Computer Networks xxx (2014) xxx–xxx

Contents lists available at ScienceDirect

Computer Networks

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

A survey on decentralized Online Social Networks

Thomas Paul [a,*], Antonino Famulari [b], Thorsten Strufe [c]

[a] Technische Universität Darmstadt, Hochschulstrasse 10, 64380 Darmstadt, Germany
[b] Télécom ParisTech, INFRES, 23, Avenue d'Italie, 75013 Paris, France
[c] Technische Universität Dresden, Nöthnitzer Straße 46, 01187 Dresden, Germany

ARTICLE INFO

Article history:
Received 20 January 2014
Received in revised form 15 September 2014
Accepted 1 October 2014
Available online xxxx

Keywords:
Online Social Network (OSN)
Distributed Online Social Network (DOSN)
Privacy

ABSTRACT

Because of growing popularity of Online Social Networks (OSNs) and huge amount of sensitive shared data, preserving privacy is becoming a major issue for OSN users. While most OSNs rely on a centralized architecture, with an omnipotent Service Provider, several decentralized architectures have recently been proposed for decentralized OSNs (DOSNs). In this work, we present a survey of existing proposals. We propose a classification of previous work under two dimensions: (i) types of approaches with respect to resource provisioning devices and (ii) adopted strategies for three main technical issues for DOSN (decentralizing storage of content, access control and interaction/signaling). We point out advantages and limitations of each approach and conclude with a discussion on the impact of DOSNs on users, OSN providers and other stakeholders.

1. Introduction

Online Social Networks (OSNs) are one of the most popular services on the Web with more than one billion users.[1] Yet, OSNs are not just tremendously popular; they have also changed the way we interact with the Web and its resources: OSNs allow non-expert users to create and maintain a personal space in the Web in a simple way. OSNs evolved in time, providing several communications and sharing facilities which cause users to share huge quantities of personal information [22] over them.

Nevertheless, users of today's popular OSNs suffer undesired side effects resulting from a centralized architecture of OSNs in which one provider has the power that is accompanied with being the operator of the system. These side effects include: the necessity for a high degree of trust in the OSN provider, censorship issues and privacy concerns.

Economic pressure to earn money due to provider-side infrastructure and maintenance costs and the provider's legitimate profit interests lead to strong incentives for OSN providers to monetize user data far beyond the user's sharing interests [20]. But users need to trust the latter not to misuse the power, accompanied with being the operator of the system, as well as to be able to protect the system against both attackers from outside and from inside the provider's organization itself. The existence of a powerful system operator combined with monetization incentives cause privacy concerns [27]. Furthermore, different types of censorship occur in today's OSNs: the content-specific censorship with respect to different rules and traditions in different countries [1,2] as well as person-specific censorship which means disallowing subsets of the population to access the network (e.g. in Syria today [3]).

However, the importance of OSNs for the daily interperson communication puts the OSN providers in a position of being gate keepers to parts of the social life of their users. Due to this dependency, users strongly tend to accept the mentioned side effects and even disadvantageous terms of usage, since the OSN providers may exclude users from the OSNs and subsequently from parts of their social contacts. Authors of decentralized OSN (DOSN) approaches aim to abolish OSN providers and the

* Corresponding author.

[1] http://allfacebook.de/userdata/ – accessed on 16th of January 2014.

http://dx.doi.org/10.1016/j.comnet.2014.10.005
1389-1286/

side-effects of centralized OSNs by creating decentralized systems, providing the social networking functionality.

Approaches for encrypting content in centralized OSNs (e.g. [27]) may mitigate content censorship and communication confidentiality concerns but they still allow the OSN provider to observe communication patterns. Individuals can still be excluded from the system to conduct censorship. Those encryption approaches also raise the question whether the business models of today's OSNs still work and allow the providers to make sufficient infrastructure available. We thus argue that decentralization is the best available concept to address the trust, the privacy and the censorship issues.

Many kinds of DOSNs have been proposed by several authors. Nevertheless, the idea of distributing OSNs has not been widely adopted. Beside Diaspora,[2] none of the DOSNs has a denotative user basis. In contrast to the authors of many DOSNs, Narayanan et al. doubt in [34] that decentralizing OSNs is a feasible way to build social networking services. We argue that distributing OSNs is a worthwhile idea and aim to help the DOSN community with this survey by elaborating and evaluating what has been suggested in the field of DOSN.

In the remainder of this survey, we define the terms, which are elementary for this article in Section 2. We state our requirements and adversary models (Section 3) and introduce a DOSN architecture model to explain the design space (Section 4) as well as the design decisions that have to be made in case of creating DOSN architectures (Section 5). These design decisions determine the properties of DOSNs. Thus, they are the basis for our classification in Table 1. In Section 6, we discuss both: the consequences caused by the design decisions as well as the properties of DOSN classes (with respect to our classification). Furthermore we list all approaches which fit in the shape of our DOSN definition, discuss the features of the different DOSN approaches and provide a publication time line to illuminate the publication history (Section 7). Several ideas to improve aspects in the field DOSNs have been published without suggesting a complete new architecture. Since we consider them to be important contributions, we introduce a selection of DOSN related approaches in Section 9. Finally, we elaborate the impact of decentralization on different OSN affiliates and summarize and conclude our article.

2. Definitions

This Section defines specific terms used in this article: Section 2.1 contains elementary terms, Section 2.2 defines different types of decentralization as well as terms that are closely related to decentralization and Section 2.3 specifies DOSN components.

2.1. Elementary terms

We use the term *Personal identifiable information (PII)* as it has been introduced by the Data Protection Directive 95/46/EC of the European Parliament. PII is "any information relating to a [...] natural person [...] who can be identified, directly or indirectly, in particular by reference [...] to one or more factors specific to his physical, physiological, mental, economic, cultural, or social identity". PII can consist of *content*, e.g. pictures and messages, as well as all types of *incidental data* which can be derived from e.g. technical properties (e.g. size) of content or communication parameters.

Authorization is a mechanism to decide about legitimization based on previously defined rules. *Access control* denotes the action to allow legitimized subjects to access content and to prohibit unauthorized access. According to "privacy as control" in [16], *privacy* in our context means the effectiveness of users to be able to restrict access to information that the user is responsible for (as a producer of the message). The effectiveness can be affected by technical and social (e.g. social engineering) interferences.

An *Online Social Network* (OSN) in this article is "an online platform that (1) provides services for a user to build a public profile and to explicitly declare the connection between his or her profile with those of the other users; (2) enables a user to share information and content with the chosen users or public" [37].

Since each OSN provides different functionality, we decided to distinguish *basic functionality* which needs to be part of the system to be considered being an OSN and the *extended functionality*, which is not qualifying but extends the service in a specific way.

Derived from the definition of OSN, *basic functionality* consists of:

- *Profile management:* creating, maintaining and deleting of user profiles, which subsequently includes authorization mechanisms for profile attributes.
- *Relationship handling:* establishing and removing new relationship declarations.
- *Interaction:* direct interactions (internal messaging system – 1:1) and indirect interactions by sharing content (1:*n*).

The *extended functionality*, we define for this article, is a set of features which some of today's OSNs provide. The reason for mentioning them in this definition is that we consider these to be important pieces, contributing to the attractiveness and popularity of the OSN platforms. We take the following into account:

- An *API*, allowing third party applications to run on the OSN platform.
- A *search* function to find other users of the OSN.
- A *recommender system* that recommends users to become friends or content to be consumed.
- A *social network connector*, bridging different social networks.

2.2. OSN decentralization definitions

Decentralization has more than one dimension in the field of OSN. We distinguish between *technical decentralization* (resource distribution) which means that

[2] https://joindiaspora.com/ – accessed on 14th of January 2014.

Q1 Please cite this article in press as: T. Paul et al., A survey on decentralized Online Social Networks, Comput. Netw. (2014), http://dx.doi.org/10.1016/j.comnet.2014.10.005