Ensuring privacy in FOAF profiles*

György Frivolt and Mária Bieliková

Institute of Informatics and Software Engineering
Faculty of Informatics and Information Technologies
Slovak University of Technology in Bratislava
Ilkovičova 3, 842 16 Bratislava, Slovakia
{frivolt,bielik}@fiit.stuba.sk

Abstract. Portals providing modeling of social relations among people became more and more popular. Although the existing FOAF (Friend of the Friend) ontology developed for modeling such social relations was introduced and enjoyed popularity, it is not used in such extent that it can be considered as a World Wide Social Network. On the other hand, the existing social network services provide wide range of services to the users and they count huge number of users, but they are not interconnectable. We believe that FOAF might become a good basis for providing personal information in the way as social network services do if the sensitive personal information were ensured against not authorized agents. We aimed to solve the problem of privacy for FOAF profiles.

1 Introduction

Portals providing *social network services* (e.g., `www.iwiw.net`, `www.hi5.com`, `www.friendster.com`) enable users to connect people with different types of interests and thus provide a virtual social environment. These portals enjoy popularity and provide several applications to the users, like looking up old friends and relatives [5], finding employer/employee using the social network (`www.linkedin.com`), sharing personal content, etc. People interlinked through social network services can form so called *online communities*.

Current social network services use their own data representation invisible for other systems that provide social network services. Users of different services cannot get connected as the social sites do not offer such possibility. Different users remain enclosed in various systems forming disconnected components of the social network. Therefore the global (world wide) social network nowadays consists of isolated islands [1].

Profiles stored inside current social network services are not addressable, whereas RDF has its URI and thus can be reused by any service having access to it. For this purpose we use an RDF based format FOAF (`http://xmlns.com/foaf/0.1`) as a basis for profile description and social relation descriptions.

* This work was partially supported by Science and Technology Assistance Agency under the contract No. APVT-20-007104 and by the Scientific Grant Agency of Slovak Republic, grant No. VG1/3102/06.

We believe that FOAF might become a standard for providing personal information on the Web. However, proof of this concept requires two problems to solve. First, the existing personal profiles residing in different resources (such as social network services) should be brought to the world of FOAF. Second, the sensitive parts of the FOAF profiles should be ensured against not authorized eyes. We are concerned about the second issue in this article.

FOAF (Friend of a Friend) is an ontology for describing information related to particular person in machine readable way. By using RDF, FOAF gains a powerful extensibility mechanism by `rdfs:seeAlso` references, allowing FOAF-based descriptions be mixed with claims made in other RDF vocabulary. Other persons' FOAF description can be referred by `foaf:knows` properties, meaning the person knows the referred one.

Researching social networks and related issues such as privacy in social networks is a vibrant field today. Several automated systems for gathering social networks from web documents exist [4,2,4]. Searching for connections between the Semantic Web and social networks, techniques for gathering social networks from the Web is an active research issue [3,6].

2 Our approach to securing FOAF profiles

We are determined by the privacy issues applied by the social portals as they need to be resolved if we want to wrap the content of them. On the other hand perhaps the same issues noticed by the social portals might show up in the world of FOAF.

Securing sensitive personal properties is a more issue. Users of social network services are able to specify the set of users they wish or do not wish to share their personal properties with. Every personal property (email, phone number, etc.) has to be specified, who is permitted to access to it, and who do not.

We define *access restrictions* for the personal properties. Access restriction consists of tuples of persons Ps_i – specified by an URI of the person's FOAF file), and properties Pr_i – URI of the FOAF properties which allowed to be seen. We use the following notation for describing the access restrictions: $(Ps_1, Pr_1), (Ps_2, Pr_2), \ldots$.

Our approach for securing the FOAF profiles is based on dividing the FOAF file to partitions, stored in separate files. One partition is the core part of the FOAF profile holding the `foaf:Person` property and the public properties. This file is referring to other files holding the properties access restricted to a person/group of persons. Each of these files is restricted to other group of persons. Partitioning of FOAF file reflecting different access restrictions is depicted on Fig. 1.

The situation depicted on Fig. 1 is compiled to files listed in Tab. 2. The main FOAF file is linked to the partial files by the `rdfs:seeAlso` property. Partitioning is realized by separating groups of persons $AccessGroup_i$ from the sets Ps_i in access restrictions in a way that for every $AccessGroup_i$ exists a set of $Ps_{k_1}, \ldots Ps_{k_m}$, where $AccessGroup_i = \bigcap_{l=1}^{m} Ps_{k_l}$.

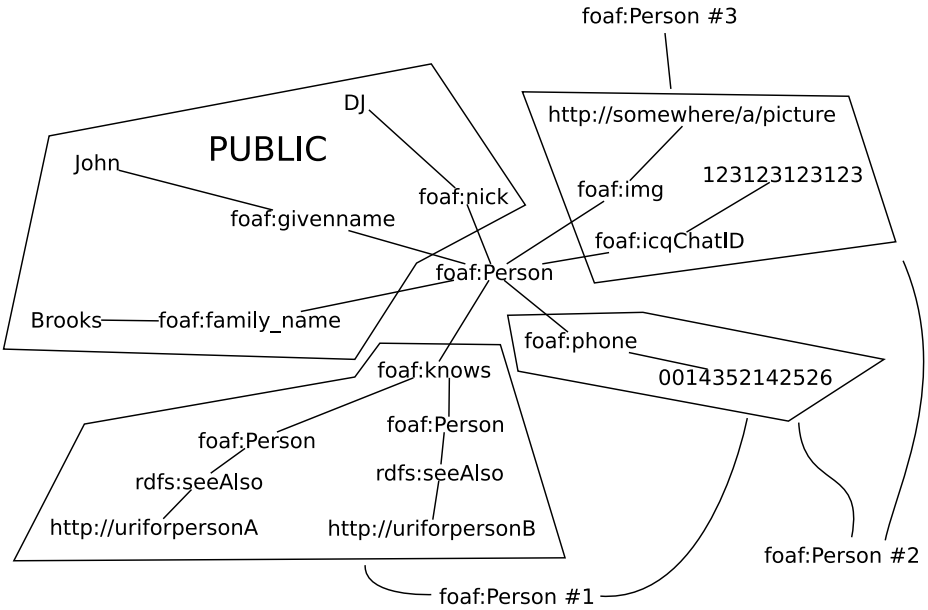

Fig. 1. Partitioning of a FOAF file. Four partitions are deduced from the access restrictions: public personal properties and three partition visible by the three persons.

Securing the privacy, i.e. disabling the access to the files is ensured by the possibilities of the HTTP(S) protocol. Restricted properties in the FOAF profile are accessible only by a username/password or by a key. Thus we need to securely pass the necessary information for authentication to the authorized person. We propose to use the public key published in the FOAF profile of the authorized person. This public key is used for encoding the authorization information for the restricted FOAF properties.

3 Summary and future work

We are concerned about the current state of social networks residing on the Web. We believe that two problems should be aimed to build a world wide social network: gathering of user profiles and ensuring at least basic privacy. Exploration of user profiles can be reached by applying information retrieval techniques on different resources containing social profiles. In this paper we have discussed the second issue and presented an approach for ensuring basic privacy for sensitive attributes in FOAF.

We are concerned about several issues for further research: identification of different profiles belonging to the same person (e.g., transformed from several social portals) ensuring consistency of the network; elaboration of the FOAF file partitioning algorithm; designing the architecture of a free interconnectable social network service software.

Header of all FOAF files:

```
<rdf:RDF
 xmlns:rdf=
  "http://www.w3.org/1999/02/22-rdf-syntax-ns#"
 xmlns:rdfs=
  "http://www.w3.org/2000/01/rdf-schema#"
 xmlns:foaf="http://xmlns.com/foaf/0.1/">
```

Public properties

```
<foaf:Person rdf:ID="me">
  <foaf:givenname>
    John
  </foaf:givenname>
  <foaf:family_name>
    Brooks
  </foaf:family_name>
  <foaf:nick>DJ</foaf:nick>
  <rdfs:seeAlso>1st_part.rdf</rdfs:seeAlso>
  <rdfs:seeAlso>2nd_part.rdf</rdfs:seeAlso>
  <rdfs:seeAlso>3rd_part.rdf</rdfs:seeAlso>
</foaf:Person>
```

Properties visible by the 1st person

```
<foaf:Person rdf:ID="me">
  <foaf:img
    rdf:resource="http://somewhere/a/picture"/>
  <foaf:icqChatID>
    123123123123
  </foaf:icqChatID>
</foaf:Person>
```

Properties visible by the 2nd person

```
<foaf:Person rdf:ID="me">
  <foaf:img
    rdf:resource="http://somewhere/a/picture"/>
  <foaf:icqChatID>
    123123123123
  </foaf:icqChatID>
  <foaf:phone rdf:resource="00143521425 26"/>
</foaf:Person>
```

Properties visible by the 3rd person

```
<foaf:Person rdf:ID="me">
  <foaf:phone rdf:resource="00143521425 26"/>
  <foaf:knows>
    <foaf:Person>
      <rdfs:seeAlso
        rdf:resource="http://URIforpersonA"/>
    </foaf:Person>
  </foaf:knows>
  <foaf:knows>
    <foaf:Person>
      <rdfs:seeAlso
        rdf:resource="http://URIforpersonB"/>
    </foaf:Person>
  </foaf:knows>
</foaf:Person>
```

Fig. 2. FOAF file partitions as it is depicted on Fig. 1

References

1. Gy. Frivolt and M. Bieliková. Growing World Wide Social Network by Bridging Social Portals Using FOAF. In *15th Int. Conf. on Knowledge Engineering and Knowledge Management Managing Knowledge in a World of Networks, EKAW 2006, Poster*, pages 9–10, 2006.
2. Y. Matsuo, M. Hamasaki, Y. Nakamura, T. Nishimura, K. Hasida, H. Takeda, J. Mori, D. Bollegala, and M. Ishizuka. Spinning Multiple Social Networks for Semantic Web. In *Proc. 21st Conf. on Artificial Intelligence, AAAI-06*, 2006.
3. P. Mika. Social Networks and the Semantic Web. In *IEEE/WIC/ACM Int. Conf. on Web Intelligence, WI 2004*, pages 285–291, Los Alamitos, CA, USA, 2004. IEEE Computer Society.
4. J. Mori, T. Sugiyama, and Y. Matsuo. Real-world oriented Information Sharing using Social Networks. In *Int. ACM SIGGROUP Conf. on Supporting Group Work, GROUP 2005*, pages 81–84, New York, NY, USA, 2005. ACM Press.
5. J.C. Paolillo and E. Wright. Social Network Analysis on the Semantic Web: Techniques and Challenges for Visualizing FOAF, 2005. Available at http://www.blogninja.com/vsw-draft-paolillo-wright-foaf.pdf.
6. S. Staab, P. Domingos, P. Mika, J. Golbeck, L. Ding, T. Finin, A. Joshi, A. Nowak, and R.R. Vallacher. Social Networks Applied. *IEEE Intelligent Systems*, 20(1):80–93, 2005.