International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 02 | Feb-2018 www.irjet.net p-ISSN: 2395-0072

Review on privacy in decentralized online social networks

Ms. Manisha Bhole

Lecturer, Department of Computer Engineering, V.P.M's Polytechnic(Thane),Maharashtra

---

Abstract - *Decentralized Online Social Networks (DOSNs) are recently captured the interest of users because of the more control given to them over their shared contents. Indeed, most of the user privacy issues related to the centralized Online Social Network (OSN) services (such as Facebook or Google+) do not apply in the case of DOSNs because of the absence of the centralized service provider. However, these new architectures have motivated researchers to investigate new privacy solutions that allow DOSN's users to protect their contents by taking into account the decentralized nature of the DOSNs platform. In this survey, we provide a comprehensive overview of the privacy solutions adopted by currently available DOSNs, and we compare them by exploiting several criteria. After presenting the differences that existing DOSNs present in terms of provided services and architecture, we identify, for each of them, the privacy model used to define the privacy policies and the mechanisms for their management (i.e., initialization and modification of the privacy policy). In addition, we evaluate the overhead introduced by the security mechanisms adopted for privacy policy management and enforcement by discussing their advantages and drawbacks.*

Key Words: Data privacy, Decentralized online social network, Access control, Security Peer to peer computing

1. INTRODUCTION

Recent years have seen unprecedented growth in the Online Social Network (OSN) services [1], with about 300 OSNs collecting information about more than half a billion registered users.[1]An OSN enables its users to define their own *profiles*, a virtual representation of themselves, and to explicitly declare the relationships with (the profiles of) other users. Regardless of their purpose, the main service provided by the OSNs to their users is the sharing of information with a set of selected contacts. Users can publish on their profiles very heterogeneous contents, ranging from personal information, wall posts, photos, videos, comments to other posts, and they can send private messages. Nowadays, the most popular OSNs are based on a centralized architecture where the service provider (e.g., Facebook) acts as central authority and takes control over users' information, by storing a huge amount of private and possibly sensitive information on users and their interactions (such as the personal information and lifestyle behaviors).

Due to the centralized infrastructures, users of the current OSNs are exposed to several privacy risks. Indeed, users of centralized OSNs are forced to share the information directed to their friends by means of the OSN service providers, increasing the risk of censorship, surveillance and information revelation. Indeed, recent events have shown that, in addition to malicious users (internal or external to the OSN), also the centralized service provider [2,3] and third-party applications [4] introduce new privacy risks. The National Security Agency (NSA) documents clearly illustrate how the agencies collected users' information by exploiting the weaknesses of the Facebook's security platform [3].

To address the previous privacy issues and leave to the users the control on their data, researchers have proposed to decentralize the functionalities of OSNs by implementing them in a distributed way. The resulting platforms are known as Decentralized Online Social Networks (DOSNs) [5,6] and they are typically based on a P2P architecture, such as a network of trusted servers, an opportunistic network, a Distributed Hash Table, or an unstructured P2P network. For this reason, in a DOSN there is no central control authority which manages and maintains available the users contents. Instead, DOSNs are based on a set of peers that store the contents and execute the tasks needed to provide a seamless service (such as, search for data [7], recommendation [8], etc.

1.1 Motivations

While decentralization gives the possibility for increasing the privacy of users with respect to the OSN provider, several studies show that privacy is an increasing concern also for DOSNs' users [12,13]. Indeed, regardless of their architectures, one of the main features provided by current DOSNs is the capability given to the users to define privacy preferences on the contents of their profiles, i.e., to define which other users are allowed to see such contents. In fact, the lack of privacy mechanisms with a suitable granularity level and flexibility could lead to a unwanted disclosure of information, thus exposing users to a number of security risks. Since the number of users' contacts, as well as the number and the type of contents shared on DOSNs, are constantly increasing, members of DOSNs need an effective way to define authorizations to protect their contents.

Users' contents must be protected by the DOSN infrastructure according to users' privacy policies from unauthorized access, i.e., only users who have been granted the proper permissions through privacy policies should be enabled to access the contents. However, while the contents produced by user u may be stored on the devices of u until u is online, when u goes offline these contents must be stored, in order to keep them available, on the devices of other users which are supposed to remain online in the system or on external trusted resources. This requires the usage of proper strategies to prevent unauthorized access to contents of u when they are stored on the devices of other users.

1.2. Contributions

The main aim of this paper is the investigation of the different approaches used by existing DOSNs to protect the privacy of the contents of their users. For this reason, we identified a large set of DOSNs which have been proposed in the literature, by considering both the DOSNs which are really deployed (such as Diaspora, Friendica, or Retro Share) and the ones which are under active development. For each of the selected DOSN, at first we briefly analyze the architectural model used to provide independence from a centralized provider, and then we study the approach adopted to enable users to define their privacy preferences and to enforce them.

2. DECENTRALIZING THE ONLINE SOCIAL NETWORKS

A current trend for developing OSNs that do not rely on a centralized service provider is moving towards the decentralization of the OSN service. A Decentralized Online Social Network [6] is a OSN implemented in a distributed and decentralized way. The approaches exploited by current DOSNs to provide independence from a centralized provider are typically based on Peer to Peer (P2P) architectures (such as a Distributed Hash Table [25] or network of interconnected trusted servers). Indeed, every participating user can act both as a server and as a client, depending on the context [26]. The approaches used by current DOSNs to provide independence from a centralized authority combine multiple architectural levels, each with its own features. According to the topology of the P2P network, the currently available DOSNs can be classified into two alternative P2P architectural styles:

Structured:

In structured P2P architectures, the peers are organized into a specific topology that ensures good performance on specific tasks of the system, such as routing. This architecture exploits hashing to associate an identifier to the peer and to pair contents with peers, so defining a DHT.

Decentralized:

This architecture does not impose any particular conditions concerning where data should be stored, since contents of users are stored on random nodes.

Unstructured:

This P2P architecture does not impose any particular structure and resources are connected according to their needs. Operations are usually implemented by using flooding or gossip-like communication between users.

Instead, the approaches used by current DOSNs to accomplish the data storage functionality are mainly based on three P2P architectural styles

Hybrid:

This architecture exploits the P2P approach, but also relies on some external service provided by a centralized entity (such as Clouds, Private Servers, Dropbox, etc.). This service allows the users to exploit permanently available resources which guarantee that their contents can be always accessed, but this also implies a cost for the DOSN's users.

Semi-decentralized:

A subset of the users in the system (super peers) takes responsibility for storing and managing information of all the users. The choice of providing super peer services can be voluntary or incentive-based.

3. PRIVACY REQUIREMENTS IN DOSNS

Decentralized OSNs address the main privacy concern about users' data that affects centralized OSNs, because data are stored on the peers of the users belonging to the DOSN or on some storage server chosen by the user, and there is no central authority that controls and stores such data. In addition, DOSNs users are able to define privacy policies, i.e., (typically simple) statements specifying who can access their contents. As a result, DOSNs shift the control over users' data to the peers that build up the system (i.e., to the users these peers belong to), thus solving some, but introducing new security issues, such as the one concerning the confidentiality of users' data with respect to the users providing the peers where such data are stored.

4. PRIVACY MODEL

Each DOSN enables its users to protect their contents by defining privacy policies that determine the set of users authorized to access each of them. The majority of existing DOSNs, provide to the users a limited and predefined set of privacy policies based on the knowledge derived from the social network, e.g., relationships (friends, family, colleagues, etc.), groups, content or profile information. For instance, some DOSNs allow their users to define groups of friends, and to specify which groups are allowed to access each of the content they publish. Table 1 summarizes the access control options of current DOSNs by reporting the privacy policy type and (if the case) the encryption schemes used by each DOSN to enforce privacy policies. The most part of current DOSNs protect users' contents by employing both asymmetric and symmetric encryption.

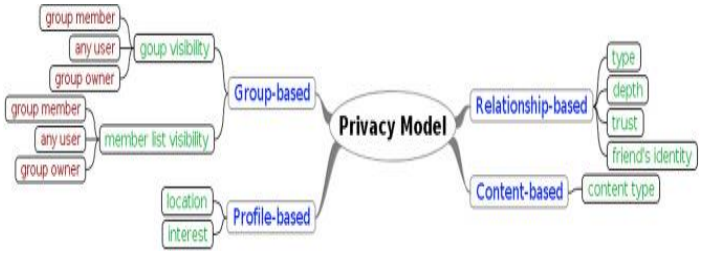
Safebook.

The privacy model of Safebook is sketched in [31] and refined in [32]. Personal information of users is organized

into atomic attributes, and privacy policies based on these attributes can be defined by each user. Contents (or artifacts) are logically grouped by labels (such as Comments, Posts, Images, etc.) and on each label a set of attributes is defined in order to be exploited in privacy policies.

4. EVALUATION

Group-based privacy policies allow users to organize their contacts into distinct groups, namely *groups* in Life Social. KOM, Vis-a-Vis, and Persona, aspects in Diaspora, circles or groups in Safebook, or file group in PeerSoN. These groups differ from those resulting by the types of the relationships because they contain contacts with different types of relationships. As a result, group resulting from the relationship-based privacy policies are homogeneous in terms of types of relationships while group-based privacy policies are meant for heterogeneous groups.



Download high-res image (240KB)
Download full-size image

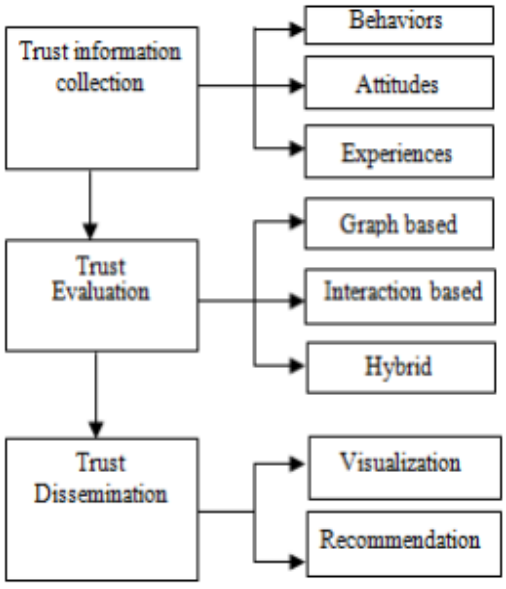


Fig.Social Trust System classificqation

5. DISCUSSION

This section discusses the implications of the security mechanisms adopted by the current DOSNs on the privacy level they guarantee to their users. In particular, based on the observations made in the qualitative analysis presented in the previous sections, we identify a set of properties which are relevant to assess the expressiveness of the privacy support of DOSNs. These properties are related to the ways a DOSN grant their users the capability to define privacy policies, i.e., respectively, to the possibility to define privacy polices based on Groups, Relationships, Profiles, and Contents.

8. CONCLUSION

We selected a relevant number of DOSNs and we investigated the mechanisms they provide to allow users to express their privacy preferences, i.e., to decide which of the contents they published should be disclosed to the other users. In particular, we classified and compared the different types of supports for expressing privacy policies provided to the users to specify access rights to the contents of their profiles. Moreover, we investigated the mechanisms adopted by these DOSNs in order to ensure that privacy policies defined by users are properly enforced. We found out that privacy policies are mainly enforced exploiting encryption, through a hybrid schema based on both symmetric and asymmetric cryptography. In addition, we observed that the security solutions exploited by DONS to enforce a privacy policy could be affected by the type of the privacy policy. As for instance, classical P2P security solutions could suffer from scalability issues if they are used for the enforcement of group-based privacy policies because the overhead introduced by encryption operations in order manage very large groups.

REFERENCES

[1] Sherchan, W., Nepal S and Paris C,"A Survey of trust in social networks" ACM Comput. Sury. 45,4 Article 47 (August 2013), 33 pages.

[2] Thapa, A.; Li, M.; Salinas, S.; Li, P. "Social Proximity Based Private Matching Protocols for Online Social Networks" Publication Year: 2014.

[3] C. Zhang, J. Sun, X. Zhu, and Y. Fang "Privacy and security for online social networks: Challenges and opportunities" IEEE Netw., vol. 24, no. 4, pp. 13–18, Jul./Aug. 2010

[4] L. Guo, X. Zhu, C. Zhang, and Y. Fang, "A multi-hop privacy-preserving reputation scheme in online social networks" in Proc. IEEE Global Telecommun. Conf., Dec. 2011, pp. 1–5.

[5] A. Cutillo, R. Molva, and T. Strufe, "Safebook: A PrivacyPreserving Online Social Network Leveraging on RealLife Trust",|| Communications Magazine, vol. 47, no. 12, 2009, pp. 94–101.

[6] W. Chen and S. Fong, "Social network collaborative filtering framework and online trust factors: A case study on facebook" in Proc. 5th Int. Conf. Digital Inf. Manage., Jul. 2010, pp. 266–273. [7] G.K.Panda, A. Mitra, Ajay Prasad,

Arjun Singh, Deepak Gour, "Applying l-Diversity in anonymizing collaborative social network" In: International Journal of Computer Science and Information Security, Vol 8, Issue 2, pp 324 - 329, 2010.

[8] Na Li, Nan Zhang, Sajal K. Das, "Relationship Privacy Preservation in Publishing Online Social Networks", In Proc. of IEEE International Conference on Privacy, Security, Risk, and Trust, Boston, MA, pp 443-450, 2011.