Using XACML for access control in Social Networks

Anna Carreras, Eva Rodríguez, Jaime Delgado

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

In our previous works, we have analyzed current privacy policies of the most relevant social networks, and identified the different elements of Digital Rights Management systems that could be used in this application scenario [1]. Furthermore, two different implementations of those policies, one based on the MPEG-21 Rights Expression Language (REL) [2] and the other one based on the eXtensible Access Control Markup Language (XACML) [3], have been presented and analyzed [4]. Finally, in line with the previous research activities, a possible architecture for the interoperability of rights expression languages based on XACML has been designed [5]. Furthermore, other relevant work in the protection of contextual information in context-aware content adaptation systems has been developed within the Visnet II NoE project [6]. In this line, the effects on user privacy have been analyzed, and a possible privacy model for Social Networks application scenario has been presented in [7].

From all this work, 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. XACML) 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, there is not yet a common standard format to describe this Social Network's context, and thus, there is a clear lack of interoperability at a semantic level.

Furthermore, 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 when thinking, for example, about the cloud computing concept. Different applications and services using different access control policy languages need to be interoperable. But this time, the incompatibility is not between different Social Networks but 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

3.1 Interoperability with "sticky policies" based on XACML

The concept of "sticky policies" was already introduced in [8] as a requirement in Web 2.0, referring to the access policies associated to the data. We agree on the fact that using "sticky policies" would be suitable in Social Networks application scenario, but apart from being a mean of enforcing the protection of personal data, we have tried to show how they may contribute to achieve the desired interoperability amongst systems. We propose a possible architecture based on XACML 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 "sticky policies". Furthermore, the use of some translators (detailed in [5]) guarantees the interoperability between RELs without losing information.
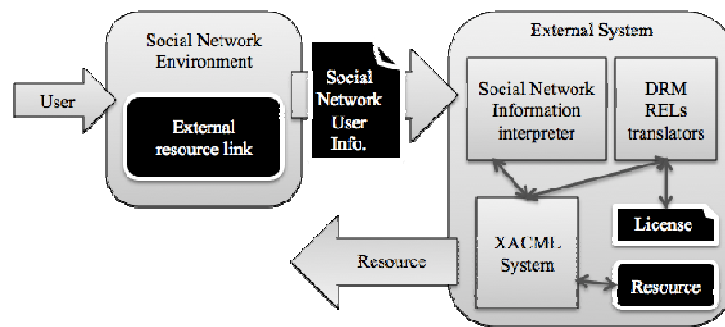
The proposed architecture is shown is Fig. 1.

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, he/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 will be past to the XACML system. This module is in charge of authorising the access, and is also detailed in [5]. 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 he/she has no rights to do that.

3.2 Negotiating the access control using XACML

As outlined in Section 2, it would be very interesting (in the Social Networks application scenario) to give the opportunity to users and service providers of negotiating 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 [2] 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.

3.3 Semantic interoperability

Our last approach tries to address the lack of semantic interoperability identified when using XACML. In our opinion, there is a clear need of a common ontology expressing the semantics of all the elements contained in access control policies.

Of course, this is not a trivial task, and requires a lot of work and time. Our idea, is to initiate it at a specific application level (i.e. Social Networks) combining the use of current existing ontologies, such as the Delivery Context Ontology [9], FOAF [10], etc. Nevertheless, from our study on the topic done so far [4], we could conclude that these existing ontologies are not enough to guarantee the desired semantic interoperability for access control, and thus, some necessary extension should also be made. The last step would be, then, to try to apply our initial ontology in other application scenarios, probably by integrating the existing ontologies of different domains in order to verify its usability and extensibility.

But we insist that this is an ambitious project that we have just initiated and will take some time to give relevant results.

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 "sticky policies" and REL (Rights Expression Languages) translators in a distributed access control architecture based on XACML. Furthermore, we have presented how XACML could be used in the negotiation of access control policies. And, finally, we have highlighted the initial steps we are taking in order to achieve the necessary semantic interoperability among systems using different policy languages.

5 Acknowledgments

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. 3, ISSN 2013-5017.
2. International Standards Organisation. Information technology – Multimedia Framework (MPEG-21) – Part 5: Rights Expression Language. ISO/IEC 21000-5:2004.
3. T. Moses (Ed.): eXtensible Access Control Markup Language (XACML) Version 2.0, Feb. 2005 http://docs.oasis-open.org/xacml/2.0/access control- xacml-2.0-core-spec-os.pdf
4. 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.
5. 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.
6. IST-1-038398 - Networked Audiovisual Media Technologies - VISNET II, "Deliverable D2.1.4: Final set of contributions on context-based content adaptation". April 2009.
7. 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. 3, ISSN 2013-5017.
8. C. E. Gates, "Access control requirements for Web 2.0 security and privacy", Position paper accepted to the Workshop on Web 2.0 Security and Privacy (W2SP) 2007, Oakland, CA, USA, May 2007.
9. Delivery Context Ontology (DCO). W3C Working Draft 16 June 2009 (See http://www.w3.org/TR/2009/WD-dcontology-20090616/.)
10. The Friend of a Friend (FOAF) Project (See http://www.foaf-project.org/.)