Available online at www.sciencedirect.com

ScienceDirect

Procedia Technology 9 (2013) 405 – 410

Procedia Technology

CENTERIS 2013 - Conference on ENTERprise Information Systems / PRojMAN 2013 - International Conference on Project MANagement / HCIST 2013 - International Conference on Health and Social Care Information Systems and Technologies

Improving content privacy on social networks using open digital rights management solutions

Joaquim Marques[a], Carlos Serrão[b,]*

[a]*IPCB/EST, Av. do Empresário 6000-787, Castelo Branco, Portugal*
[b]*ISCTE-IUL/ADETTI-IUL, Av. das Forças Armadas, 1649-026, Lisboa, Portugal*

Abstract

Among Internet users, the social networks have gained a huge popularity. Millions of users are part of some online social network in order to share their own experiences and content with others. Documents, videos, music and pictures are among some of the most shared content types online, relying on the privacy and security controls that are offered by the social network platform. In this equation, the end-user has little control, resulting in serious privacy concerns – once content is shared on the social network, is out of end-user hands and they cannot enforce their own privacy rules.
A different approach for social networks shared content privacy is proposed in this paper - centered on the user and not on the social network platform. To ensure this, an architecture based on an open rights management platform is presented. This architecture will enforce the necessary security and privacy mechanisms extending the original controls provided by the social network platform. That way, users will be able to control the disclosure and protection of their content, even when they are no longer part of the social network (because they have deleted or suspended their accounts).

Keywords: social networks; privacy; security; user-generated content; rights management systems.

* Corresponding author. Tel.: +351 272 339 300; fax: +351 272 339 399.
E-mail address: carlos.serrao@iscte.pt.

doi:10.1016/j.protcy.2013.12.045

1. Introduction

Social networks are currently among the most popular services the Internet has to offer. These services are attractive to users because they allow communication with new persons and concede users the ability to expose their own network of friends to others. This permits the creation of pairings that otherwise would not be possible [1] and helps creating virtual relations between multiple users and content. Social networks allow users to share different types of content. Users take advantage of this functionality to share all kinds of digital content within the social network, with other users (either they are their direct contacts or they are other one's connections). These social network-sharing functionalities are extremely powerful and engaging of further social interaction. However, they are at the same time, the cause of serious privacy and security problems because sharing control is not on the end-user side. This represents a serious threat to the user privacy since content shared in these platforms can easily be exposed to a wider audience in just a few seconds [2]. It is difficult, for an ordinary user, to select specific sharing properties for the content placed in social network and ensure that it stays under its control. In this article, the authors present the concept and the architecture proposed to lay the control of shared content on the user-side that would improve user control over content shared over social networks.

2. User-centric social network content privacy control

Why users cannot control their own content? One of the major contributions of this work consists in the paradigm shift with regard to the privacy of social networks users, empowering social networks users on the control and safeguard of its privacy, passing the content sharing control the end-user side, using open rights management systems. The proposed approach follows the path of creating a mechanism that protects the shared content on the social network platform and that provides the content sharing and access control to the end-user. Some other authors also uphold the same approach [16], where rights management systems and social platforms are used together to improved the user content privacy.

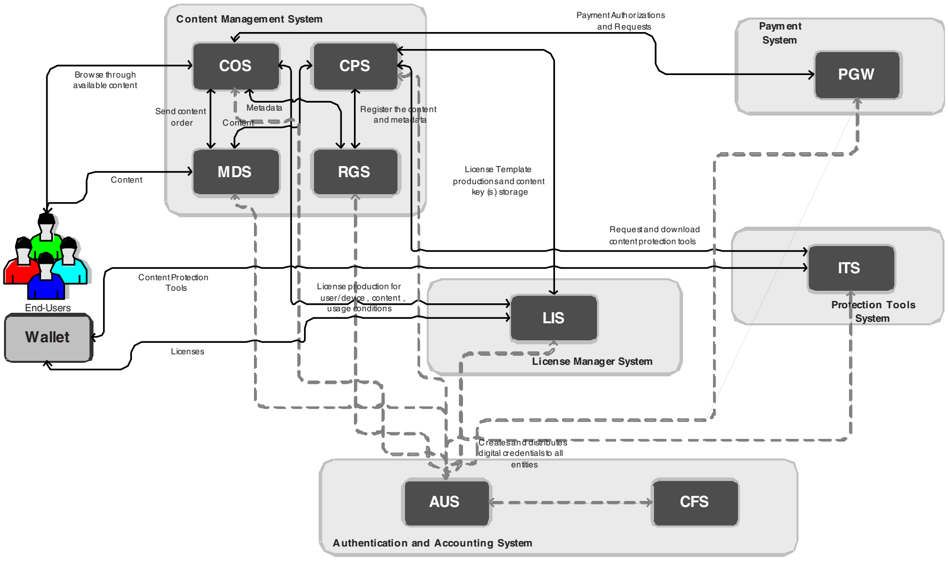
Content Management System
COS
CPS
MDS
RGS
Browse through available content
Send content order
Metadata
Content
Register the content and metadata
Content
End-Users
Wallet
Content Protection Tools
License production for user/device, content, usage conditions
Licenses
Payment Authorizations and Requests
Payment System
PGW
License Template productions and content key (s) storage
Request and download content protection tools
ITS
Protection Tools System
LIS
License Manager System
Creates and distributes digital credentials to all entities
AUS
CFS
Authentication and Accounting System

Fig. 1. General architecture of the OpenSDRM platform

The proposed architecture is based on a generic rights management framework and platform called OpenSDRM. The Open and Secure Digital Rights Management system (OpenSDRM) [8] is an adaptable DRM architecture [16]. This architecture can be configured for use with several business models and different types of content. OpenSDRM deploys a traditional DRM solution for content rights protection and can be applied for publishing and trading of digital multimedia content (Fig. 1) [9]. This OpenSDRM has already been described on other scientific papers [10][11][12][13], however it is important to notice that to its modularity and openness it can easily be adapted for other scenarios. This modularity is achieved through a set of independent components that are implemented using a service-oriented approach. For the purpose of this paper, and for the implementation scenario at hand, some of the OpenSDRM components have a bigger importance. Also, on the client-side (user-side) it was implemented a specific browser extension that allows the social network user to register on the OpenSDRM platform, upload content to the platform that he wants to share online, define the access control rules for all the other registered users to access the published content, and mediate the access to the content, allowing it to be rendered at the social network. The following sections of this paper will describe the system and the interaction between the different components in order to achieve its objectives. First of all, it is important to make some previous notes and assumptions: (a) all the components of the platform are trustworthy, have not been tampered and behave exactly as expected, (b) all the components exchange messages through a secure and authenticated channel. Every component has its own key-pair that is used to establish this channel: $K_{pub}^{Component}$, $K_{priv}^{Component}$ and (c) all the components that compose the framework (or a subset of the framework, depending on the implemented scenario) are registered on the AUS and have a valid AUS credential: $Cert^{AUS}_{Component}$.

2.1. User registration on the platform

To use the OpenSDRM system the users need to be registered. User registration on the system is performed through a specific developed browser extension that the user obtains and installs on the web browser. In the OpenSDRM framework, the “Wallet” represents this. The Wallet is responsible for handling important user information and for managing the licenses that mediate the shared content access. When the user starts the browser extension by the first time, the user registration process begins: (1) the Wallet creates a key-pair for the user: K_{pub}^{U}, K_{priv}^{U}; (2) the user creates a passphrase for the Wallet. This passphrase is hashed, resulting in a storage key that will be used to create a secure repository database: $K_{SecureStorage} = SHA1(passphrase)$. K_{priv}^{U} is securely stored. The passphrase is not stored anywhere and is known only by the user; (3) the Wallet requests some additional information from the end-user, confirming the email address of the user, and sends it to the AUS component: $K_{pub}^{AUS}\{U_{ID}$, user information + $K_{pub}^{U}\}$; finally (4) the AUS confirms the user registration and issues a credential to the User, confirming the registration: $Cert^{AUS}_{U}$. This credential is used to authenticate the User to the other services on the OpenSDRM framework. After this process is concluded, the User can start sharing content on the social network, using the OpenSDRM services to preserve its security and privacy.

2.2. Sharing content through the platform

This is one the most important functionalities on the system, that allows a registered user to share the content with others on a social network platform. The major difference between the content sharing functionalities on a normal social network and OpenSDRM is that the second puts the user in total control of what it shares with whom. In order to share content on a specific social network platform, the user uses the OpenSDRM from the browser extension that is installed:

- The user selects the proper browser extension. If the user has not yet initiated its session on the system, or if the session has already expired, it has to enter its login information and the secret passphrase;

- The system validates also the user through the OpenSDRM component, AUS. If the user has the appropriate credentials and is authenticated in the system, it initiates the session.

Imagine that the user whishes to share a picture with some specific friends through a social network site. The user will start by uploading the content to the OpenSDRM platform:

- The user uploads the content (Content) to the OpenSDRM through the MDS (Media Delivery Service). Additionally the user also fills some metadata (Metadata) that will describe the content the user is uploading;
- The Content is uploaded to the CPS (Content Preparation Service). The CPS is responsible for preparing the content to be shared on the social network platform. This may include content re-packaging, scrambling and protection. Depending on the protection method used, the content can be protected in several manners. For simplicity purposes, the authors consider that the content is encrypted;
- Depending on the protection mechanism applied, the CPS may need to obtain the appropriate protection tools to apply (if it doesn't have those yet). In order to do that, the CPS contacts the ITS (Protection Tools Service) and downloads the appropriate tools;
- The CPS contacts the RGS (Registration Service) and registers the content and the content metadata. The RGS assigns a unique registration identifier (CID) to the content and returns it to the CPS, signing it: KpubCPS{KprivRGS[CID]};
- The CPS creates a content key (CEK) that is used to cipher the content uploaded by the user. This CEK is sent to the LIS (License Service) together with the content identifier: KpubLIS{KprivCPS[CEK, KprivRGS[CID]]};
- The CPS protects the user content, ciphering it using the protection tools selected and the CEK: CEK{Content}. The result is returned to the MDS in conjunction with the unique content identifier: KpubMDS{KprivCPS[KprivRGS[CID]]}, KprivCPS[CEK{Content}]. The MDS stores the protected content;
- The MDS then creates a special URL that contains the unique content identifier and returns it to the end user. That URL is a global shortcut to the governed content placed in the OpenSDRM platform.

The content that was uploaded by the user is now stored, protected and governed by the OpenSDRM platform. The user can use the resulting URL to share on the social network platform, using the sharing mechanisms provided by the platform. In fact, the user can even share everything publicly on the social platform, since those sharing mechanisms will always be override by the OpenSDRM sharing mechanisms. In the following section, the OpenSDRM sharing mechanisms will be presented. The flexibility of the OpenSDRM sharing will be used to share the content with others.

2.3. Defining the sharing rules

Sharing is one of the most important parts in the system. It allows the end user to define how the shared content is going to be used and who can access it. When the user uploads content to the OpenSDRM platform, an interface allows him to define how the content can be used. The result from this operation is that a license is produced and it is tied to the content placed under OpenSDRM governance. These licenses are used to support the expression of rights over the content. Therefore, when the user uploads content to the OpenSDRM platform, and following the sequence of operations that were described in the previous paragraph, the subsequent steps are taken place:

- The CPS contacts the LIS and requests a list of available license templates. A license template is an XML-formatted document (using a specific format) that contains the definition of a specific rights expression case. The template contains customizable fields that can be adapted to specific rights situations;

- The license templates are presented to the end-user through the MDS, in a form, and the user can select the one that is more appropriated to its case. If the user feels that the license templates presented are not enough, then the systems offers the opportunity for the user to define its own license template;
- A typical license template for this scenario would be composed by following elements: (a) User ID (UID), Multiple Users ID (UID1..UIDn), Group ID (GID) representing the unique identifier(s) of the persons/users with whom the content will be shared with. In this case, the content can be shared with a single specific user, with several users, or with a group that was previously established by the user; (b) Content unique identifier (CID): this is the unique identifier obtained in the previous steps from the RGS; (c) Number of visualizations (Condition1..Conditionn): this is a component of the license that, if present, will limit the number of visualizations of the content, by the user or group or users; (d) Validity date (Validity): if present, this element will define the period of time during which the license is valid; (e) Content encryption key(s) (CEK1..CEKn): this element is the content encryption key that was used to protect the content (depends on the protection method that was used). The content encryption key is protected with the public-key of the user (KpubU{CEK1..CEKn}); and the (f) License signature: the contents of the license are signed by the LIS: License = KprivLIS[UID|UID1..UIDn|GID, CID, Condition1..Conditionn, Validity, CEK1..CEKn, KpubU{CEK1..CEKn}].
- The user creates the license with the appropriated parameters and that license is stored on the LIS. Therefore, the content uploaded to the platform is bounded by the conditions defined by the end-user in this license.

2.4. Accessing content

After a user has shared some content on the social platform governed by OpenSDRM, the user on the social network shares the URL returned by MDS. The user places the URL on the share box and selects the social network sharing options (the sharing can be public on the social network, since the permissions are overridden by OpenSDRM). The user, registered on the OpenSDRM platform, and with the proper browser extension installed, is browsing through the available posts and content on the social network. Whenever the browser extension detects a special OpenSDRM-ready URL (representing some type of governed content) or if the user explicitly selects one of these URL.

The User authenticates on the system through the browser extension. While pressing the URL, the browser extension checks if the user already has some licenses for the content identifier (C_{ID}) represented by the URL. If a license exists on the system: (a) The extension checks the license contents, validating the license digital signature (using the K_{pub}^{LIS}), and verifies the C_{ID}; (b) If the C_{ID} is the right one, the Validity is checked and the conditions ($Condition^1..Condition^n$) are analysed; (c) If the conditions are met content is deciphered. The CEK is retrieved from the license ($K_{priv}^U\{\ K_{pub}^U\{C_{EK}^1..C_{EK}^n\}\}= C_{EK}^1..C_{EK}^n$) and used to decipher the content ($C^{EK}\{Content\}$); (d) Content is rendered on the page on the social network. The content is rendered while the license conditions are met.

If the user browser still does not have a valid license for the C_{ID} that it is trying to view, the following operations take place: (a) The MDS contacts the LIS, passing the U_{ID}, the respective user AUS credentials ($Cert^{AUS}{}_U$) and the C_{ID}: $K_{pub}LIS\{K_{priv}{}^{MDS}[U_{ID}, Cert^{AUS}{}_U, C_{ID}]\}$; (b) The LIS receives and validates the information sent by the MDS. Using the U_{ID} and C_{ID} the LIS verifies the existence of a License and returns the license to the user through the MDS and the browser extension; (c) The license is securely stored by the browser extension: $K_{SecureStorage}\{License\}$; (d) The extension checks the license contents, validating the license digital signature (using the K_{pub}^{LIS}), and verifies the C_{ID}; (e) If the C_{ID} is the right one, the Validity is checked and the conditions ($Condition^1..Condition^n$) are analysed; (f) If the conditions are met, the content is deciphered. The CEK is retrieved from the license ($K_{priv}^U\{\ K_{pub}^U\{C_{EK}^1..C_{EK}^n\}\}= C_{EK}^1..C_{EK}^n$) and used to decipher the content ($C^{EK}\{Content\}$); (g) Content is rendered on the page on the social network. The content is rendered while the license conditions are met. Every time the user renders the OpenSDRM content on the social network page, the license validation occurs to validate if the user is not violating the conditions established by the sharing user.

3. Conclusions and Future Work

Major social network sites offer limited content sharing control options to their users [3][5][6][7]. Sharing options are social network centric while they should be user centric. Although current social network depend on the user-generated content to implement their own business models, it is important to draw a frontier between the willingness of the user to share the content with others, and the complete loss of control of that content. It is clear that the present model puts in the "hands" of the social platform the complete control of the user's content. This lack of user control, represents most of the times the most serious attacks to the user privacy, on what concerns the lifetime and sharing of user-generated content [4][14][15]. Therefore it is important to find the appropriate balance between the social platform dependency on user generated content and the user right to control the dissemination and usage of its content.

The proposed solution can help achieve such balance, presenting an alternative to user content privacy management offering the user a better user content privacy control that overrides the privacy offered by the social network platforms. OpenSDRM is an example of the usage of open rights management solution to govern user-generated content on multiple social networks.

References

[1]. Boyd, D. M., & Ellison, N. B. (2008). Social Network Sites: Definition, History and Scholarship. Journal of Computer-Mediated Communications 13, 210-230.

[2]. Beye, M., Jeckmans, A., Erkin, Z., Hartel, P., Lagendijk, R. & Tang, Q. (2010). Privacy in Online Social Networks. University of Twente Publications.

[3]. Facebook: Data Use Polity. (23 September 2011). Obtained in 12 March 2012, from Facebook: https://www.facebook.com/about/privacy/

[4]. Boyd, D., Golder, S., & Lotan, G. (2010). Tweet, Tweet, Retweet: Conversational Aspects of Retweeting on Twitter. Hawaii International Conference on System Sciences, 1-10.

[5]. Twitter Privacy Policy. (23 June 2011). Obtained in 13 March 2012, from Twitter: https://twitter.com/privacy

[6]. Google Plus: Overview. (2011). Obtained in 15 March 2012, from Google Plus: http://www.google.com/intl/en-En/+/learnmore/

[7]. Google Plus: Privacy Policy. (1 March 2012). Obtained in 15 March 2012, from Google Plus: http://www.google.com/intl/en-En/policies/privacy/

[8]. OpenSDRM web-site, http://www.opensdrm.org, as visited in March 2010

[9]. OpenSDRM specifications, "OpenSDoRM API Specification", 2007

[10]. Serrão C., Dias M., Delgado J., "Using Service-oriented Architectures towards Rights Management interoperability", in Proceedings of the International Joint Conferences on computer, Information and Systems Sciences and Engineering (CISSE06), University of Bridgeport, USA, 4-14 December, 2006

[11]. Serrão C., Siegert G., "Open Secure Infrastructure to control User Access to multimedia content", in Proceedings of the Second International Workshop on Security In Information Systems (ICEIS2004-WOSIS2004), Porto, Portugal, 13 April, 2004

[12]. Serrão C., Neves D., Kudumakis P., Barker T., Balestri M., "OpenSDRM – An Open and Secure Digital Rights Management Solution", in Proceedings of the IADIS International Conference e-Society 2003, Lisboa, Portugal, 3-6 June, 2003

[13]. Torres V., Serrão C., Dias M., Delgado J., "Open DRM and the Future of Media," IEEE MultiMedia, vol. 15, no. 2, pp. 28-36, Apr.-June 2008, doi:10.1109/MMUL.2008.38, ISSN 1070-986X

[14]. Sengupta, S., "F.T.C. Settles Privacy Issue at Facebook", The New York Times, November 29 2011, http://www.nytimes.com/2011/11/30/technology/facebook-agrees-to-ftc-settlement-on-privacy.html, as visited in November 2012

[15]. Vaknin, S., "Five ways Google's unified privacy policy affects you", C|net, March 2012, http://howto.cnet.com/8301-11310_39-57388626-285/five-ways-googles-unified-privacy-policy-affects-you/, as visited in February 2013

[16]. J. Delgado, E. Rodríguez, S. Llorente, "User's privacy in applications provided through social networks", in 2nd ACM Workshop on Social Media, 2010