User’s Privacy in Applications provided through Social Networks

Jaime Delgado, Eva Rodriguez, Silvia Llorente
Distributed Multimedia Applications Group
Dept. Arquitectura de Computadors
Universitat Politecnica de Catalunya
C/ Jordi Girona, 1-3, 08034 Barcelona
jaime.delgado@ac.upc.edu, evar@ac.upc.edu, silviall@ac.upc.edu

ABSTRACT
The number of users of social networks (SN) has increased dramatically during the last years. In turn, the number of applications offered by SNs, as well as their usage by SN users, has also increased significantly. These applications are developed by third parties and access users’ data to operate. This fact poses serious privacy risks, since SNs do not provide mechanisms to specify users’ privacy preferences for the usage done by third party applications over their personal data. This paper proposes a solution based on the usage of access control languages to keep track of the usage done by SN applications of users’ personal data.

Categories and Subject Descriptors

General Terms
Security, Standardization, Languages.

Keywords
Social networks, privacy protection, access control, applications.

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

Facebook [1], the most popular SN, is an example. Facebook states that applications used by their users have access to their information to operate. Specifically, these applications have access to the basic information account 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) [2] and to the information that users have made visible “for all” when they defined their privacy preferences in their profiles.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.

WSM’10, October 25, 2010, Firenze, Italy.
Copyright 2010 ACM 978-1-4503-0173-2/10/10...

Nowadays, different institutions, as well as European projects, have analyzed the risks of social networks. Two examples are the Spanish National Institute of Communication Technologies (INTECO) [3] and the PrimeLife European Project [4]. 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 organized into five parts. Section 2 provides background information on the architectures of social network platforms, focusing 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 to those related with the usage done by third party applications of users’ information. Section 4 proposes a solution, based on access control languages and enforcement services, that overcomes 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 [5] or LinkedIn [6], 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 55000 active applications (in June 2010). These applications access to users information to operate. For example, the restaurants guide and critics application makes use of the users’ information. The information might be exploited for commercial purposes.

One of the current main concerns for users is the use that these applications make of their data. Figure 1 shows the flow of users’ data in online social networking platforms. Users share information within the social network (SN) and, afterwards, access to the applications available through the SN. Applications obtain users’ information from the SN in order to properly work.
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 policy languages, such as the eXtensible Access Control Markup Language (XACML) [8] 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 [10], authors address privacy risks related to third party applications by means of anonymization 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 anonymization) 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 privatize an existing social network.

4.1 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 [2] 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 seems to be to put privacy responsibility on the user, giving her all options about how much she wants her data to be protected. In [11] and [12] 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 [13], 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 [14] and pointed out by the Electronic Frontier Foundation [15]. So, there is still a need of protecting users’ privacy even into Facebook platform.

Regarding applications and user privacy, Facebook clearly states in [16] 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 to 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 [17] 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 this 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 [18].

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.

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, although your privacy settings regarding applications should be considered. 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.

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, it 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 XACML 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 policy language proposed.

5. PROTECTION OF PRIVACY IN 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 that we proposed in [19].

Figure 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.

Figure 2. Social networks and third party applications.

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.

5.1 Describing Access to User’s Information

We propose the use of XACML policies for describing what an application can access from a Facebook’s user profile. To this end, we are implementing a web application where users can chose their privacy preferences regarding to applications. Figure 3 shows the proposed solution, which enables users to chose their privacy preferences stating if applications are allowed or not to access or use their personal data (e.g. family, relationships, etc.), as well as their digital assets (e.g. photo albums, videos, etc.).
The privacy preferences initially stated by the users apply to all the Social Network applications. Users can express their privacy preferences in terms of allow/deny access and allow/deny usage. However, if an application needs to access or use some of the user data in order to properly operate, but it does not have permissions to do so, a message, like the one sketched in Figure 4, will be shown to the user in order to request her for permission. It is worth noting that current SNs applications request permission for access/usage all the user data although it is not necessary for their normal operation.

In order to express the allow access permission, we have defined a new action social_network_application_access to permit social networks applications the access to the corresponding user’s information. Figure 5 shows an example of XACML policy file giving access to the user’s birthday, part of the basic information account (that is accessible by default by applications), that users may be willing to control access to.

Figure 4. Permission access application request message

```
<xacml:Policy PolicyId="urn:fc:ap:policyid:008891"
  RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:deny-overrides">
  <xacml:Description> Third party application access control policy </xacml:Description>
  <xacml:Target/>
  <xacml:Rule RuleId="urn:oasis:names:tc:xacml:2.0:example:ruleid:1" Effect="Permit">
    <xacml:Description>FarmVille application can access to user 00325802 birthday</xacml:Description>
    <xacml:Target>
      <xacml:Subjects>
        <xacml:Subject>
          <xacml:SubjectMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
            <xacml:AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
              urn:AppFarmVille:fc:002233998
            </xacml:AttributeValue>
            <xacml:SubjectAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id" DataType="http://www.w3.org/2001/XMLSchema#string"/>
          </xacml:SubjectMatch>
        </xacml:Subject>
      </xacml:Subjects>
      <xacml:Resources>
        <xacml:Resource>
          <xacml:ResourceMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
            <xacml:AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
              urn:fb:us:00325802.rdf
            </xacml:AttributeValue>
            <xacml:ResourceAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:2.0:resource:target-namespace" DataType="http://www.w3.org/2001/XMLSchema#string"/>
          </xacml:ResourceMatch>
        </xacml:Resource>
      </xacml:Resources>
      <xacml:Actions>
        <xacml:Action>
          <xacml:ActionMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
            <xacml:AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
              social_network_application_access
            </xacml:AttributeValue>
            <xacml:ActionAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id" DataType="http://www.w3.org/2001/XMLSchema#string"/>
          </xacml:ActionMatch>
        </xacml:Action>
      </xacml:Actions>
    </xacml:Target>
  </xacml:Rule>
</xacml:Policy>
```

Figure 5. XACML policy file for giving access to user information
5.2 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. To do so, we propose the use of several services that form part of DMAG’s Multimedia Information Protection and Management System (MIPAMS) [20], an architecture implemented by DMAG [21] in the context of several research projects.

Although we have centered our discussion on Facebook, this schema applies to any external application working through a SN. Our use case is separated into several phases. The first one, shown in Figure 6, describes how a user asks for access to an external application. The second one, shown in Figure 7, describes how a user makes use of the application. The third one, shown in Figure 8, describes how the application may request some more information from the user if needed.

As shown in Figure 6, 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 to the user (step 2) which information she wants to be permitted (showing checkboxes or a similar mechanism). This can be seen as a registration phase, that the user makes only once. User verifies the permitted information (step 3) and returns it to the application, which asks for the creation of an XACML policy to the Policy Service (step 4). After the policy is created 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.

So, when the Authorization Service gives a negative response (step 3), the application asks the user for the permissions (access to profile’s information) required (step 4). User responds with the new permitted information (if any, step 5) and a new policy file 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 XACML policy for this user and create a new one with the newly added permissions. Step 7 depends on information permitted by user.

In the use case presented, we are using the XACML Authorisation Service and XACML Policy Services from MIPAMS. These modules are currently under development, but they will be based on the existing Authorisation and License Services that implement MPEG-21 Rights Expression Language (MPEG-21 REL) [22] authorization mechanism and license creation, respectively.

6. CONCLUSIONS AND FUTURE WORK

In this paper we have described some of the privacy problems that social networks users may find when using applications provided through social networks. We have centered 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 their millions of users.

Facebook has updated its privacy policy [11] and also added some documentation to help users on selecting its privacy preferences [10]. 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 XACML policy files. Using
these policies, SN applications could clearly know which information they are going to access from users and request for authorization 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, MIPAMS. Obviously, it is up to the SN to implement such a solution for providing privacy to their users.

We have made some tests implementing an application provided through Facebook. When a user accepts using this application, she is giving access to all the information that Facebook manages about her (personal information, contact list, etc.). Making such a test, we have realized that privacy needs to be given by Facebook, which should control access to its users’ information (both from applications or users). So, the SNs should be concerned with their users’ privacy and provide means to preserve it.

This paper opens new lines of research for us, considering how privacy could be integrated into current social networks design. We have centered our discussion on the external applications access to users’ information, making use of an existing architecture, MIPAMS, which has to be augmented with some new services to support XACML. However, what we consider more relevant for the future 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. In this sense, MIPAMS is also a good starting point to protect and govern user’s information in order to provide privacy to SN users. We are planning the preparation of some real tests in order to determine the feasibility of the solution presented.

7. 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).

8. REFERENCES