblogging updates via text message on her mobile phone about Bob's postings concerning technology, but not regarding his personal details. Instant messaging faces similar problems: instant messaging applications such as Skype for example allow to define access rules for incoming calls and chats, but is not fine-grained enough to make call acceptance dependent on the call context, such as time or the callee's current location. For example, one may allow to be disturbed in a meeting by colleagues, but not by family members. Complex filters as we know them from mail clients, are missing for emerging newer communication channels online, and even those complex filters in mail clients still do not allow features such as consistency checking, sharing and aligning along the social network, beyond simple address book synchronisation with social network sites at best.

A trusted and privacy-aware Web

Using a practical Semantic Web approach to enable trust and privacy

Taking trust and privacy into account for both, publishing and consuming information on the Social Web, raises the need for privacy and trust policy statements on the Web. But to what extent can those privacy policy statements be automatically enforced? How big are the usability issues if a user is faced with the request to define such a policy? Or are there ways to elicit policy statements, for example from a user's behaviour in a social network or from users' semantically enriched personal data?

There is plenty of research available in the area, however with little or only limited-scope impact so far. We have recently developed the "Provenance-Trust-Privacy" (PTP) model [2] where basically two aspects are covered: the real life and the online world, that is, the Web. In the PTP model we deal with three orthogonal, nevertheless interdependent dimensions, (1) the social dimension, (2) the interaction dimension, and (3) the content dimension. We envision large-scale, real-world testing and experience, backed up by sound theoretical work.

Let's imagine that Alice wants to give access to her wedding pictures only to people that are fellows on both Flickr and Twitter and that have a blog she commented at least twice during the last 10 days. This privacy policy is quite complex. It involves activities from different Social Media websites and it is evolving, as Alice may add people on Twitter and may also comment on some blogs while older comments become obsolete for that policy definition. To face this complexity, Semantic Web technologies are appropriate means for modelling and formalisations. Indeed, by weaving social networks to FOAF (Friend Of A Friend) and social activities such as blog comments to SIOC (Semantically-Interlinked Online Communities,), the Semantic Web provides a complete interlinked graph on top of existing applications. FOAF and SIOC exporters are currently available for major Web 2.0 services and weblogging applications and more details regarding SIOC can be found on the related position paper of that workshop.

Retrieving information from this graph, for example information about who commented on who's blog, can be exploited for deciding whether a policy applies or not, i.e., whether access to a picture is granted or not. Such policies can be expressed and evaluated e.g. using the SPARQL query language to aggregate RDF, or RIF as a format to express policy rules. Still, although liaisons between the responsible W3C working groups exitst, more work is needed to make these standards play well together. A use case driven alignment of the related standards could well be in scope of a newly established working group.

Moreover, from a practical aspect, OpenID can be used here as a logging scheme, especially since there are ties between FOAF and OpenID relating a persons profile to her actual OpenID and therefore providing a certain amount authentication, as we examplified through the development of SparqlPress. This can be used as a starting point for establishing trusted sources of information (e.g., a personal FOAF file) and hence, help a system to automatically check if a user logging-in to her private pictures is actually allowed to access the data or not.

However, when e.g. using FOAF information on the Web to extract links to OpenID, authoritativeness of the provided information needs to be checked. We have proposed earlier already mechanisms to include a notion of authoritatativeness in OWL reasoning [3], which prevents RDF and OWL statements made by a non-authoriative party from affecting reasoning. This notion needs to be extended to the instance level though, for determining authoritativeness of OpenID links. Nonetheless, what is important here is that we consider a widely agreed notion of authoritativeness of RDF statements a necessary and missing prerequisite for further trust based applications on the Social Semantic Web.

It is not only social data that can be used in that process. Any semantically annotated data - exposed from existing RDMS or legacy systems for example - that is in consideration when deciding trust or privacy policies can be used. For instance, Bob may allow access to his resume only to people interested in Semantic Web technologies. Such interest can been modeled using for example using identifiers provided by DBpedia (an RDF-ised version of Wikipedia). By using the graph layer, the relationships between interests, and standard Semantic Web reasoning techniques, people interested in SPARQL or RDFa will be authorized, since both, SPARQL and RDFa, are considered related to the Semantic Web (these relations are already present in the current DBPedia export).

Policy-based approaches to Trust and Privacy

Privacy and Trust on the Web has been approached from several different perspectives over the last years. One of the most expressive and flexible approach for privacy is policy-based access control. In general, a policy is a well-defined statement that guides a system's or agents' behavior. Policies specify exactly how a system behaves under certain conditions - for example whom to grant access to a resource at a given time/place. In the last years, the concept of Semantic Web policies gained momentum [4] since they are the most promising means to establish the security and trust layer in the Semantic Web stack. Semantic Web policy languages have a well defined semantics and therefore, they make behavior descriptions machine-understandable. They exploit Semantic Web technologies for making decisions and sharing concepts among different parties. Although prominently applied to security, decisions described by policy statements are not only restricted to security, they also include many other scenarios such as, among many others, network configuration or agent negotiations. Currently, there are many policy frameworks available based on semantic technology, such as Protune, Rei or Kaos.

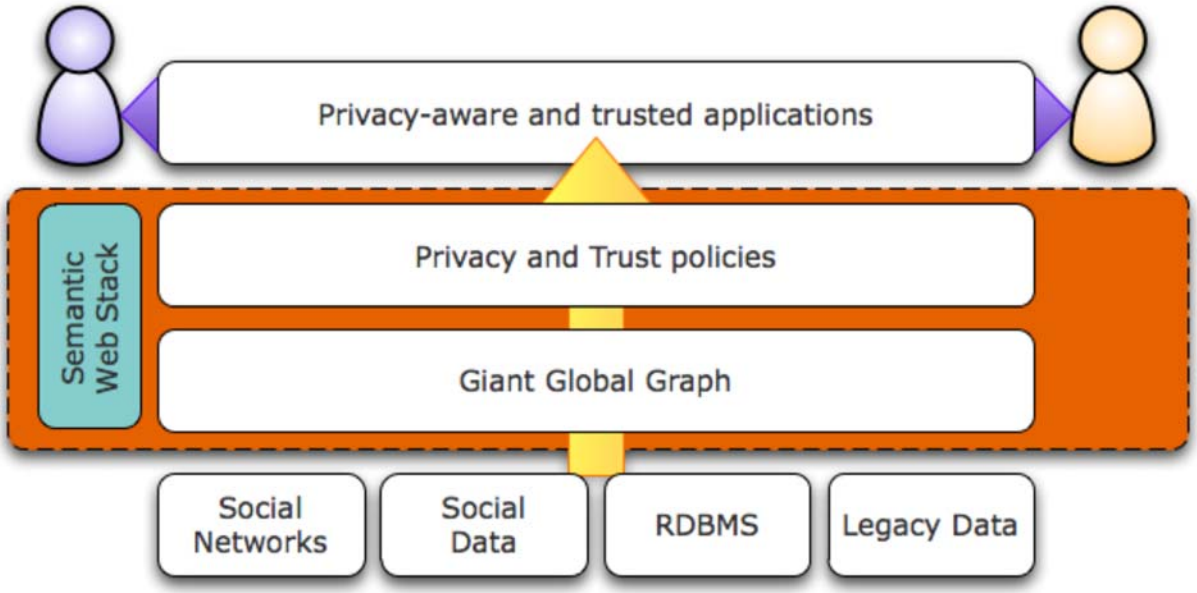
Most of the current access control approaches do not fit well an open system like the Social Web. Well known concepts like Role-based Access Control cannot be applied since there is no fixed set of users and no fixed set of roles on the Web. Moreover, also the set of service providers is not known in advance and is growing. So how shall a user trust a service provider that she never used or heard of before? And how shall a service provider trust a new client? On the Social Web we are facing a similar situation: people who do not know each other do interact and may either avoid or strive for information sharing.

Trust negotiation [5] is an approach where two parties exchange information in order to build up mutual trust in a step-by-step manner. Here, policy statements are protecting specific information or resources. Hence, in trust negotiation, policy statements express what is needed in order set up the desired relationship such as to get access or to put through a message. By matching or exchanging the policy statements of both parties, a successful exchange of information yielding to a trust relationship can be identified automatically. On the Social Web, these techniques provide solutions for cases where an interaction requires a certain level of trust. If, for example, a user who is currently off-line receives a chat message via skype, then, based on the level of trust established between the caller and the callee, this message may be forwarded to the callee's mobile phone or not. Consequently, policies are not only exploited to control access to potentially private data on the Social Web, they also serve for the opposite direction, that is, information that a user receives can be filtered according to her personal level of trust and therefore reducing the burden of social spam.

Towards policy-aware and trusted applications

To summarise these use cases, the Semantic Web stack, which (1) provides an interlinked graph of data needs to be enriched by (2) suitable, agreed models for defining policies as well as provenance/authoritativeness, both by using existing data from different sources. Such an infrastructure can be ideally used in existing applications to provide them with the expected layer of Trust and Privacy. Users can immediately benefit from such an enriched Semantic Web stack when publishing, sharing or browsing data, in a flexible and autonomous way, taking into account various patterns and especially the evolution of their social behaviours, cf. Figure 1.

Figure 1: Semantic Web stack for Trust and Privacy on the Social Web



Next Steps

We think that Semantic Technologies could provide an ideal solution (open, based on standards) to the issues of privacy and trust on the Social Web. While our current experiments are mainly focused on research datasets, we expect to apply those techniques on large-scale systems with industrial partners. RDF and Semantic technologies are being taken up in the Social Web, for instance, by the recent use of SIOC in Yahoo! SearchMonkey, or the availability of Freebase in RDF, or other social sites starting to export RDF. These trends enable to search and aggreate social information. While we see a huge potential in these activities and similar trends are to be expected in the Mobile Web, we also emphasize the need for providing means to assess trust and guarantee a reasonable level of privacy.

Semantic techniques are available to help realising a trusted Social Web, however there are a number of open issues such as usability, interplay of existing standard, scalability and acceptance by end-users and service providers yet to be resolved. We will organise a workshop on the topic at the next European Semantic Web Conference so that researchers and practicioners can discuss the topic further. Moreover, we also see the need for a potential working group in terms of standards to describe policies, define "authority", as well as providing guidelines and best practices for publishers, and discussing further means to reveal pricacy threats to users.

References

[1] Proceedings of the *ISWC2008 Workshop on Social Data on the Web (SDoW2008)* Karlsruhe, Germany, October 27, 2008.
[2] W. Halb, M. Hausenblas. *Position Paper on select * where { :I :trust :you }*. International Workshop on Interacting with Multimedia Content in the Social Semantic Web (IMC-SSW 2008). Dec 2008.
[3] A. Hogan, A. Harth, A Polleres. *SAOR: Authoritative Reasoning for the Web*. In Proceedings of the 3rd Asian Semantic Web Conference (ASWC 2008), volume 5367 of Lecture Notes in Computer Science, pages 76-90, 2008.
[4] P. A. Bonatti, C. Duma, N. Fuchs, W. Nejdl, D. Olmedilla, J. Peer, and N. Shahmehri. *Semantic web policies - a discussion of requirements and research issues*. In 3rd European Semantic Web Conference (ESWC), volume 4011 of Lecture Notes in Computer Science, Budva, Montenegro, 2006. Springer.
[5] M. Winslett. *An introduction to trust negotiation*. In iTrust, pages 275-283, 2003.


W3C
XHTML
+ RDFa