Computer Networks 75 (2014) 531–543

Contents lists available at ScienceDirect

Computer Networks

journal homepage: www.elsevier.com/locate/comnet

Distributing privacy policies over multimedia content across multiple online social networks

Constantinos Patsakis [b,*], Athanasios Zigomitros [b,c], Achilleas Papageorgiou [b], Edgar Galván-López [a]

[a] Distributed Systems Group, School of Computer Science & Statistics, Trinity College, College Green, Dublin 2, Ireland
[b] Department of Informatics, University of Piraeus, Greece
[c] Institute for the Management of Information Systems, "Athena" Research Center, Greece

ARTICLE INFO

Article history:
Received 15 November 2013
Received in revised form 18 July 2014
Accepted 11 August 2014
Available online 5 October 2014

Keywords:
Social networks
Digital watermarks
Identity theft
Privacy

ABSTRACT

Online Social Networks (OSNs) are currently playing a crucial role in our everyday social life. Their great growth has sparked the interest of hackers and individual users that try to disclose as much information as possible, which in many cases unfortunately is possible. In such events, the users' privacy settings are bypassed by the leakage of their shared media content. To address this challenging but important research problem, we introduce a new distributed scheme for media content sharing on online social networks that may minimize users' privacy exposure, through automated procedures. The novelty of the proposed scheme is the ability to enforce a user's privacy policies across multiple online social networks, even if she is not subscribed to all of them, without using a trusted third party. Moreover, the proposed framework is a step towards enabling OSNs to interact, exchange information with equal rights, independently of their size, focus and underlying infrastructure.

1. Introduction

In the web based interconnected world, the processing, storage and distribution of users' data consist of very sensitive area. Web communities, companies or even governments try to provide more secure and privacy oriented services and regulate such services. Millions of users worldwide share, everyday, huge amounts of private information through blogs, wikis, Online Social Networks (OSNs) and more social media applications. The technological advantages in big data storage, cloud computing, semantic web, mobile services and other fields, facilitate the design and development of new social web services.

Social media platforms like Facebook, Google+, Twitter and LinkedIn have completely changed people's behavior on the web. Simultaneously, new social media like Pinterest and Instagram highlight that multimedia sharing, more precisely images, either personal or computer generated, are a modern niche market with huge revenues for the service providers. Without any doubt, the biggest part of the shared information within social media is multimedia content, uploaded and shared by their users. Nevertheless, the provided security and privacy is often questioned [14,24,27,29].

Many of the privacy risks that a user's privacy is exposed to stem from the authentication and management mechanisms of published information. Malicious users have reportedly managed to bypass users' privacy settings of these services in many cases. As a result, new offenses ranging from identity theft up to personal information

* Corresponding author.
E-mail addresses: kpatsak@unipi.gr (C. Patsakis), azigomit@unipi.gr (A. Zigomitros), axilpapa@gmail.com (A. Papageorgiou), edgar.galvan@scss.tcd.ie (E. Galván-López).

http://dx.doi.org/10.1016/j.comnet.2014.08.023
1389-1286/

exposure are disclosed on a daily basis. The ease of re-uploading and re-publishing a user's images, without any form of notification, often harm the original owner both social and economically.

It should be noted that the term of ownership, throughout this work, should not be considered in terms of property or copyright, but it rather refers to the fundamental right to privacy. Users expect that by submitting their personal photos on OSNs, they are free to set their own privacy policies, allowing access only to the users that they decide. The uploaded content is part of their private lives and therefore belongs to them. Therefore, users should be able to selectively reveal themselves to the world [15].

Modern users normally do not have a single account for an OSN. In fact, users have accounts in many OSN and/or even multiple accounts in some of them. Let us assume that Alice and Bob belong to the same online social network OSN_1. Bob can easily download a photo from Alice's profile, obviously without Alice's consent or any kind of notification. Bob can make several alterations on Alice's photo offline, and then share it in another online social network OSN_2. It is clear that Alice will not be notified of the incident and no matter what privacy policies she has set on the photo, they will be bypassed.[1]

The core of this problem is that currently OSNs do not check what multimedia are being uploaded, *e.g.* whether a photo has already been published, by whom, what are the privacy policies etc. Additionally, modern OSNs treat themselves as a separate entity, which have nothing to do with any other OSN. Of course, even if many of the existing OSNs have a different orientation like socializing, health issues, professional or academic profiles, OSNs do not tend to interact, in order to gather more users. Due to the competition, this attitude seems fairly logical, nevertheless, redefining the problem in the context of other services, such as telecommunications or emails, reveals the importance of the problem. In this case, the subscribers of one provider would only be able to communicate with others of the same provider. However, the growth of both these services was achieved because the users were allowed to exchange information independently of the provider. Therefore, to further advance OSNs it is crucial to allow and develop mechanisms, in which all OSNs can exchange information.

This change is very probable to become a need quite in the near future. According to several researchers, fragmentation of current social networks is due to come. For instance, Boyd argues that fragmentation is closer to the human state of being since it allows them to focus on specific groups of interests, rather than generic and monolithic ones [6]. Additionally, while major OSNs allow some flexibility in creating smaller "groups" which are user created and more coherent, their actual capabilities are rather restricted, compared to smaller yet "specialized" OSNs. The latter fulfill the actual needs of their target groups as they are specially crafted for them, thus they are far more efficient than trying to provide patches to allow some additional functionality.

Independently of whether fragmentation of OSNs will happen, or how users log into their accounts, it is definite that through cooperation, OSNs may protect their users or even offer them additional services. In this work we focus on former.

This work is motivated by the following research question: "*Can we have more privacy-aware solutions for current Online Social Networks?*". We argue that such solutions do exist, even by applying well-known techniques. Thus, we focus on how they can be achieved and their feasibility within current structures, in terms of implementation effort, processing needs and economic constraints. The main contribution of this work is a new scheme that enables collaboration between OSNs to enhance users' privacy. The novelty of the scheme resides in the fact that it is completely decentralised and does not depend on a trusted third party (TTP). The proposed scheme counters many problems that stem from sharing multimedia content on OSNs such as identity theft, unauthorized content sharing and distortion of malleable content. Additionally, the scheme allows a new feature, the shared ownership of multimedia content.

One may argue that the current business model does not allow for such changes as the big "players" do not have the proper incentive to push such solutions forward. They are well established and want to increase their market shares. Therefore, one could claim that cooperation does not seem probable. The recent example of Schema.org[2] exemplifies that this is far from true. The search engine giants decided to cooperate and create a common framework that helps them to carry out their business easier and more efficiently. One should also take into consideration the role of regulatory authorities. The recent deal between EU anti-monopoly authorities and Google[3] signifies that big players can be forced to play with more "open" rules. Thus, developing a common privacy-aware framework for OSNs under the pressure of regulatory authorities[4] is not a far-fetched plan.

It is worthwhile to notice that while OSNs disregard each other, there is another link between many of them. Major OSNs may not interact with each other, nevertheless, they allow smaller OSNs to exploit their authentication mechanisms. Therefore, the majority of smaller OSNs are not registering their users directly, but rather obtain user authorization, through *e.g.* OAuth,[5] to use some of the information from bigger OSNs. This fact indicates that OSNs can further cooperate.

The main concept of this work is based on [37], updating and extending the findings of the conducted experimental results and discussing them in depth. However, the main contribution of this work is the introduction of a novel distributed scheme, without TTPs, which allows multiple OSNs to apply the privacy policies of their users among them, even if one user is registered to a single

[1] The case where Bob re-uploads the photo on the same OSN is addressed in [37].

[2] www.schema.org.

[3] http://europa.eu/rapid/press-release_IP-14-116_en.htm.

[4] https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2014/14-07-14_PH_for_EV_online_EN.pdf.

[5] http://www.oauth.net.