Secure Management of Social Networks Applications Data

Silvia Llorente, Eva Rodríguez, and Jaime Delgado

Distributed Multimedia Applications Group (DMAG),
Departament d'Arquitectura de Computadors,
Universitat Politècnica de Catalunya,
C/ Jordi Girona, 1-3, 08034 Barcelona
{silviall, evar, jaime.delgado}@ac.upc.edu
http://dmag.ac.upc.edu

Abstract. The number of users of online social networks has increased dramatically during the last years. In turn, the number of applications offered by these sites, as well as their usage by social networks users has also increased significantly. These applications, developed by third parties, access users data in order to properly work. This fact poses serious privacy risks for users, since social networking sites don't provide them mechanisms to specify their privacy preferences for the usage done by third party applications over their personal data. This paper proposes a solution based on the usage of rights expression languages to control the usage done by social networks applications of users' personal data.

Keywords: Social networks, privacy protection, access control, ODRL

1 Introduction

Current online social networking platforms give, to applications developed by third parties, access users' data. This fact poses serious privacy risks for social networks users, since third party applications can access their personal data.

Facebook [1], the most popular social network, is an example. The applications used by the users of this social network have access to their information to operate, as Facebook states. Specifically, these applications have access to the public information of the users' profile (user ID, name, email, gender, birthday, profile picture URL, current city, networks, list of friends, and pages of which you are a fan) and to the information that users have made visible "for all" when they defined their privacy preferences in their profiles.

Nowadays, different institutions, as well as European projects, have analysed the risks of social networks. Two examples are the Spanish National Institute of Communication Technologies (INTECO) [2] and the PrimeLife European Project [3]. Both have identified the possible situations of privacy risk for users of current social networks. One of the identified risks is related to the use that third party applications could make of social networks users' data. For example, this information might be exploited for commercial purposes.

This paper is organised into five parts. Section 2 provides background information on the architectures of social network platforms, focussing on the users' data flow between the social network and third party applications. Section 3 analyses privacy risks for social network users', paying special attention on those related with the usage done by third party applications of users' information. Section 4 proposes a solution, based on rights expression languages and enforcement services that overcome the privacy risks resulting of exposing users' data to third party applications. Finally, section 5 concludes the paper and outlines future research work.

2 Online Social Networks

Online social networks, such as Facebook [1], Tuenti [4] or Linkedin [5], are widely used nowadays. They allow users to create a profile and to be connected with other registered users of the network. Many social network users have integrated these sites into their daily habits, investing a great amount of time to communicate with their friends. The information shared by users of these networks is subject to privacy policies specified in each network. These privacy terms protect users to a certain extent and permit them to define privacy preferences over the information (e.g. personal data or digital contents) they share. One example is Facebook, which enables users to choose their privacy preferences (in terms of "all", "my friends" and "friends of my friends") for their profile and their contact information.

Online social networks also offer, to their users, applications developed by third parties. These applications have gained great popularity among social network users. As an example, Facebook has 550000 active applications (in May 2010). These applications access users' information to operate. For example, the restaurants guide and critics application makes use of the users' geographical location to provide them recommendations.

One of the current main concerns for users is the use that these applications make of their data. Fig. 1 shows the flow of users' data in online social networking platforms. Users share information within the social network (SN) and, afterwards, makes use of the applications available through the SN. Applications obtain users' information from the SN in order to properly work.

3 Privacy Protection in Online Social Networks Applications

Social networks users cannot explicitly choose their privacy preferences regarding applications. They cannot specify to which information third party applications can access. This fact poses serious privacy risks by making available users private data to external applications. For example, Facebook applications can access the information that users have made visible for all, as well as to the public information of their profile, which includes the user ID, name, email, gender,

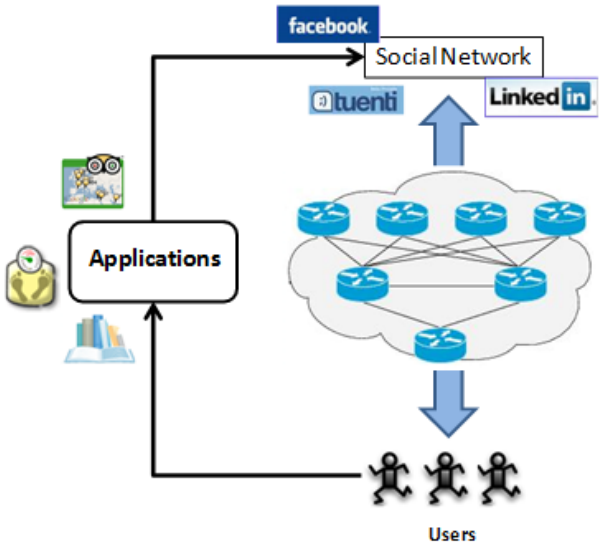

Fig. 1. Social networks and third party applications

birthday, current city, profile picture URL, and the user IDs of the user's friends who have also connected with your application, as defined in [6] as basic account information. Also fan pages are defined as basic account information by Facebook [7].

This paper proposes a solution based on the usage of licensing techniques to prevent privacy risks resulting from making accessible users' data to third party applications. The novelty of this solution lies on providing users the ability to choose their privacy preferences for the data to which third party developers will access. Social network users will control, in a very flexible way, which of their information will be available to third party applications and the usage that these applications will be allowed to do with these data. Specifically, we propose the usage of Rights Expression Languages's, as pointed out in [8], as well as policy languages, such as the eXtensible Access Control Markup Language (XACML) [9]. The work presented here makes use of the Open Digital Rights Language (ODRL) [10] to specify the access permissions to personal information of social networks users by third party applications.

Some related work can be found in the literature to protect user privacy in social networks. In [11], authors address privacy risks related to third party applications by means of anonymisation techniques. They propose a privacy-by-proxy solution to preserve users' privacy. Using this solution the social network does not provide personal data to third party applications.

Our solution is complementary to the privacy-by-proxy one, since both techniques (privacy policies and anonymisation) can be combined to provide a global

solution to enforce users' privacy preferences to third party applications. One more general solution may be to provide a social network developed using a privacy-by-design approach, instead of trying to privatise an existing social network.

3.1 Accessing User Information from Social Networks Applications

Social networks (SN) in general and Facebook in particular, are becoming to be concerned about privacy of user information transferred to external applications accessible through their environment. Although Facebook cannot control what happens with user's data after being transferred to the third party application, they want to be on the "safe side" by defining Developer Principles & Policies [6] that clearly explain (even with images and examples) how a third party application should behave in order to be trustworthy for the user. In this context, it is important for an application to be trustworthy inside the SN, as users will not only perceive it as useful or entertaining but also they can recommend it to their friends, making it more popular between SN members. In the end, the more the user stays inside the SN (directly or through the associated applications), the more the SN benefits from applications usage.

Nevertheless, current Facebook position is to put privacy responsibility on the user, giving her all options about how much she wants her data to be protected. In [12] and [13] Facebook explains how users can change privacy settings for the information managed inside Facebook and Facebook's privacy policies, respectively. These documents change frequently and usually after users' reaction against some Facebook's practices that are not accepted by them. The final result is that Facebook has solved some of the privacy problems described in [14], just to maintain their users' trust on the platform. However, not everything regarding users' privacy stated by Facebook seems to be true, as it has been demonstrated by several researchers [15] and pointed out by the Electronic Frontier Foundation [16]. So, there is still a need of protecting users' privacy even into Facebook platform.

Regarding applications and user privacy, Facebook clearly states in [17] which information is directly accessible from an application and what to do if it needs access to user's private information, either from the user or from her friends. In the first case, the application has to explicitly ask for extended permissions in order to access users' private information, for instance, user's photos. In general, the application must ask the user to give it extended permissions for any extra private information needed by it (for instance, friends' photos or friends' birthday). Again, the privacy responsibility is on the user, who can even give access to the application to most of her friends' content (see [18] for details on extended permissions). However, the permission is given by the user of the application, not by the affected friend.

So, we can raise several questions regarding SN and user's privacy and try to respond to them from our point of view after reviewing Facebook documentation regarding privacy and applications.

First question is how the SN can control that applications really behave in a trustworthy way? The response to the first question is not easy, as when data goes out from the SN, it will be difficult to control what application developers do with it. Obviously, if data obtained from the SN is used for injuring users in any way, this could be punishable and prosecuted by law. In this sense, Facebook collaborates with justice when required [19].

Another question is, does SN really want to control what applications do with users' information? Again, the response depends on users' privacy perception when using the application. In our opinion, Facebook is quite concerned about this, as it provides guidelines to application developers regarding application behaviour. However, it cannot guarantee that an application respects users' privacy as it does not know what the application does with the users' information gathered from the SN.

Our final impression is that Facebook has solved some privacy issues regarding its own platform, but there is still a need of protecting privacy when Facebook users' interact with external applications. Many Facebook's users avoid using applications offered through Facebook because they do not know what will happen with their personal data which include not only public information but also photos, videos, etc.

In the next section we present some guidelines for implementing applications that respect users' privacy accessible through Facebook. These guidelines could provide confidence to those users concerned with their privacy when using applications through Facebook. It is worth noting that it is up to Facebook's application developers to follow these guidelines (or similar ones) when implementing new applications.

4 Protecting Users' Privacy on Social Networks Applications

In this section we describe how to implement an application inside Facebook platform for those users concerned with the privacy of the information they publish on their Facebook profile. This solution could be also used in the application for the management of governed multimedia audiovisual content through Facebook proposed in [20].

Fig. 2 presents current situation regarding users' privacy settings in Facebook. At the present moment, Facebook users' can define their privacy settings using the "Privacy Settings" option of the Facebook account. Privacy settings include the visibility and access to personal information, contact information, friends and connections, searches, applications and websites and blocking lists.

If we take a closer look to the applications and websites tab, we can see it permits controlling what you share and what your friends can share about you when using external applications and websites. However, almost any information your friends can see about you (status, presence on-line, family and relationships, etc.) can be shared by them to an external application by default. Moreover, when you create a Facebook account (even with the minimum information) you are

connected to several applications with predefined privacy settings that depend on the application. For instance, the Groups application is visible to Anyone while the Photos application is only visible to Friends of friends. This gives an idea of the complexity of privacy configuration in Facebook and Facebook's applications.

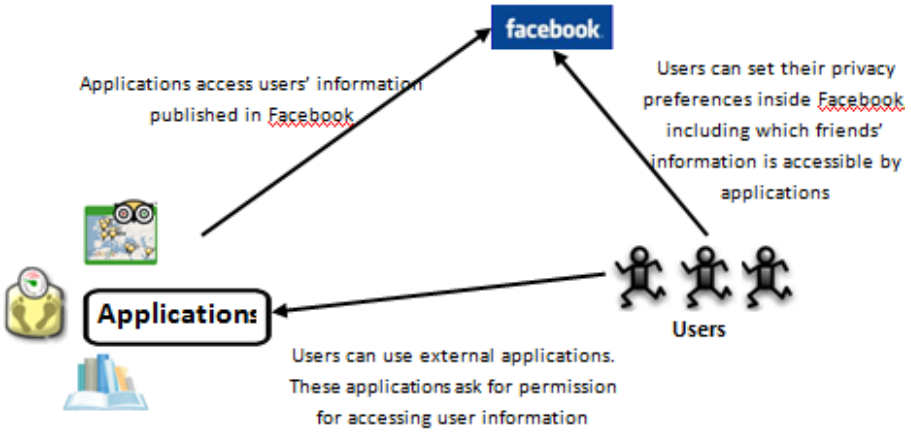

Fig. 2. Privacy on Facebook and External Applications

Apart from those predefined applications, any user can connect to other applications offered through Facebook. They are grouped into different categories like lifestyle, applications, sport, education, etc. When a user wants to connect to these applications, they ask for permission to access user information. The problem is that they do not specify neither which user information they want to access from the user's profile or why they need this information for the application to work. So, if a user is concerned with her privacy is at this point where she can decide not to use an application that does not clearly state neither which information is going to gather from Facebook nor what it is going to do with it inside (or outside) the application.

In order to solve this privacy problem, we propose using ODRL to describe which user information is accessible by an external application in Facebook. In the next subsections we are going to describe how a Facebook application should behave in order to be trustworthy to users concerned with their data's privacy and how it should use the rights expression language proposed.

4.1 Describing Access to User's Information

We propose the use of ODRL licenses for describing what an application can access from a Facebook's user profile. Fig. 3 shows an example of ODRL license

giving access to the user's birthday. Birthday is part of the basic information account accessible by default by applications, but users may be willing to control access to it. We have used version 2.0 of ODRL [21] to express the agreement, although this version is still work in progress. The license agreement consists of the assigner, the assignee, the action and the asset. The assigner represents the user of the application, which is uniquely identified by her Facebook User ID. In this example, the assigner grants to the FarmVille application the right to access to her birthday. To this end, we have defined a new right "social network application access" to allow social networks applications the access the corresponding user's information. Finally, the asset, which is the user' birthday, is identified by the birthday element of the standard user info and the assignee by its unique identifier.

```
<o:rights xmlns:o="http://odrl.net/2.0/" uid="urn:fb:500325802:003"
type="http://odrl.net/2.0/type/agreement">
  <o:permission>
    <o:asset uid="urn:facebook:500325802:birthday"/>
    <o:action resource="http://dmag.ac.upc.edu/action/social_network_application_access"/>
    <o:party uid="urn:facebook:500325802:uid" role="http://odrl.net/2.0/role/assigner"/>
    <o:party uid="urn:AppFarmVille:fc:002233998" role="http://odrl.net/2.0/role/assignee"/>
  </o:permission>
</o:rights>
```

Fig. 3. ODRL license for giving permission for accessing specific user information

4.2 Use Case: Implementing Privacy in Social Networks Application

In this subsection we describe a use case that proposes how a social network application (SN) should behave in order to respect users' privacy and clearly state which information is going to use from a user's profile.

Although we have centred our discussion on Facebook, this schema applies to any external application working through an SN. Our use case is separated into several phases. The first one, shown in Fig. 4 defines how a user asks for access to an external application. The second one, shown in Fig. 5 describes how a user makes use of the application. The third one, shown in Fig. 6, describes how the application may request some more information from the user if needed.

As shown in Fig. 4, the user wants to start using a new application through the SN (step 1). This application needs access to some user's profile information. It requests it to the user (step 2) by means of a screen where the user can check the information she wants access to be permitted. This can be seen as a registration phase, that user makes only once. User verifies the permitted information (step 3) and returns it to the application, which asks for the creation of an ODRL license to the License Service (step 4). After the license is created

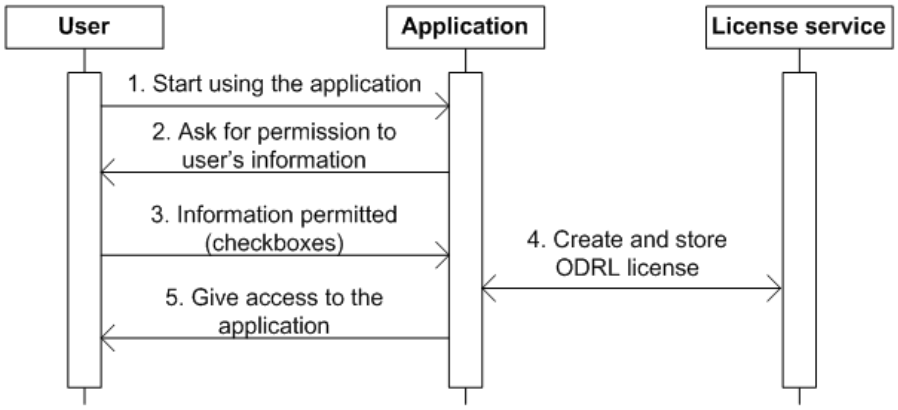

Fig. 4. Registering in the application (First access)

and stored, the application can give access to the user (step 5). The application may give partial functionalities if the information access permitted by the user is not enough to provide full access.

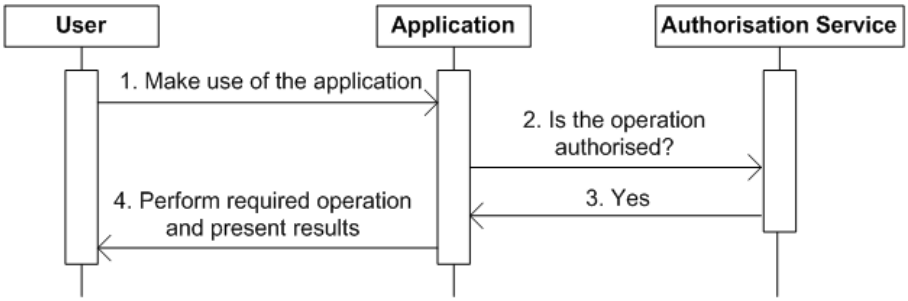

Fig. 5. Making later use of the application

Fig. 5 illustrates a later use of the application done by the user. When the user wants to perform an operation (step 1), the application asks, to the Authorisation Service, to be authorised to access user's information (step 2). In this case, the response is positive (step 3) and the user can perform the requested operation (step 4). Fig. 6 illustrates what may happen when the response to the authorisation (step 3) is negative. Steps 1 and 2 are the same in both cases.

So, when the Authorisation Service gives a negative response (step 4), the application prompts the user with a new screen asking for the permissions (access profile's information) required. User responds with the new permitted informa-

tion (if any, step 5) and a new license is created to reflect changes in permissions given (step 6). If they are enough, application gives access to the required functionality to the user (step 7). In this phase, there are some alternatives in steps 5, 6 and 7, described next. In step 5, user may not give additional permissions. In this case, steps 6 and 7 should be replaced by a new step where the application tells user not to have access to the required functionality. Step 6 should revoke old ODRL license for this user and create a new one with the newly added permissions. Step 7 depends on information permitted by user.

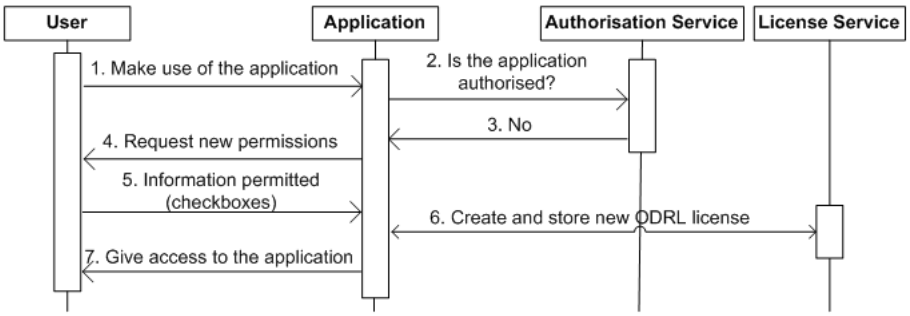

Fig. 6. Making later use of the application and asking for more permission

5 Conclusions and Future Work

In this paper we describe some of the privacy problems that social networks users' may find when using social network's applications. We have centred our discussion regarding users' privacy on Facebook, "the" social network (SN) nowadays, although most of the problems found apply to any SN. Nevertheless, privacy issues concerning Facebook have more relevance, as they are published on the news almost every day and affect millions of their users.

Facebook has updated its privacy policy [13] and also added some documentation to help users on selecting its privacy preferences [12]. However, privacy is not set at all by default (everyone can see almost everything about a user) and it is quite complex to know if you have properly defined your privacy settings for your content, applications, photos, contacts list, what information your friends can share about you with external applications, and so on. In any case, taking into account last Facebook movements, this situation may change in the next months, or even weeks.

We are concerned about this privacy breach in SN: social networks applications. These applications are not directly offered by the SN, but through it, and they request access to the user's profile information without specifying which information they are going to access and what they are going to do with it. On

the other hand, we have also found that the SN does not control at all what the applications do with their users' information, although they give some guidelines of how they should behave in front of the SN users.

In order to solve these privacy problems, we have proposed a possible solution based on the use of ODRL licenses. Using these policies expressed as licenses, SN applications could clearly know which information they are going to access from users and request for authorisation of access when needed. To demonstrate how this solution could be implemented, a use case has been presented, giving the building blocks of such an application. Obviously, it is up to the SN to implement such a solution for providing privacy to their users.

This paper opens a new line of research for us, considering how privacy could be integrated into current social networks design, especially on the external applications access to users' information. However, what we consider more relevant from the research point of view is to describe how an SN should be implemented following the privacy-by-design principle, where all the SN structure is implemented to preserve users' privacy from the beginning.

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).

References

1. Facebook, http://www.facebook.com/
2. Communication Technologies National Institute (INTECO), "Study on the Privacy of Personal Data and on the Security of Information in Social Networks", December 2009.
3. PrimeLife Project, http://www.primelife.eu/
4. Tuenti, http://www.tuenti.com/
5. Linkedin, http://www.linkedin.com/
6. Facebook Third Party Applications' Developer Principles & Policies, http://developers.facebook.com/policy/. May 2010
7. Facebook FAQ regarding public information, http://www.facebook.com/help/?faq=16374
8. Carreras, A., Rodriguez, E., Delgado, J., Maroñas, X., "Access Control Issues in Social Networks". WISMA 2010, CEUR-WS Vol. 583. May 2010.
9. eXtensible Access Control Markup Language (XACML) V2.0, http://www.oasis-open.org/specs/index.php#xacmlv2.0
10. Open Digital Rights Language (ODRL) , http://odrl.net
11. Felt, A., Evans, D., "Privacy Protection for Social Networking Platforms". Web 2.0 Security and Privacy Workshop. Oakland, California. May 2009.
12. A Guide to Privacy on Facebook, http://www.facebook.com/privacy/explanation.php. May 2010.

13. Facebook's Privacy Policy, http://www.facebook.com/policy.php. April 2010.
14. Rodríguez, E., Rodríguez, V., Carreras, A., Delgado, J., "A Digital Rights Management approach to privacy in online social networks", Workshop on Privacy and Protection in Web-based Social Networks (within ICAIL '09), Barcelona, June 2009.
15. Krishnamurthy, B., Wills, C.E, "On the Leakage of Personally Identifiable Information Via Online Social Networks" http://conferences.sigcomm.org/sigcomm/2009/workshops/ wosn/papers/p7.pdf. August 2009.
16. Electronic Frontier Foundation. "Facebook Violates Privacy Promises, Leaks User Info to Advertisers", http://www.eff.org/deeplinks/2010/05/facebook-privacy-promises. May 2010.
17. Applications Authentication, http://developers.facebook.com/docs/authentication May 2010.
18. Extended Permissions, http://developers.facebook.com/docs/authentication/permissions/. May 2010.
19. Electronic Frontier Foundation, "EFF Posts Documents Detailing Law Enforcement Collection of Data From Social Media Sites", http://www.eff.org/deeplinks/2010/03/eff-posts-documents-detailing-law-enforcement. March 2010.
20. Maroñas, X., Rodríguez, E., Delgado, J., "An architecture for the interoperability between Rights Expression Languages based on XACML", Proceedings of the 7th International Workshop for technical, economic and legal aspects of business models for virtual goods, Virtual Goods 2009, September 2009.
21. Ianella, R., "ODRL V2.0 - XML Encoding", Open Digital Rights Language Initiative (ODRL Initative), February 2010.