D-FOAF - Distributed Identity Management based on Social Networks

D-FOAF

Distributed Identity Management based on Social Networks

Sebastian Ryszard Kruk
WETI, Gdansk University of Technology, Poland
DERI, NUI Galway, Ireland
sebastian.kruk@deri.org

Adam Gzella
WETI, Gdansk University of Technology, Poland
DERI, NUI Galway, Ireland
adam.gzella@deri.org

Sławomir Grzonkowski
WETI, Gdansk University of Technology, Poland
DERI, NUI Galway, Ireland
slawomir.grzonkowski@deri.org

ABSTRACT

Contemporary Web consists of more than just information, it provides a large number of services, which often require identification of it's users. Since distributed or shared identification systems are not yet widely adopted many users have to maintain a large number of different credentials for different services. Furhermore current authorisation systems require strict centralisation of the authorisation procedure. Although the feature of enabling user's friends or good friends of a friends to access user resources would be benefical for services and business on the Web, it is not usually offered by existing systems. In this article we present D-FOAF, a distributed identity management system that utilizes social networks. We show how information inherent in social networks can be utilised to provide community driven access rights delegation and distributed authorisation.

Keywords

Identity Management, Distributed Computing, Social Networking

1. INTRODUCTION

The proliferation of Internet services introduced many problems like no single identity for Internet users or no scalability in trust and access rights management. Some of those problems have been addressed in many ongoing projects.

The main difference between internet and real world services are authorisation procedures. In the real world each person has a single identity expresses with credentials like an ID card, a passport or a driving licence. This allows real world service providers to easily confirm the authentity of the presented credentials. In the Internet, each user has to deal with a number of identities with different credentials like login-password pairs. Since there is no notion of single identity, service providers are usually inclined to introduce new credentials for each user. As a result the trust to each user is build within each service separately.

Approaches like Microsoft Passport [2], Sxip [7] or Liberty Alliance Project [3] are aiming to provides a solution to the single-sign-on problem. Due to various problems. none of those projects has been widely addopted by service providers so far. So they are useless for the majority of Internet users with the ever growing number of service.

Most of online services are usually based on very simple user profile management implementations that do not address problems stated above. Access rights are based on predefined, fixed lists of groups and neither allow finer granularity nor trust delegation.

The notion of social networking emerged in the Internet with online community portals like Orkut [10] that allow users to control access to the information based on the structure of the social network. Each user can restrict access to some parts of his/her profile information delegating trust within given number of degrees of separation.

Some of problems encountered in Microsoft Passport [2] were overcome by Sxip [7], which enable users to gain more control over their profile information stored on one of home servers. Next version of Sxip 2.0 will provide increased anonymity for users with the Identity 2.0 [1], a protocol for exchange of digital identity information. The general idea is to provide users with more control over what others know about them. Furthermore, it will be possible to adjust security needs to the specific site.

In this short article we introduce the main requirements of the Identity 2.0 protocol (see 2). We present how some of them, including support for mobile computing paradigm, have been implemented in D-FOAF (see 3). Finally we describe an overview of the demo we would like to present at ESWC2006 (see 4).

2. TOWARDS IDENTITY 2.0

Nowadays we have as many identities as services we use. Usually, we can hardly transfer the digital identity from one website to another. Thereofre the trust we gain in one community is useless in another because it does not affect our reputation there. Thus we are forced to repeat the whole process of gathering trust again and again.

Since the contemporary systems does not allow users to decide which information is available for the other portal users, it causes the lack of privacy control over the user profile.

These problems should be resolved by means of an advanced social network system that would model the social interaction close enough to a real world ones. In addition,

Demos and Posters of the *3rd European Semantic Web Conference (ESWC 2006)*, Budva, Montenegro, 11th - 14th June, 2006

the solution must be easy to use and enable users to share the credentials among many services. Although the strong security support to protect identities of the users must be provided, all of these features should be transparent from the end-user perspective.

The main objective of Identity 2.0 protocol is to provide users with full control over their virtual identities. It seems to be a suitable solution for the described problem. The presented below the FOAFRealm(see section 3) system aims to meet the requirements of the Identity 2.0 and extend them.

3. DISTRIBUTED FOAFREALM

The FOAFRealm [9] is a library for user identity management based on the FOAF vocabulary [4]. FOAFRealm enables users to control their profile information defined in the open FOAF metadata. To provide enhanced resource rights management FOAFRealm extends generic FOAF description by friendship evaluation based on reification of <`foaf:knows`> RDF statements.

Generic FOAFRealm consist of three general parts:

- FOAF metadata and collaborative filtering ontology management. It wraps the actual RDF storage being used from the upper layers providing simple access to the semantic information. The Dijkstra algorithm for calculating distance and friendship quantisation is implemented in that layer.
- Implementation of the `org.apache.catalina.{Realm, Valve}` interfaces to easily plug-in the FOAFRealm in to Tomcat-based web applications. It provides authentication features including autologin based on Cookies.
- A set of Java classes, Tagfiles and JSP files plus list of guidelines that can be used while developing user interface in own web applications

D-FOAF (Distributed FOAFRealm) [6] project aims to make the FOAFRealm work in fully distributed environment. A new distributed communication layer introduced in D-FOAF provides access to highly scalable HyperCuP Lightweight Implementation [11, 8] of P2P infrastructure to communicate and share the information with other FOAFRealm implementations.

The most important D-FOAF features are:

- Distributed user authentication - realization of Single-sign-on conception.
- Distributed user identity merging - ability to merge distributed user identity on demand.
- Computing distance and trust levels between users in distributed environment.
- Security of distributed computing - creating suitable identity protection.

Next step in FOAFRealm/D-FOAF development is DigiMe, a ubiquitous indentity management compliant with Identity 2.0 assumptions. We made first steps towards DigiMe, by building ubiquitous search and browsing application [5]. It was developed on J2ME platform, and provides simple access to FOAFRealm/D-FOAF identity for mobile devices.

FOAFRealm/D-FOAF system has been successfully deployed with JeromeDL - semantic digital library. In addition to unique distributed identity management FOAFRealm allows JeromeDL to integrate user and author list in semantic query expansion algorithm.

4. PRESENTATION PLAN

During the demo session we will present how distributed identity management based on social networking works in existing systems and how it can be easily deployed in new services. The demonstration will consist of:

1. Generic FOAFRealm in JeromeDL: registering new user, logging into library, adding friends.
2. D-FOAF's distributed authentication: logging into different JeromeDL instances using existing set of credentials.
3. D-FOAF's user identity merging: gathering distributed user identity in JeromeDL.
4. D-FOAF's distance and quantisation level computing: accessing the protected resource using the friedship informations saved in different JeromeDL instance.
5. DigiMe mobile application: managing identity information, friends list and bookmarks using mobile device.

4.1 Acknowledgments

This work was supported by Science Foundation Ireland Grant No. SFI/02/CE1/I131 and by the Knowledge Web project (FP6 - 507482) and partially by KBN, Poland under grant No. 4T11C00525. The authors would like to acknowledge Stefan Decker, John Breslin, Tomasz Woroniecki, Choi Hee Chul, the DERI Semantic Web Cluster and the Corrib.org working group for fruitful discussions.

5. REFERENCES

[1] Identity 2.0: http://www.identity20.com/.
[2] Microsoft Passport: http://www.passport.net.
[3] L. Alliance and WS-Federation. A Comparative Overview. White Paper. Technical report, 2003.
[4] L. Dodds. An Introduction to FOAF. http://www.xml.com/pub/a/2004/02/04/foaf.html, 2004.
[5] S. Grzonkowski, A. Gzella, M. Cygan, and S. R. Kruk. Digime - ubiquitous search and browsing for digital libraries. In *Submitted to MoSo 2006 Workshop*, 2006.
[6] S. Grzonkowski, A. Gzella, H. Krawczyk, S. R. Kruk, F. J. M.-R. Moyano, and T. Woroniecki. D-foaf - security aspects in distributed user management system. In *TEHOSS 2005*, September 2005.
[7] D. Hardt. Personal Digital Identity Management. In *FOAF Workshop proceedings*, 2004.
[8] HyperCuP Lightweight Implementation project: http://www.hypercup.org/.
[9] S. R. Kruk. FOAF-Realm - control your friends' access to the resource. In *FOAF Workshop proceedings*, http://www.w3.org/2001/sw/Europe/events/foaf-galway/papers/fp/foaf_realm/, 2004.
[10] Orkut. http://www.orkut.com/.
[11] M. Schlosser, M. Sintek, S. Decker, and W. Nejdl. HyperCuP–Hypercubes, Ontologies and Efficient Search on P2P Networks. In *Third International Workshop on Agents and Peer-to-Peer Computing*, 2004.