A comparison framework for Decentralized Online Social Networks

Antonino **FAMULARI** (famulari@enst.fr) and Artur **HECKER** (hecker@enst.fr)
Télécom ParisTech (ENST) – CNRS LTCI UMR 5141
Paris, France

Introduction

In the current OSNs, by construction, the OSN provider retains a predominant position: a user must trust the OSN platform provider in many regards. However, as several cases from the past show, this trust is often unfounded. Quite in contrast, there are actually good reasons [1] [3] to mistrust providers: these can be bound to the business models, to dubious practices with regard to privacy, to sudden policy changes, or to specific negative experiences [4].

Moreover, current OSNs explicitly put users in a condition of dependence on one single OSN Service Provider (SP) in that users can only interact with other members of the same OSN platform. Migration from one platform to another is not supported by current mechanisms. Finally, the presence of a Central Authority (CA) in form of the OSN provider implies the possibility of some form of censorship.

Several authors [5] [6] [7] [8] proposed a more user-centric approach to Online Social Networking, so that users maintain control on their data, regarding what they share and with respect to their social relationships and interactions. As these requirements cannot be fulfilled in a centralized architecture because of the mentioned predominant position of the platform owner, the only alternative is to follow decentralized and distributed approaches. Consequently, the current trend in OSN privacy is to offer an analogous OSN service through a realization that prevents any entity from a full access to user data and from getting a full awareness of user interactions.

Although several proposals already exist for Distributed architectures for OSNs (DOSN), the subject is still relatively new. So far, the existing proposals do not contain comparison frameworks of reference. In this work, we fill such lack proposing a framework for decentralized OSN architectures: we first define a new architectural model extending previous proposals [6]. We then define requirements for a user-centric approach to OSNs. Next, we identify problems raised by service decentralization: we analyze what already exists in the literature and frame the state of the art according to our requirements. Finally, we conclude with an evaluation of the existing proposals, pointing out strong points and weaknesses. This results in new guidelines for future works for DOSNs.

A new architectural model

To compare different existing proposals, we propose a new 3-layers architecture for OSNs. Each layer is characterized through MUST, SHOULD and MAY requirements. The proposed model consists of:

3. Social Application Layer (SA)
2. Social Network layer (SN)
1. Social Networking Services layer (SNS)

The SA layer provides support for social applications. It is composed of two applicative domains: the first concerns third-party applications. SA layer MAY provide development APIs (like Facebook or Google+) for such external applications, handling a limited and transparent facilities to access sensitive data. The second domain concerns OSN's core functionalities: this domain MUST provide primitives for activities such as interacting with friends, browsing activities of friends or sharing data also defining Access Control policies.

The SN layer deals with the social network. It concerns the social sphere of users and MUST exploit social information to support requests of the SA layer. This layer, in fact, is the only one aware of user-to-user connections at a social network level. The organization of first-hop relationships (i.e. Google+ circles, Facebook lists of friends etc.) is handled at this level.

The SNS layer defines the OSN platform. It MUST define the logical structure of the different involved entities and implement all the mechanisms allowing the interactions between the latter by providing storage of content, content retrieval facilities, access control on such content (on the basis of policies defined at the SA layer and of the relationship nature as defined in SN) and so on. In general at this layer there is no correspondence between real social network.

Requirements and challenges of a user-centric approach to OSNs

On the basis of the existing literature [9] [6] [5], we then propose a new set of requirements for a user-centric approach to Online Social Networking.

i) Users must keep rights on shared content.

ii) None but communicating entities (or explicitly authorized) must be aware of each interaction.
   a. Direct (non-mediated) interactions if possible
   b. Impossibility to identify interacting parties in P2P OSNs [6]

iii) Users do not need to join one specific common platform for interacting with each other.

iv) Users must have the possibility of terminating their own account without any accessible trace remaining in the system.

Such privacy/independence requirements are in contrast with the current centralized approach to OSNs for all the mentioned reasons. The necessary bandwidth, storage capacity, security mechanisms and so on, represent in fact a huge cost for a provider, leading SPs to put users' privacy in the background [2].

Yet, decentralization does not come for free and bears its own problems. Indeed, some mainstream OSN features such as complex search are noticeably more difficult to implement in a decentralized OSN realization. Besides, a distributed system *per se* is not a warranty for a better privacy or security. Quite the reverse, decentralization of storage and other functionalities raise new questions in terms of security of such a distributed system, security of exchanges within and with the latter, high availability of user profiles, distributed access control on user data, keeping the complete social graph out of the control of any single CA, or countering typical attacks against OSNs without the help of any Central Authority.

Evaluation of the State of the Art

We conducted an analysis of the state of the art on DOSNs so as to evaluate different existing approaches with respect to the defined requirements. We identified four main characteristics that permit to distinguish different solutions:

1) Node topology at the SNS layer (e.g. P2P or client-server)
2) Distributed content storage mechanism (i.e. on peers, on external storage servers etc.)
3) Content retrieval mechanism (i.e. DHT, out-of-band mechanisms, DNS etc.)
4) Distributed access control (i.e. cryptography-based, access control lists etc.)

We classified existing works according to these characteristics and evaluated the proposed solutions pointing out some open issues.

In general, the dynamicity of information and relationships/interactions that characterize OSNs [2] makes pure P2P OSNs harder to implement than designs that rely on persistent logical nodes such as external storage servers. The main open issue related to P2P OSNs is the availability of user data: replication mechanisms may be hard to manage, since shared resources are subject to frequent changes both in the content and in the access control preferences. However, they are in general costly in terms of resources (such as storage space at peers, bandwidth, etc). Also, since data are stored on peers, the access control may require a certain degree of trust toward such peers [6] [10].

In general, architectures relying on external storage entities can provide better guarantees in terms of data availability with respect to P2P architectures. Yet, in the existing works, such external storage servers are much more than mere storage facilities, since they need to play active roles e.g. in user authentication, security policy enforcement, etc.. In general, such functionality is not provided for free; therefore, this implies costs for the end users.

Conclusions

We show that current decentralized OSNs do not yet provide a valid alternative to logically centralized counterparts in terms of functionalities and facilities to the final users. Also, they do not fulfill all the requirements in terms of security/privacy that we defined.

On the basis of such considerations, we formulate guidelines for a new DOSN that should limit efforts and the corresponding costs for Service Providers, feature good privacy assurances for users and still provide the same core functionality as logically centralized counterparts.

References

[1] ***The Status Quo of Online Social Network Security: A Survey;*** H. Gao and J. Hu and T. Huang and J. Wang and Y. Chen; IEEE Internet Computing 2011

[2] ***Business Models in Social Networking ;*** M. Falch and A. Henten and R. Tadayoni and I. Windekilde ; CMI International Conference - Social Networking and Communities ; 2009

[3] http://businessetc.thejournal.ie/facebook-security-breach-allowed-advertisers-access-to-user-data-134549-May2011/ ; december 2011

[4] http://www.ftc.gov/opa/2011/11/privacysettlement.shtm; december 2011

[5] ***Persona: AN Online Social Network with User-Defined Privacy***; R. Baden and A. Bender and N. Spring and B. Bhattacharjee and Daniel Starin ; SIGCOMM'09

[6] ***Safebook: Feasibility of Transitive Cooperation for Privacy on a Decentralized Social Network ;*** A. Cutillo and R. Molva and T. Strufe

[7] ***PeerSoN: P2P Social Networking - Early Experiences and Insights*** ; S. Buchegger and D. Schioberg and L. Vu and A. Datta ; SNS'09

[8] ***Lockr: Better Privacy for Social Network***; A. Tootoonchian and S. Saroiu and A. Wolman, Y. Ganjali; CoNEXT'09

[9] ***A Case for P2P Infrastructure for Social Networks - Opportunities & Challenges*** ; S. Buchegger and A. Datta ; WOSN'09

[10] ***Privacy, Cost, and Availability Tradeoffs in Decentralized OSNs ;*** A. Shakimov and A. Varshavsky and L. P. Landon and R. Càceres ; WOSN'09