Providing Security for user Images stored in Social Networking site

Sarpuru Venkatesh, P.Suresh

Sarpuru Venkatesh, PG Scholar, Dept.of CSE, CREC, Tirupathi, AP, India
P.Suresh, Asst.Professor, Dept. of CSE, CREC, Tirupathi, AP, India

Abstract:

The term "social media" refers to the wide range of Internet-based and mobile services that allow users to participate in online exchanges, contribute user-created content, or join online communities. Online social networks are websites that allow users to build connections and relationships to other Internet users. Social networks store information remotely, rather than on a user's personal computer. Social networking can be used to keep in touch with friends, make new contacts and find people with similar interests and ideas. The relation between privacy and a person's social network is multi-faceted. There is a need to develop more security mechanisms for different communication technologies, particularly online social networks. Privacy is essential to the design of security mechanisms. Most social networks providers have offered privacy settings to allow or deny others access to personal information details. In certain occasions we want information about ourselves to be known only by a small circle of close friends, and not by strangers. In other instances, we are willing to reveal personal information to anonymous strangers, but not to those who know us better, Social media's become one of the most important part of our daily life as it enables us to communicate with a lot of people. Creation of social networking sites such as MySpace, LinkedIn, and Face book, individuals are given opportunities to meet new people and friends in their own and also in the other diverse communities across the world. Users of social-networking services share an abundance of personal information with a large number of "friends." This improved technology leads to privacy violation where the users are sharing the large volumes of images across more number of peoples. This privacy need to be taken care in order to improve the user satisfaction level. The goal of this survey is to provide a comprehensive review of various privacy policy approaches to improve the security of information shared in the social mediasites.

Keywords: *Online information services, web-based services, Content sharing sites; Privacy; Meta data*

1 Introduction

Social networking sites (SNSs) are the most representative result of the rise of the Web 2.0 and its related technologies. In these environments, users publish and share information and services that can be easily accessed by a global audience. The success of these platforms can be effectively measured in terms of number of users, and the results are really stunning. Specifically, main players like Face book or Twitter claim to have more than 800 and 100 million active users respectively [1]. More impressive is the fact that those numbers grow each day and their limit cannot be still envisaged.

With such a huge quantity of users and so many different activities available on SNSs, the amount of user data which can be gathered from those places is especially large and heterogeneous.

The existence of sensitive information among the data publicly shared by the users may represent a relevant privacy threat due to the fact that third parties can gather and exploit that knowledge for their own benefit. More specifically, leakage of personal data, especially one's identity, may invite malicious attacks From the cyberspace, recently, these privacy concerns have been reported to negatively affect the way the users use SNSs.

In this way, a survey presented in [4] shows a strong association between low engagement and privacy concern. Specifically, users who report concerns around sharing control, comprehension of sharing practices or general SNS privacy concern, also report consistently less time spent as well as less posting, commenting and "Likeing" of content. This situation can be harmful for the SNSs since their business model requires large quantities of users generating new content without limit, Therefore, in the last years, the SNSs themselves have provided some privacy settings for their users that allow them to set the privacy level of their online profiles and to disclose either some or none of the attributes in their profiles [5].

However, this privacy-preserving approach suffers from two main problems:

(i)these privacy settings are generally not sufficiently understood by the average users who seldom change the default configuration [6](according to [7], this configuration generally makes most of the user information public [7]; and (ii) this method does not prevent the SNS itself from gathering the sensitive user data, in fact, a relevant percentage of the users are worried about how SNSs protect their privacy [8] due to the fact that they are aware of their data being exploited by advertisers [9].

1.1 Contribution and plan of this paper:

In this paper we propose a new scheme that enables the users of SNSs to decide exactly which individuals can access to their published sensitive data. This implies that other users, third parties or even the SNS itself cannot obtain any protected information if this is not explicitly allowed by the owner. Obviously, this approach does not rely on the active collaboration of the SNS.

The target platform of this proposal is a typical SNS where the user has a profile, a list of friends and a place to publish photographs or images (e.g., Photo Album or similar). Even though the proposed mechanism can be deployed in any SNS that fulfils those requirements, in this work, we have implemented it to be used with Face book, Section 2 introduces the state of the art related to the privacy-preserving approaches which can be found in this field of research. Section 3 introduces the system model. Section 4 details our new proposal. Section 5 evaluates the runtime cost of the proposed scheme. Finally, Section 6 reports some concluding

2. Proposed Model:

As explained previously, we propose a new privacy-preserving scheme that enables the users of SNSs to decide exactly which individuals can access to their published sensitive data. We next detail the kind of SNSs which can be the target of our proposal. Then, the requirements of the designed system are provided. Finally, we briefly describe how our system works and its architecture.

2.1Target SNS

Our work has been designed at high level to be integrated with any SNS that offers the following assets: (i) a user profile; (ii) list of friends; and (iii) place to publish photographs or images (e.g., Photo Album). The main idea behind the proposed system is to replace the sensitive data that can be found in the "User Profile" section of a SNS with fake information introduced by the user herself. The proposed scheme first uses cryptography to protect the original sensitive information and, then, it hides the ciphered data in a certain image by means of steganography. Access-control techniques are applied to allow only certain users to retrieve the original information. The resulting image is finally published in the place reserved by the SNS to publish images (e.g., Photo Album).When any entity (e.g., users, external third-party, the SNS itself) tries to read the "User Profile" of a protected user, two main situations may apply depending on whether this entity is aware of the privacy-preserving system used or not Due to the fact that Face book is a really well-known SNS that properly fulfils all those requirements, we have chosen this platform to implement our proposal and retrieve some empirical results. Accordingly, Face book is considered the target SNS in the rest of this document. he reader is not aware. In this case, this entity only obtains the fake information introduced by the user who runs the privacy-preserving method. If the target SNS does not allow users to obfuscate their personal information, the introduced fake data must look real in order to fool it. The reader is aware.

In this case, the reader looks in the Photo Album for the image that contains the real information (i.e., the steno-object), obtains the Ciphered data and applies its cryptographic material to retrieve the authentic user profile. At this point, the access control method grants or revokes the reader depending on whether it has been authorized by the user running the

Privacy-preserving system or not Our scheme in detail In this section, we detail the two main algorithms that are used to protect personal data and retrieve it. After that, we focus on the steganographic technique used to hide the protected information in the SNS and also the method used to perform the cryptographic key management which is essential to perform a proper access control on the protected data. Finally, some deploy ability issues are discussed Hiding information from the SNS

As explained previously, SNSs generally do not allow their users to publish fake information in their accounts. Therefore, published fake data must look real in front of the SNS and the protected information must be hidden some- where. In this way, the authors in proposed to store all the protected data steganographed within images published in the SNS itself. Using certain steganograp hic methods, a lot of data can be hidden inside standard images. Unfortunately, in this scenario, achieving a good information rate is not enough. More specifically, we require a steganographic scheme that also provides imperceptibility and robustness. Moreover, it should be oblivious (the recovery algorithm should not require the original unmarked image)

2.2including remarks

In this paper, we have proposed a new system that enables the users of SNSs to protect their personal data. More specifically, by means of our proposal, they can exactly decide which individuals can access to their published information. As a result, even the SNS that hosts the user data cannot obtain any protected information if this is not explicitly allowed by the user. In addition to that, the new scheme has been designed to work properly with well-known SNSs such as Face book.

3. References

1. McMillan, G.: Twitter reveals active user number, how many actually say some-thing. In: Time)
2. Consumer Reports National Research Center: Annual state of the net survey
3. Zhang, C., Sun, J., Zhu, X., Fang, Y.: Privacy and security for online social
networks:
4. Staddon, J., Huffaker, D., Larking, B., Sedley, A.: Are privacy concerns a turn-off?
engagement and privacy in social networks. In: Proc. of the Eighth Symposium on
5. Zheleva, E., Getoor, L.: To join or not to join: The illusion of privacy in social
networks with mixed public and private user profiles.
6. Van Eecke, P., Truyens, M.: Privacy and social networks. Computer Law & Security
7. Bilton, B.: Price of facebook privacy? start clicking. In: The New York Times.(May 2010)
8. Wilson, D.: Users are worried about social network security and privacy.
9. Crimes, S.: Twitter sells old tweets to should users be worried?
10. Dhia, I., Abdessalem, T., Sozio, M.: Primates: a privacy management system for
social networks.