A SURVEY ON PRIVACY IN SOCIAL NETWORKING WEBSITES

Dr. N. Jayalakshmi[1], R.G. Kavitha[2].

[1] Professor, Dept. of Computer Applications, Saveetha Engineering College, Chennai, India.
[2] Assistant Professor, Dept. of Computer Applications, RNS First Grade College, Bangalore, India.

Abstract - Most Social Networking Websites facilitate users with the features like online interaction, sharing of information and developing new relationships etc. As a result, more and more data containing personal information such as name, gender, age, birthday, email address, phone number, current university/company, political views and so on are published over the Internet, which might be lead to a serious privacy leakage. Since some of these items are sensitive, access control is widely employed in order to protect the privacy of users. The current protection mechanisms, such as privacy policies and access control mechanisms fall short on protecting the privacy of the users. This paper presents a survey on different frameworks for privacy enhanced social networking websites, which technically enforces the protection of the personal information of a user, when interacting with social applications.

Keywords: *Privacy, Social Networking Sites, trust, privacy watch, privacy crypt, Hippocratic Social Network*

1. Introduction

Social networking websites have become a potential target for attackers due to the availability of sensitive information as well as its large user base. Therefore, privacy and security issues in online social networks are increasing. Privacy issue is one of the main concerns, since many social network users are not careful about what they expose on their social network space. Many social networking sites try to prevent the exploitations, but many attackers are still able to overcome those security counter measures by using different techniques. Social network users may not be aware of such threats. A survey on different privacy frameworks in social networking websites to prevent from the privacy issues are discussed in this paper.

2. OAUTH (Open Authorization) Framework

Mohamed Shehab et al. proposed OAuth framework. It provides a secure and efficient mechanism for authorizing third-party applications without releasing a user's access credentials. OAuth framework increases user privacy by separating the role of users from that of third party applications. Users need not share their private credentials with third party application, instead OAuth issues a new set of credentials. These new credentials are represented via an Access Token. An access token is a string which denotes a unique set of permissions granted to a third party application. After getting the approval from the resource owner, an authorization server issues access token to the third party application. Authorization code flow is shown in the figure 1. The authorization flow process consists of three parties: End-user (resource owner) at browser, Client (third-party application), Authorization server (e.g., Facebook). When a third party application needs to access user's resources, it presents its Access Token to the service provider. The authorization server authenticates the end user, and decides whether to grant or deny the third-party application's access request [1].

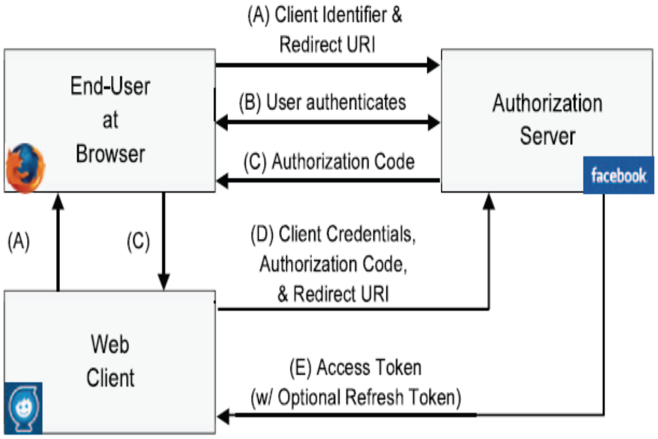
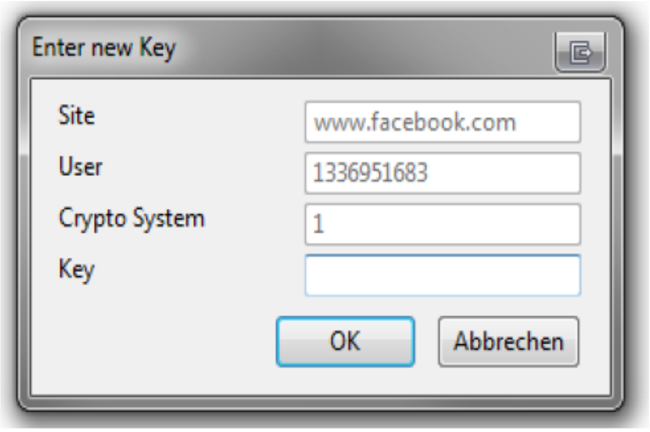

(A) Client Identifier & Redirect URI
End-User at Browser
(B) User authenticates
Authorization Server
(C) Authorization Code
facebook
(A)
(C)
(D) Client Credentials, Authorization Code, & Redirect URI
Web Client
(E) Access Token (w/ Optional Refresh Token)

Figure 1. Authorization code OAuth flow.

3. Privacy Crypt

Robert Koch et al. implemented a prototype called Privacy crypt. It uses two core modules (the crypto-module and encoding module) and the page module. It is an extension of well known Firefox browser. It ensures the privacy of data released on public severs in the internet. When the user requests a website, a small key-icon is shown in the status bar of the Firefox browser. On clicking the icon, a dialog box will be displayed. Figure 2 shows the dialog box which asks the user to enter the key. The key is stored in the database as strings. Once the key is entered, the user can work just as usual. When the user sends a new status message, privacy crypt encrypts it and sends the cipher to the server. The user can not see the encrypted text. Both the encryption and decryption process are fully transparent and carried out in the background. The friends of the user must enter this key. Then the cipher text is decrypted and the readable message is shown as usual. Therefore the user and his friends who know the key can only read the message. Using Privacy crypt, the user can control the distribution of her data in an easy and effective way [2].


Enter new Key

Site www.facebook.com
User 1336951683
Crypto System 1
Key

Figure 2. Dialog for entering a new encryption key

4. Privacy Management Models

Gorrell P Check et al. proposed two privacy management models namely Group-based policy Management with assisted friend grouping and Same-as Policy Management. Gorrell P Check et al. predefined ten relationship groups: family, close friends, graduate school, under graduate school, high school, work, acquaintances, friends of friend, community, and other. Group based policy management helps the user to populate groups based on relationship. It also assigns object permissions to the groups. Assisted friend grouping assists in grouping their friends and setting friend level exceptions within the group policy. Figure 3 shows role based access control. Same-as policy management leverages users' memory and opinion of their friends to set policies for other similar friends [3].

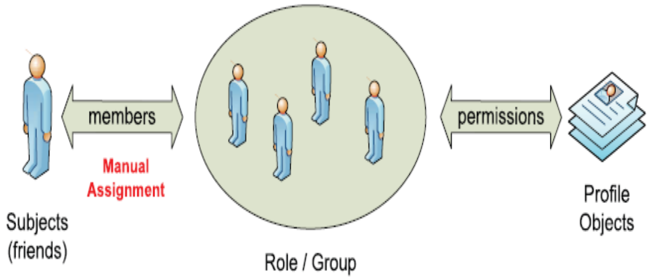


Figure 3. Role based access control.

5. Digital Image Authentication Model

The images from social networking websites can be easily downloaded, edited, morphed and shared. The validation of the ownership is practically impossible due to high degree of replication. Nidhi Grover et al. proposed digital image authentication model to secure the unintentional use of personal images by someone else. Embedding algorithm and extraction algorithm are used in this model.

The subscriber's login detail and current timestamp will be converted to binary and it will be hidden the original image. It is done using embedding algorithm. Embedding algorithm is shown in figure 4.

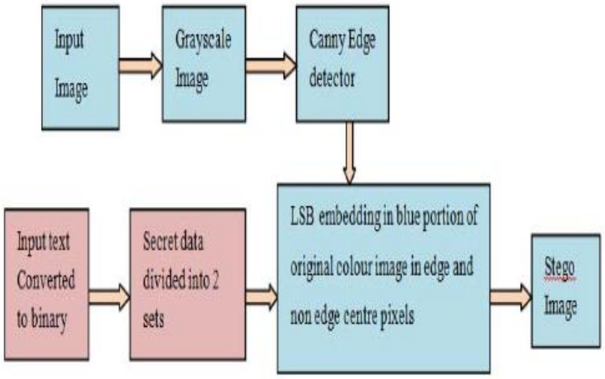

Input Image
Grayscale Image
Canny Edge detector
Input text Converted to binary
Secret data divided into 2 sets
LSB embedding in blue portion of original colour image in edge and non edge centre pixels
Stego Image

Figure 4. Embedding Block diagram

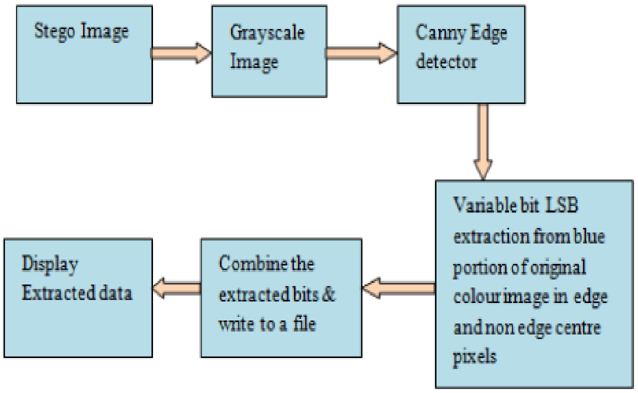

Stego Image
Grayscale Image
Canny Edge detector
Variable bit LSB extraction from blue portion of original colour image in edge and non edge centre pixels
Combine the extracted bits & write to a file
Display Extracted data

Figure 5. Extraction Block Diagram

If any fake user tries to use the original image for creating a fake ID, SN provider compares it with the original embedded data and detects the fake use. It is done by extraction algorithm. Misuse of the images can be prevented using the model is shown in figure 5 [4].

6. Multiparty Access Control (MPAC) model

Hongxin Hu et al. introduced MPAC model. MPAC model enables the protection of shared data associated with multiple users in SNS. MPAC model enforces privacy concerns over data associated with multiple users in SNS. It describes relationships of five individuals, Alice (A), Bob (B), Carol (C), Dave (D), and Edward (E), along with their groups of interests. Figure 6 shows an example of Multiparty social networking. It shows that the users may be directly connected by more than one edge labeled with different relationship types. In addition, the users may also have transitive relationship, such as friends-of-friends (FOF), colleagues-of-colleagues (COC) and classmates-of-classmates (LOL). It is noticed that some data items have multiple controllers and some users may be the controllers of multiple data items. It also shows that the users can participate in the fashion and hiring group. Some users can also join in multiple groups. Thus MPAC model can greatly enhance the flexibility for regulating data sharing in SNSs [5].

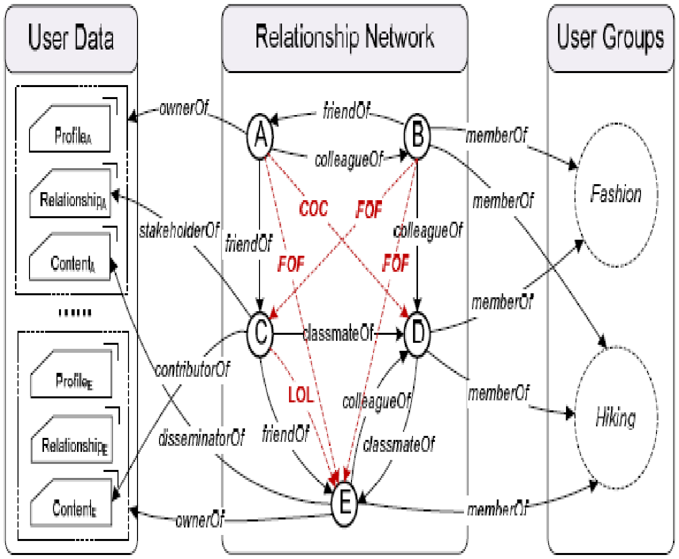
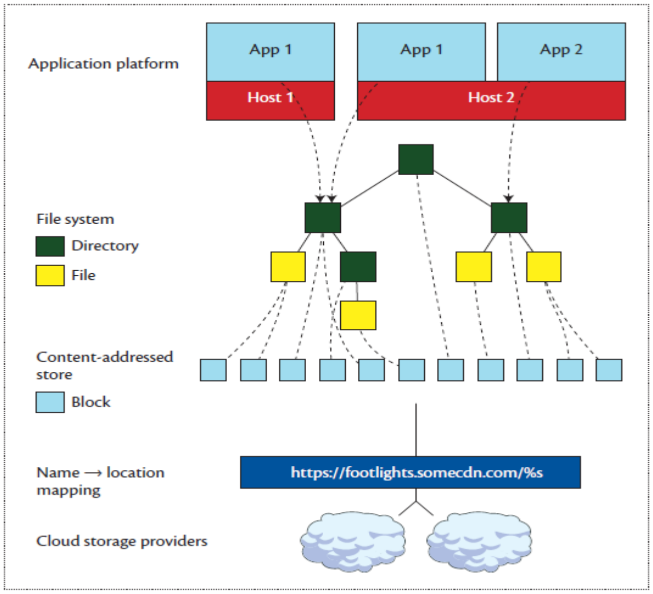


Figure 6. An example of multiparty social network presentation.

7. Footlights

Jonathan Anderson et al. designed and implemented an architecture called footlights. Footlight's design constraint is trust. Users need not trust any third party with their private data.



Footlight uses cloud storage providers to hold user data. This data is broken into fixed sized blocks and then encrypted. When the users share with their friends, footlights reveals encryption keys to the client software of the chosen users only. The local Footlights client software interprets blocks that have been shared with it as a file system. The subsets of these data can be exposed to applications through a security API. Figure 7 shows file system layers visible to applications. Footlights provide an API that lets applications work with user data but not leak it beyond the user's consent.

Applications bundle files in a directory to be shared with other users, but footlights allows sharing only with explicit expression of user intent. Applications can access data such as photos directly if the user explicitly expresses intent [6].

Figure 7. File system layers visible to applications.

8. Privacy watch

Esma Aïmeur et al. introduced privacy watch framework. Privacy watch provides users with an easy and flexible to specify and communicate their privacy concerns to other users, third parties and SNS service provider. There are four privacy levels: No Privacy, Soft Privacy, Hard Privacy and Full Privacy. Based on his privacy level, the user can determine how much information he would like to share with the provider. Figure 8 shows the overview of Privacy watch.

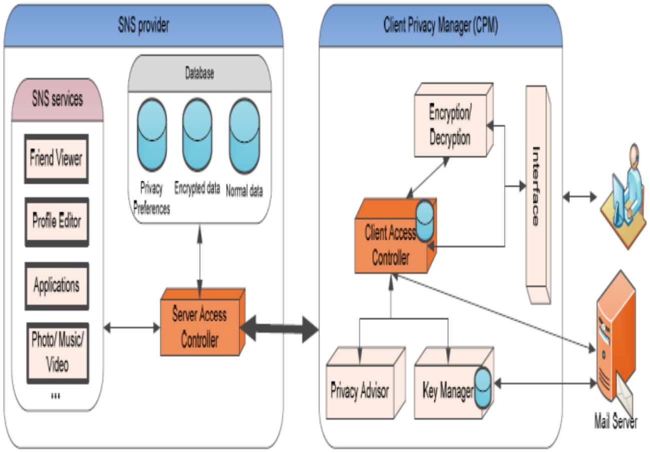


Figure 8. Overview of Privacy Watch

Server access control in privacy watch manages the access control mechanism to the personal information of the user for his friends. It acts as a proxy sitting between the personal information of the user and his friends. The SNS server is responsible for strong the personal information of the user. The users have Client Privacy Manager. It is responsible for helping the user to maintain their sovereignty of their personal information. Privacy watch relies on third party email server such as Hotmail and Gmail. It is used to store and exchange encryption and decryption keys as well as UPP (User Privacy Policy) between users.

The user generates a public verification key for each group and transmits it to the SNS server. Each friend of the group will receive the private signature key through an email. Using the private signature key, a friend of the user can sign messages. The SNS server can use the public verification key of the group to check the validity of the signature. Thus Privacy watch fulfills the most of the privacy criteria for a privacy-enhanced social networking site [7].

9. Hippocratic Social Network

Rajneeshkaur Bedi et al. proposed Hippocratic Social network to enhance the user profile privacy in online social network. It has four components:

- Watermarking Module
- SNS Interaction Module
- Data Perturbation Module
- HSN Repository

Watermarking module inserts a visible or invisible watermark in the database record of user profile. This helps in tackling with the profile cloning attacks. SNS interaction modules read the request for profile data. It identifies the level of security that has to be added to the profile data. Then it modifies and returns the profile data to the requesting application. Data perturbation module takes the record form SNS interaction module and modifies it using generalization or suppression method. HSN repository has Retention Table, Compliance Table, Consent Table, Sharing Limit, Data Generalization and suppression metadata. Retention table stores the time for which the information will be disclosed to a third party application or another person. Compliance table shows that whether his profile data is disclosed to other user or not. Consent table stores the user's consent about his profile data disclosure in regards of a particular group or a person or a third party application. Sharing limit specifies the number of time the information will be disclosed to a particular user [8].

10. Trust model for SNS

Nafaa Jabeur et al. proposed a trust model for SNS. Trust model deals with five trust aspects: What to trust? , When to trust, Where to trust, whom to trust? and Why to trust? Direct and indirect are two types of trust. Trust may have risks and benefits. Context affects the trust. Trust characterizes the relations of the SNS user with other SNS users. The trust model helps in preventing the leakage of personal data. It also helps in personalizing privacy and trust to better fit the current context, user profile and data context [9].

11. Recommendation for SNS users

Michael fire et al. presented eight recommendations for SNS users to help them improve their security and privacy in Social Network Websites [10]. The eight recommendations are as follows:

- Remove Unnecessary Personal Information.
- Adjust Privacy and Security Settings.
- Do Not Accept Friend Requests From Strangers
- Install Internet Security Software
- Remove Installed Third-Party Applications
- Do Not Publish Your Location.
- Do Not Trust Your SNS Friends.
- Monitor Your Children's SNS Activity.

12. Comparison of various Privacy Models

Foot light Model and OAuth Model authorize the third party application to work with user data but not beyond the user's consent. Privacy Management Model helps to populate groups based on relationship. Digital Image Authentication Model is an efficient model to secure the unintentional use of personal images by someone else. Multiparty Access Control Model enforces privacy concerns over data associated with multiple users in SNS. Privacy Crypt Model, Privacy Watch Model, Hippocratic Model and Trust Model help in protecting the privacy of user profile data.

13. Conclusion

This paper presented the various privacy risks that a user incurs while putting personal information on the Social Networking Websites. It also exposed the privacy frameworks for a privacy enhanced Social networking websites, Social networking sites try to implement different security mechanisms to prevent from the privacy issues, and to protect their users, but attackers will always find new methods to break through those defenses. Therefore, social network users should be aware of all these threats, and be more careful when using them. Social network users should be careful about what they expose on their social network space.

REFERENCES:

1. Mohamed Shehab et al., Recommendation Models for Open Authorization, IEEE Transactions on dependable and secure computing, Vol. 9, No. 4, July/August 2012.
2. Robert Koch et al., Data Control in Social Networks, 978-1-4577-0460-4/11/$26.00 ©2011 IEEE.
3. Gorrell P. Cheek et al., Human Effects of Enhanced Privacy Management Models, IEEE Transactions on dependable and secure computing, Vol. 11, No. 2, March/April 2014.
4. Nidhi Grover et al., Digital Image Authentication Model Based on Edge Adaptive Steganography, 2013 Second International Conference on Advanced Computing, Networking and Security.
5. Hongxin Hu et al., Multiparty Access Control for Online Social Networks: Model and Mechanisms, IEEE Transactions on Knowledge and Data Engineering, Vol. 25, No. 7, July 2013.
6. Jonathan Anderson, Frank, Must Social Networking Conflict with Privacy, Co published by the IEEE Computer and Reliability Societies May/June 2013.
7. Esma Aïmeur, Sébastien Gambs, Ai Ho, Towards a Privacy-enhanced Social Networking Site, 2010 International, Reliability Conference on Availability and Security.
8. RajneeshKaur Bedi, Nitinkumar Rajendra Gove, V.M. Wadhai ,Hippocratic Social Network ,2013 Fifth International Conference on Computational Aspects of Social Networks (CASoN).
9. Nafaâ Jabeur, Sherali Zeadally, Sergey Maydebura, Improving Trust and Privacy Models in Social Networks, 978-1-4673-0229-6/12/$31.00 ©2012 IEEE.
10. Michael Fire et al., Online Social Networks: Threats and Solutions, IEEE Communication surveys & Tutorials, Vol. 16, No. 4, Fourth Quarter 2014.

Author Name	**Name of the Privacy Model**	**Features**
Mohamed Shehab	OAuth Model	It uses the concept of Access Tokens to authorize the third party applications
Robert Koch	Privacy Crypt Model	Using Crypto module, Encoding module and Page module, it can control the distributions of user's data in an easy and effective way.
Gorrell P. Cheek	Privacy Management Models	It uses Clustering techniques to group the friends. We can also set the policies for friends of friends.
Nidhi Grover	Digital Image Authentication Model	Using Embedding algorithm and Extraction algorithm, it secures the unintentional use of personal images by someone else.
Hongxin Hu	Multiparty Access Control Model	It enables the protection of shared data associated with multiple users in SNS.
Jonathan Anderson and Frank	Footlights Model	It provides an API that lets applications work with the user data but not leak it beyond the user's consent.
Esma Aïmeur, Sébastien Gambs, Ai Ho	Privacy Watch Model	Based on the privacy level set by the user, it protects the user privacy.
RajneeshKaur Bedi ,Nitinkumar Rajendra Gove, V.M. Wadhai	Hippocratic Model	It protects the privacy of user profile data based on the user consents. It uses different modules and tables.
Nafaâ Jabeur, Sherali Zeadally, Sergey Maydebura	Trust Model	It helps in personalizing privacy and trust to better fit the current text, user profile and data context.