Privacy Challenges in Online Social Network

Jia-Hua Lin[1)]

Kwangio Kim

Department of Compute Science, China university of Geosciences(Wuhan), P.R.China

Department of Computer Science, KAIST, Korea

Abstract

The privacy of Online Social Network has been confronted with unprecedented challenges on the era of Big Data. To address this problem, researches have proposed various defenses emphasized on different types of OSNs. In this survey, we give the definitions and classification of OSNs based on their topology. Then we discuss the privacy challenges and their comprehensive solutions. After that we highlight the future trend in OSN architecture design, we come up an idea about hybrid OSN. Finally, three considerations to achieve technology in both privacy and usability are listed.

I. Introduction

Online Social Networks (OSNs) nowadays has been more intelligent due to the analysis and forecast over vast amounts of user data. However, at the same time it threatens our privacy greatly than ever before as a side-effect. As the computing power is enhancing, the privacy protections are more complex: instead of key words the whole public data should be covered. Moreover, the traditional anonymization doesn't work well since we can match it from various data resources, just like leakage issues in AOL and Netflix[1]. Besides, OSN is the product of multi-technologies combination, which means the privacy protection level is determined by the lowest-privacy-preserving technology, just like Liebig's barrel. In short, the privacy protections should be comprehensive. However, this results one extreme: heavily emphasis on privacy while ignore the utility in real world. The main contributions of this work are that a) we summarize the privacy challenges and solutions which are traditional and innovative; b) suggest an idea about hybrid OSN architecture and 3)propose 3 concerns to meet balance in privacy and utility.

II.Background

OSN is a platform that provides the service users can set up their public profiles and interact with friends or acquaintance, also supports the development and usage of social applications in its platform. Fig.1 gives the classification on OSN. From the perspective of architecture, there are distributed and centralized OSN (COSN, which is distributed architecture as P2P system and social network as online social network). While considering the OSN carriers, there are web-based social network which means social

1) The paper was done while the first author is visiting KAIST, 2013.

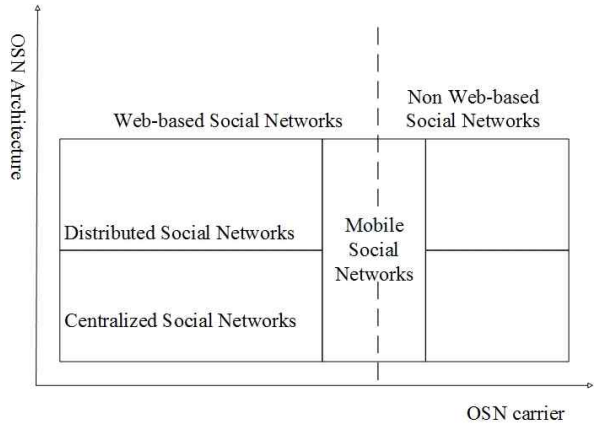

Fig. 1 the OSN category

network sites and non web-based social network which refers to social applications in mobiles or computers. The category of OSN is vital, for every OSN has its own emphases on privacy protection, as shown in Table 1.

III. Privacy challenges and solutions

In this section, we summarize the privacy challenges in social network and solutions[2]. We classify that there are 7 major privacy problems: a) linked mining in public released data; b) recommender system applied in OSN; c) location-based service in mobile social network; d) authentication ;e) access control; f) third-party app in OSN; and g) website leakages in web-based social network. The approaches to defense these problems are wide-ranged. And anonymization and cryptographic protocols are the two widely-applied studies in privacy protection. Besides, some original ideas have proposed as well, such as Differential privacy, Homomorphic encryption. In Table 2 we give more detailed descriptions.

When an individual's sensitive data disclosed to an adversary, it is defined as a privacy breach. There are four types of privacy breaches: identity disclosure, attribute disclosure, social graph disclosure and affiliation link disclosure[3].They interact with each others, and one leakage could lead to others disclosure.

Table 1. Emphases on OSN privacy protection

Privacy challenge	P2P OSN	Centralized OSN
Linked mining in public released data		●
Recommendation		●
Service Providers		●
Authentication	●	
Access control	●	
Third-party App	●	●
Website leakage		●

IV. Future trend in OSN architecture

Many researchers have turned to the idea of a Distributed OSN (DOSN) and believe it as a future trend[4]. However, a DOSN still confronted with lots of challenges including security problems[5], *e.g.*, to ensure the access control of authorized users, the encryption on data must be done. However, how to handle the key distribution and maintenance so that the authorized group can access data but flexible enough to deal with churn, additions and removal to the user's social network is a problem. In this part, we introduce the typical DOSN design, Safebook and pointed out its pros and cons. Finally, we give an idea about hybrid online social network which could leverage the advantages of centralized OSN in its performance and without compromising the privacy.

4.1 A Distributed OSN

This section outlines a DOSN called Safebook proposed by L.A Cutillo *et al.*[6].Safebook consists of three major different components: 1) the Trusted Identity Service, invited users only are able to get certifications from TIS, and then join the social network; 2)the

Table 2. Privacy challenges and solutions

Privacy challenge	Solution	
	Traditional	New
Linked mining in public released data	Anonymization; Randomization.	Differential privacy ; Distribute social network.
Recommendation	Anonymization; Randomization; Cryptographic Protocols: -Secure multi-party computations; -Secret sharing; -Zero-knowledge proofs.	Differential privacy; Homomorphic encryption.
Location-based service	Anonymization; Private Information Obfuscation; Cryptographic Protocols: -Blind signature; -Zero-knowledge proofs. Client-Server Solutions ; Middleware support.	
Authentication	Cryptographic Protocols; Smart card ; Biometric identification technology.	
Access control	Access Control Policy: -Attribute-based access control -Role-based access control	Context-Aware Access Control
Third-party Apps	Security API; Privilege authorization.	
Website leakage	Browser-based solutions ; Reusing security paradigms ; Anonymization.	Semantic approach; User-managed access control.

Matryoshkas which are specialized overlays network encompassing each user to protect the identified participation; 3) a P2P location substrate, which is implemented for the purpose of locating other users' Matryoshkas. The authors indicated two strong points of Safebook which are: 1) using decentralized architecture to avoid the violations by the provider; 2) trusting the real life friends to solve the problems in building trusted and privacy-preserving mechanisms. However, researches have pointed out that this architectural attempts lack a viable economic model[7,8] and suffered the performance penalties[9] the achievement ratio of accessing data from friends is low with 90% only.

Even though we believe that DOSN offers better privacy protection, nothing proposed to date provides viable incentives to move users away from existing OSNs.

4.2 Hybrid OSN architecture

Since COSN has performance guarantee while DOSN provides privacy preserving. How about the combination of these two?

Anderson came up an idea about semicentralized OSN called Footlights[10]. He proposed a subscription model--users pay for cloud data storage at very low price (1dollar/user/year) and without trust it (for the user data has been segmented into 4KB encryption blocks). Meanwhile a local client achieves access control, key distribution and supports running of social applications with security API. This proposal gives us an inspiration on hybrid architecture on OSN. In Fig.2, we show the topologies of centralized , distributed and hybrid OSNs.

If the capacity of service providers is storage only, why not do we add it into the distributed OSN to enhance the performance and resist the churn in dynamic network?

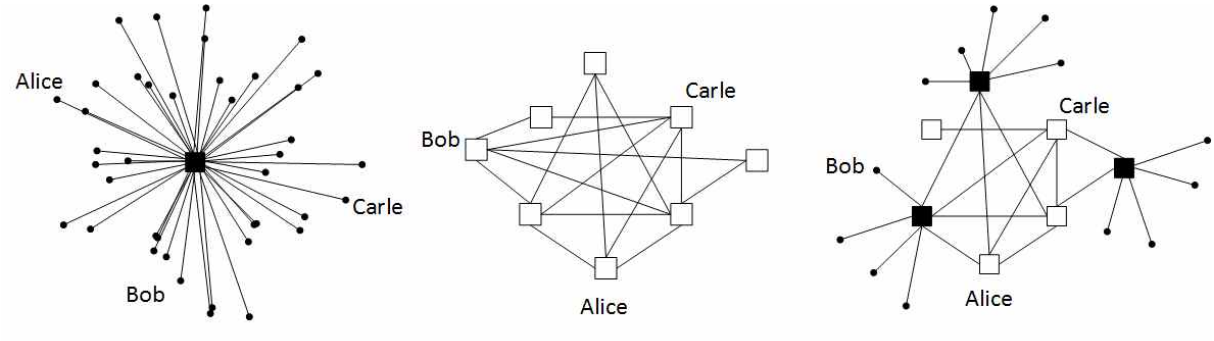

Fig.2. The topologies of centralized, distributed, and hybrid OSNs. Dots are representations of participants in the social network, black box is OSN providers. In the distributed and hybrid scenarios, white boxes indicate no distinction between users and providers.

V. Conclusion

Although there are diverse privacy-protection approaches in OSN, the widespread uses in reality are limited, for they are in a dilemma in utility and privacy usually. Hence, we suggest three concerns in proposing privacy technology:

a) To what extent the compromise in usability is acceptable? Such as the accuracy in recommender will definitely decreased while emphasize on privacy protection, but uses can bear it if the accuracy is not low.

b) How much users will care about this design? It seems that great amount of people call for privacy protections, but the study indicates that most of uses are using default setting in Facebook actually[11], for they have no idea about what they need and results in leakages. Therefore, when achieving privacy goals in the Back-end, should we offer some corresponding, and more intelligent technologies in user-computer interaction to help users understanding in privacy?

c) Will this approach invade the existed economic interests? Such as users can enjoy free services in OSN because we leak partial data to advertisers or other parties. But when moving to distribute OSN, who will support the technologies?

If the technology can solve the above questions, in other word, it meets the criteria to apply in reality use.

References

[1] Machanvajjhala and J. Reiter, "Big Privacy: Protecting Confidentiality in Big Data", XRDS, Vol.19, No.1, 2012.

[2] Richard Chbeir and Al Bouna, Bechara (Eds.), "Security and Privacy Preserving in Social Network", Springer, 2013.

[3] Elena Zheleva and Lise Getoor, "Privacy in social networks: A survey."Social Network Data Analytics", Springer, 277-306, 2011.

[4] Ching-man Yeung, Au, et al. "Decentralization: The future of online social networking", W3C Workshop on the Future of Social Networking Position Papers, Vol. 2, 2009.

[5] Anwitaman Datta, et al. "Decentralized online social networks." Handbook of Social Network Technologies and Applications, Springer, 349-348, 2010.

[6] Leucio Antonio Cutillo, Refik Molva, and Thorsten Strufe, "Safebook: A privacy-preserving online social network leveraging on real-life trust", Communications Magazine, IEEE 47.12, 94-101, 2009.

[7] Jonathan Anderson and Frank

Stajano, "Must social networking conflict with privacy?", IEEE Security & Privacy, 11(3), 51-60, 2013.

[8] Balachander Krishnamurthy, "Privacy and Online Social Networks: Can colorless green ideas sleep furiously?", IEEE Security & Privacy, 11(3), 14-20, 2013.

[9] Ina Jain, M. Choudary Gorantla, and Ashutosh Saxena, "An anonymous peer-to-peer based online social network", India Conference, 2011 Annual IEEE.

[10] J. Anderson, "Privacy Engineering for Social Networks", Ph,D Dissertation, Computer Laboratory, Univ. Cambridge, 2012; www.dspace.cam.ac.uk/handle/1810/244239.

[11] Eszter Hargittai. "Facebook Privacy Settings: Who Cares?." First Monday, 15(8) 2010.