Access control issues in Social Networks

Anna Carreras, Eva Rodríguez, Jaime Delgado, Xavier Maroñas

Distributed Multimedia Applications Group (DMAG)
Universitat Politècnica de Catalunya (UPC), Jordi Girona 1-3, E-08034 Barcelona, Spain
{annac, evar, jaime.delgado, xmaronas}@ac.upc.edu

Abstract. Social Networks, as the main axis of Web 2.0, are creating a number of interesting challenges to the research and standardisation communities. In this paper, we analyse the current and future use of access control policies in Social Networks. Subsequently, two main issues are addressed: the interoperability amongst systems using different policy languages and the lack of elements in the existing policy languages when trying to express Social Networks' access control. In particular, our approach is based on the use of the XACML standard.

Keywords: Privacy, social networks, access control policies, XACML.

1 Introduction

In the last few years, social networks have been actually *the* Internet phenomenon, and the main axis of the so-called Web 2.0, while creating a number of new interesting challenges to the research community. *Online social networks* are communities in the Internet, usually around one website, which connect users voluntarily sharing information. In this context, mainly due to the growing amount of (personal) data being shared nowadays through internet, users' concern about privacy has risen. From our previous work [1]-[4], we have identified two important issues that still need to be fully solved by the standardization and research communities. First, the existing standardized access control policy languages (i.e. Extensible Access Control Markup Language (XACML) [5]) are missing some elements when trying to express Social Networks current and future privacy policies. And second, the interoperability between different policy languages still needs to be solved. Thus, in the next section, we will first go into details of the aforementioned open issues, and then, in Section 3, we will present our initial approach to solve them, as well as some preliminary work done in this direction. Finally, Section 4 will conclude the paper.

2 Open issues on access control policies languages for Social Networks

As introduced in Section 1, Social Networks present new interesting challenges when trying to address the protection and/or governance of the shared data. In few words, they have created a highly dynamic environment in which users have a producer-consumer role and their actions are based on the idea of "trust". Furthermore, new types of "resources" need to be protected (such as "relationships" or "events"), and a high degree of expressiveness is demanded by users in order to define their own access control (privacy) preferences. Policy expressions mainly depend on the context of the access (apart from the nature of the "resource" that needs to be protected, and the "user's" characteristics). Although XACML has been proved to be flexible enough to describe any type of access control policy, it presents some limitations when applied to privacy protection for Social Networks. For example, as identified during the last W3C Workshop on Access Control Application Scenarios [6], it does not support neither credential based access control, which would allow a more user-friendly privacy protection for Social Networks, nor the use of sticky policies, suitable when addressing data handling. Furthermore, it lacks of attributes to guarantee semantic interoperability among different Social Networks. Indeed, this lack of semantic interoperability, apart from being an issue to be solved at an application-specific level, should be also addressed in a more generic way. Nowadays, different applications and services using different access control policy languages may also need to be interoperable. This time, the incompatibility is not only between different Social Networks but also between a number of heterogeneous services/applications, and thus the interoperability between the different access control policies languages may be even harder to achieve.

Users voluntarily share information, but not only content, also actions and personal information. In addition, service providers are collecting even more information on users' behaviour. However, not only this "voluntarily" provided shared information must be protected. There is an increasing amount of "third parties" which have seen a business opportunity in Social Networks, and are offering all kind of applications to these communities of users. It is important that users had means to decide the access control policies applying to "friends", but also to these "third parties". The implementation of an access control model based on a symmetric level of trust would be recommendable, for example, including the possibility of negotiating policies.

3 Our approach and preliminary work

In this section we address the two main issues previously identified: the lack of interoperability between different Access Control Policy Languages, and the lack of privacy protection when dealing with third-party applications within Social Networks. Thus, we propose a possible architecture which allows (Social Networks') users to control the access to their content without the need of giving it to the Social Network Provider and through the use of policies based on XACML. Furthermore, the use of

some translators (detailed in [3]) guarantees the interoperability between RELs without losing information. The proposed architecture is shown is Fig. 1.

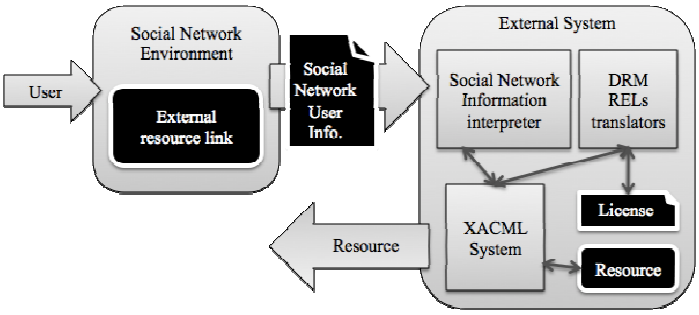

Fig.1 Proposed architecture for access control in Social Networks application scenario

A user would be able to publish an external resource link in her user profile in order to share some of her pictures stored in an External System (external from the Social Network, for example, it could be her private server) with some access control. Then, when another user would check that link, she would be redirected to the external system. The later would extract the necessary context from the Social Network and process the request. Finally, if the object license is not in the XACML language, the RELs translators would generate the appropriate policy and the result would be passed to the XACML system. This module is in charge of authorising the access, and is also detailed in [3]. If the authorisation were positive, the system would access the content, and would show it to the user. If not, it would just show the user a message telling him that she has no rights to do that.

As a next step, it would be very interesting (in the Social Networks application scenario) to give the opportunity to users and service providers to negotiate the access control policies. This is mainly due to the dynamicity of the application scenario being addressed in this paper, and in order to give the maximum control to users over the protection of their contents. For this purpose, a message expressing an "offer" instead of imposing a policy may be required. XACML, as well as RELs, can be used to express offers in which users of a system may propose to other users of the system usage rules for their content according to the rights and conditions that they negotiate. MPEG-21 REL [7] defines the "obtain" right for this purpose, which can be conceptualised as an advertisement to share or sale the associated grant. Within this grant, the rights and conditions initially stated by the offer maker will be defined. Then, in XACML, a similar mechanism can be used to provide this capability. Nevertheless, in [6], held in November 2009, the question on how to establish a user feedback channel in XACML stayed unsolved.

4 Conclusions

In this paper, some novel issues on the access control in Social Networks application scenario have been analysed. In particular, two main issues have been addressed. On the one hand, the interoperability among Social Networks which are using different policy languages and, on the other hand, the lack of elements of the current existing standards trying to express access control policies in Social Networks. In our approach, we have shown how the desired (syntactic) interoperability could be achieved by using policies and REL (Rights Expression Languages) translators in a distributed access control architecture based on XACML. And finally, we have presented how XACML could be used in the negotiation of access control policies. In the future, we will try to contribute on solving the lack of semantic interoperability among Social Networks. In this line, we are already studying some standardisation initiatives such as the Delivery Context Ontology (DCO) [8], the Friend Of A Friend (FOAF) project [9], and the work developed by the Policy Language Interest Group (PLING) [10].

5 Acknowledgments

This work has been partially supported by the Spanish government through the projects MCM-LC (TEC 2008-06692-C02-01) and Segur@ (Centre for the Development of Industrial Technology (CDTI), CENIT-2007 2004, under a subcontract with Safelayer Secure Communications).

6. References

1. E. Rodríguez, V. Rodríguez, A. Carreras, J.Delgado, "A Digital Rights Management approach to privacy in online social networks", in Proc. of the 1st Workshop on Privacy and Protection in Web-based Social Networks (within ICAIL '09), Barcelona, Spain, June 2009. IDT Series, vol. 6, ISSN 2013-5017.
2. V. Rodríguez, A.Carreras, E. Rodríguez, J. Delgado, "Applications to improve privacy on online social networks", in Proc. of the First Workshop on Law and Web 2.0, Antoni Roig (ed.), September 2009.
3. X. Maroñas, E. Rodríguez, J. Delgado, "An architecture for the interoperability between rights expression languages based on XACML", in Proc. of the 5th International ODRL Workshop (within Virtual Goods' 09), Nancy, France, September 2009, ISBN: 978-2-905267-69-6.
4. A. Carreras, J. Delgado, E. Rodríguez, R. Tous, "The Impact of Contextual Information on User Privacy in Social Networks", in Proc. of the 1st Workshop on Privacy and Protection in Web-based Social Networks (within ICAIL '09), Barcelona, Spain, June 2009. IDT Series, vol. 6, ISSN 2013-5017.
5. T. Moses (Ed.): eXtensible Access Control Markup Language (XACML) Version 2.0, Feb. 2005. [Online]. Available: http://docs.oasis-open.org/xacml/2.0/access control- xacml-2.0-core-spec-os.pdf.

6. W3C Workshop on Access Control Application Scenarios, 17-18 November 2009, Luxembourg. [Online] Available: http://www.w3.org/2009/policy-ws/.
7. International Standards Organisation. Information technology – Multimedia Framework (MPEG-21) – Part 5: Rights Expression Language. ISO/IEC 21000-5:2004.
8. Delivery Context Ontology (DCO). W3C Working Draft 16 June 2009. [Online]. Available: http://www.w3.org/TR/2009/WD-dcontology-20090616/.
9. The Friend of a Friend (FOAF) Project. [Online]. Available: http://www.foaf-project.org/.
10. W3C Policy Language Interest Group (PLING). [Online]. Available: http://www.w3.org/Policy/pling/wiki/Main_Page.