Proceedings of the I-SEMANTICS 2012 Posters & Demonstrations Track, pp. 43-47, 2012.

User Controlled Privacy for Filtering the Web of Data with a User-Friendly Manager*

Owen Sacco, Alexandre Passant, and John G. Breslin

Digital Enterprise Research Institute,
National University of Ireland, Galway, Ireland
{owen.sacco,alexandre.passant}@deri.org,{john.breslin}@nuigalway.ie

Abstract. Web of Data applications simplify the process for publishing information such as user's personal information. Although some provide privacy settings, these are limited and users require further options to restrict access to some parts of their data. In this demo paper, we present the extended Privacy Preference Manager (PPM) that enables users to (1) create privacy preferences using the Privacy Preference Ontology (PPO) and (2) grant or restrict access to their data to third-party users based on user profile features for example interests.

1 Introduction

Web of Data applications provide minimum privacy settings such as restricting access to private data to those who are in approved user lists. Yet, users require more complex privacy settings as some current systems do not meet their requirements for example in Social Networks [1]. Current work, for instance [5], use specific policy languages which require users to understand how to interpret privacy rules.

In addition to the full-paper from the research track [2], in this demo paper we describe the implementation and user interface of the extended Privacy Preference Manager (PPM). Moreover, we also demonstrate how it solves the above issues by allowing users to: (1) create fine-grained privacy preferences using the Privacy Preference Ontology (PPO) [3] for data residing in documents or SPARQL endpoints; and (2) let other users access this data, filtered according to these privacy preferences.

2 Overview of The Privacy Preference Ontology (PPO)

The Privacy Preference Ontology (PPO) [3] [2] – `http://vocab.deri.ie/ppo#` – is a light-weight vocabulary that allows people to describe fine-grained privacy preferences for granting or restricting access to specific Web of Data. Besides

* This work is funded by the Science Foundation Ireland (grant SFI/08/CE/I1380 (Líon 2)) and by an IRCSET scholarship co-funded by Cisco systems.

other use-cases, PPO can be used to grant part of a FOAF user profile only to users that have specific attributes. It provides a machine-readable way to define preferences for instance "Provide my work email address only to DERI colleagues" or "Grant write access to my blog only to my relatives"; assuming that the requester's attributes are trustworthy.

A privacy preference defines: (1) the resource, statement, named graph, dataset or context it applies to; (2) the conditions refining what to grant or restrict, including operators that connect several conditions; (3) the access control type; and (4) a SPARQL query, (`AccessSpace`) *i.e.* a graph pattern that must be satisfied by the user requesting information. The access control type is defined by using the extended Web Access Control (WAC)[1] vocabulary which defines the `Create`, `Read` and `Write` (which also includes `Update`, `Delete` and `Append`) access control privileges.

3 *The Privacy Preference Manager (PPM)*

The *Privacy Preference Manager (PPM)*[2], enforces privacy preferences for filtering data on the Web of Data. Although it is designed to work with any data on the Web of Data[3], we demonstrate how to define privacy preferences for FOAF profiles. Our aim is to illustrate how PPO can be applied to create privacy preferences and how personal information can be filtered based on those preferences.

The *PPM* allows users to manage their privacy preferences and also grants or denies access to user's information when requested by others. During this demo, users can (1) create their own Privacy Preference Manager instance; (2) authenticate to their instance and create privacy preferences for their data such as their FOAF profile; and (3) authenticate to other user's instance and access the filtered data, in this case filtered FOAF profile of these users.

The architecture of the system, illustrated in figure 1, consists of: (1) WebID Authenticator: handles user sign-on using the FOAF+SSL protocol [4]; (2) RDF Data Retriever and Parser: retrieves and parses RDF data such as FOAF profiles from SPARQL Endpoints or RDF documents; (3) Privacy Preferences Creator: defines privacy preferences using PPO; (4) Privacy Preferences Enforcer: queries the RDF data store to retrieve and enforce privacy preferences; (5) User Interface: provides users the environment to create privacy preferences and to view filtered RDF data; and (6) RDF Data store: an ARC2[4] RDF data store to store the privacy preferences[5].

[1] WAC — `http://www.w3.org/ns/auth/acl`

[2] Screencast online – `http://vmuss13.deri.ie/ppmv3/screencast/screencast.html`

[3] Currently Web of Data modelled as RDF

[4] ARC2 — `http://arc.semsol.org`

[5] Although ARC2 was used for the implementation of the Privacy Preference Manager, any RDF store can be used.

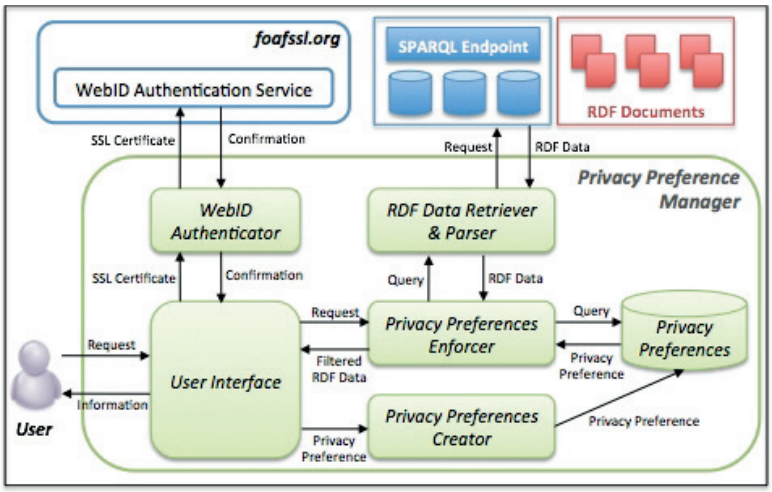

Fig. 1. Privacy Preference Manager

3.1 Creating Privacy Preferences

The system's interface provides users to create privacy preferences. Privacy preferences can be applied to triples retrieved from either a manually inputted SPARQL query; or a manually inputted URL; or from a users' FOAF profile extracted from the URL within a WebID certificate.

Once the triples are retrieved, the interface then consists of 2 columns representing: (1) on the left - the profile attributes which the user wants to share; (2) on the right - other attributes that a requester must satisfy to get access to the specific information. Once the choices are validated, the corresponding PPO preferences are created and stored in the system. For example, fig. 2 represents how a user can enable that his name, contact details, homepage and affiliation are available only to people working at DERI.

3.2 Requesting and Enforcing Privacy Preferences

The *PPM* has been extended to support both granting and restricting access; unlike previously that only supported granting access and assumed that everything is private by default unless defined otherwise.

The sequence in which privacy preferences are requested and enforced, consists of: (1) a requester authenticates to another user's manager instance using the WebID protocol so that the system can request the other user's FOAF profile; (2) the privacy preferences of the requested user's FOAF profile are queried to identify which preference applies; (3) the access space preferences are matched according to the requester's profile to test what the requester can access; (4) the requested information (in this case, FOAF data) is retrieved

Fig. 2. Creating privacy preferences in the Privacy Preference Manager

based on what can be accessed; and (5) the requester is provided with the filtered data she can access.

During the demo, the user is able to view how other users would see his/her profile based on the privacy preferences created which enables the user to validate that the privacy preferences created are the ones that were intended. Moreover, the user can also log into other user's instances to view the filtered information which they can access based on the instance owner's privacy preferences.

4 Conclusion

Privacy Preference Manager provides users to create privacy preferences for their data on the Web of Data and it filters data on the basis of these privacy preferences, which will be demonstrated during the demo session. Although an evaluation is still ongoing, we evaluated the system with 15 users who all confirmed that the filtered FOAF profile is what they expected after creating their preferences. As next steps, we will enhance the user interface based on users' feedback, notably to provide more options from which they can select from.

References

1. D. Boyd and E. Hargittai. Facebook privacy settings. Who cares? *First Monday*, 15(8), August 2010.
2. O. Sacco and J. Breslin. PPO & PPM 2.0: Extending the Privacy Preference Framework to provide finer-grained access control for the Web of Data. In *Proceedings of the 8th Int. Conference on Semantic Systems, I-SEMANTICS'12*, 2012.
3. O. Sacco and A. Passant. A Privacy Preference Ontology (PPO) for Linked Data. In *Proceedings of the Linked Data on the Web Workshop, LDOW2011*, 2011.
4. H. Story, B. Harbulot, I. Jacobi, and M. Jones. FOAF + SSL : RESTful Authentication for the Social Web. *Semantic Web Conference*, 2009.
5. J. Zeiss, R. Gabner, A. V. Zhdanova, and S. Bessler. A Semantic Policy Management Environment For End-Users For End-Users. In *Proceedings of International Conference on Semantic Systems, I-SEMANTICS'08*, 2008.