Confidentiality in social networks with third party applications

Syed Azharuddin¹, Mohammed Osman² and Ms Shahana Tanveer ³

¹M.Tech, Scholar at Lords Institute Of Engineering & Technology,
Hyderabad, Andhra Pradesh, India.

²M.Tech, Scholar at Lords Institute Of Engineering & Technology,
Hyderabad, Andhra Pradesh, India.

³Associate professor at Lords Institute Of Engineering & Technology,
Hyderabad, Andhra Pradesh, India.

Abstract: As the development of Web 3.0 technologies the advantages are: improved information linking, more capable searching, more efficient web browsing and increased communication where the online social networks are able to provide a broader platform to enable the flawless sharing of their profile data by trusting the social network interfaces. These open interfaces pose serious privacy concerns since they are given access permissions to the third party applications and the main focus is on user interactions in a social network by ignoring the third party applications. We propose an access control framework in this paper which is capable of managing the third party application by enabling the user to specify the data attributes to be shared with the application by using artificial intelligence which formulates minimal attribute generalization and we propose a solution that maps with the shortest path problem to find the minimum set of attributes by cryptography that generalizes the access of application services. We used the weka tool to produce the results.

Keywords: Web 3.0, social networks, privacy, cryptography.

1. INTRODUCTION

With the development of Web 3.0 technologies a variety of online social networks are intended to provide open platforms that enables the seamless searching and sharing of a user profile data to enable public developers to interface and extend the social network services as application program interfaces such as, mylife, Facebook, etc.

These applications provides anyone to create a software plug-in which can be added to user profiles to provide services based on profile data which also includes serious privacy risks as the user’s profile in fact have a great commercial value for marketing companies, competing networking sites, and identity thieves.

Now a day’s social networking sites are acting as the major means of internet access by millions of users throughout the world where these sites allows us to share a lot more information with friends, some of the most used social network sites are: mylife, Facebook, Twitter and MySpace has created many interesting and challenging security and privacy problems where a user manages his/her profile, communicates with other users, and participates into different communities and also includes some basic information such as user name, date of birth, communication address, contact details, email, education, hobbies, photographs, music, videos, and many more attributes. The below is the figure representing the daily active users according to the results of a survey conducted:

![Figure 1 daily active users in a social network](image)

Social networks platforms have privacy concerns as they have been raised growing concerns amongst users on the dangers of giving out too much personal information and the threat of sexual predators and also the users of these services must be aware of data theft or viruses where as some services such as MySpace and Netlog works with the law enforcement to try to prevent such incidents.

While installing social network applications users have to grant the applications all the requested permissions in order to successfully complete the installation process below are the figures which specify the application permission request displayed by the Google and Facebook platforms respectively when the user attempts to install an application.

![Figure 2 Criminal case game of facebook social networking site](image)
2. RELATED WORK

Information security must evolve from just an Information Technology project to the core of critical business decisions where one must protect enterprise data from compromise and drive innovation at the same time where the main question lies is are you supporting business outcomes or inhibiting them?

Enormous number of studies has been conducted in the past few years which are based on the identification of need for solutions to address the problem of information leakage or data leakage detection in the areas of social networks that are based on interpersonal relationships and are very flexible social interactions.

Some related works have analyzed both privacy risks associated with information disclosure in a social network and developed a initial mechanisms that are tend to protect against some un-voluntary information disclosure by providing a framework for deriving a privacy score based on some algorithms to inform the user of the potential risks to their privacy that represents their activities with other users within the social network by mitigating against these information leakage channels.

2.1 Identity & Access Management

The identity access is more important than ever as the organizational boundaries continue to evolve where a user needs a well developed identity and access management program to drive cost cutting and business agility and also support new product innovation by supporting users anytime and anywhere.

- **Stateless Identities:** This deal with what identities standards are mission critical for your basic information security programs and are you prepared to offer consistent identity services to users and what best practices do you need to support the identity in the cloud.

- **Authentication:** a user should explore stronger authentication to raise identity assurance levels in order to do so we need to consider what emerging authentication techniques.

- **Information Protection:** due to growing amounts of data make us harder to secure enterprise information and we need to assess that how much more data do we need to detect an advanced attack and is it possible to protect your enterprise from malicious activity.

2.2 Cryptography in a social network

Majorly there exist two tasks for encryption in the development of online social network where first one is to restrict the information that is being available to applications as precisely as possible so that the individual applications are not entrusted with large volumes of personal information as it is tempting to focus only on the exchange of information with friends where there exist some applications that may benefit from limited access based on a users profile or messages instead of having broad exposure. The second task is to restrict the information that is most often which is shared with the friends that might be appropriate as the term friend.
includes family, neighbor, peer, boss, etc, regardless of the actual relationship.

The above said two problems can be easily solved by imparting users define access policies that include or exclude defined groups of friends accessing information by which a use can post on his wall stating “busy at work” such that no other user can disturb. To provide this type of functionality more efficiently without the implementation of a trusted application provider we require some form of cryptographic support for group keying.

### 3. SOCIAL NETWORK API’S

Almost all the current social networking web sites are exposing their services by providing web programming interfaces (APIs) due to the development of web 3.0 technologies. For example Facebook Web API provides a programming interface to query pages related to users through Facebook user developed applications similarly several social network web sites have released APIs that allow developers to attain and aggregate the information stored in user profiles and provide extended social network services where as a API is basically a set of web services that provide a limited and controlled view for the application to interface with the social network site with a architecture as shown in below figure.

![Architecture of Social network system](image)

**Figure 4** Architecture of Social network system

Users’ profiles are the unique combinations of different data items that are associated with each data item that is defined over a finite domain of values for a user say i, with a set of attributes $A = \{a_1, a_2, ..., a_n\}$ in a domain $D$ that also includes a null value $\phi$. A generalization disclosure policy that is being accomplished by assigning a disclosed value that is more general than the original attribute value for example a user can make the address information less specific by omitting the street and city and revealing just the zip code which is depicted in the below figure that shows an example of a partial value generalization hierarchy of the address attribute.

![Address field partial value hierarchy generation](image)

**Figure 5** Address field partial value hierarchy generation.

### 4. CRYPTOGRAPHY

For building a social network there are two tasks for encryption where the first is to restrict the information available to applications as precisely as possible and the second task is to restrict the information shared with friends to what might be appropriate. These two problems may be easily solved using the abstract goals of hiding personal information from aggregators and hiding personal information from other users by refining these goals down to concrete requirements for cryptographic methods.

#### 4.1 Public Key Approach

Each user must generate an asymmetric key-pair and distributes the public key out-of-band to other users with whom they want to share data such as friends by allowing the users to create groups and choose which users are part of a given group which can be control access to personal data by encrypting groups by allowing users to have fine-grained control over access policy, which permits exchanging data with more restrictions.

Cryptographic primitives must be designed such that it must allow users to flexibly specify and encrypt groups which may defined by users using some specific criteria where as we expect users to choose groups based on transparent relationships such as neighbor or co-worker or on attributes such as cricket fan or beast buddy and these groups created by one user should be available for use and not just for decryption but also for encryption by friends.

As we know that by combining the traditional public-key and symmetric cryptography to generate an efficient group of encryption primitives where a user encrypts a newly generated group key with the public key of each member of the new group and then distributes this key to the members of that group and uses the key to encrypt messages to the group where the group key may be symmetric such that only group members can encrypt to the group and if it is asymmetric key then non-members are allowed to encrypt as well.

In order to send or broadcast a new group key process that may include sending of a created new message to all the friends where this process may include both the keys and the data in the same object for efficiency reusing a group and key for many messages could require separating the keys from the data and caching the group key for use on later messages.

As this protocol is computationally inexpensive since it does not require digital signatures which probably an attacker could do is provide a faulty key that would soon be discovered and the original creator can enumerate any set of friends to include in the group. A user can encrypt with one group key and then the other but the colluding members of each set could decrypt the message intended for only the members with both attributes and keys. If we allow the users to encrypt data for non member groups then it requires additional infrastructure which uses an
asymmetric key pair by publishing a list of her groups and their public keys.

4.2 Attribute Based Encryption (ABE) Approach

This approach can be used to implement encryption to groups where a user generates an ABE public key and an ABE master secret key for each friend and then the user can generate an ABE secret key corresponding to the set of attributes that defines the groups that friend should be part of it, in some cases a friend may be part of multiple groups then in such case the system should generate and distribute an ABE attribute secret key that includes all those attributes related to distinct groups in which a user is participating.

Here each encryption must specify an access structure that includes: a logical expression over attributes instead of groups who has an attribute secret key with either attribute which will be able to decrypt the message and can also encrypt it, in this scenario the ABE construction ensures that only friends with both attributes will be able to decrypt the message where as in traditional cryptography approach a single encryption operation is sufficient for a new group and it provides the symmetric key that protects the rest of the message.

5. IMPLEMENTATION

Our approach to assess the proposed solution is a two-fold one. Firstly we investigate the architectural changes that our approach would entail on an existing social network and we develop a proof-of-concept implementation using an existing open source framework for social network sites. Secondly we would like to show the feasibility of our proposed approach by conducting user studies on a widely-used social network platform.

The below algorithm generates minimal preferences:

\[ V \rightarrow V_b, \]
\[ E \rightarrow E_b, \]
for each \( e \in E \)
for each \( b \in UPL \)
if \( h < e \)
\[ c, w = \phi \]
\[ e, v = e, b \times w_a \]
//initializing distance from \( s \)
for each \( v \in V_b \)
\[ d[v] = 0 \]
\[ w[v] = \phi \]
\[ d[s] = 0 \]
//computing shortest path from \( s \)
\[ V_b \rightarrow Q, \]
while \( Q \) is not empty
\[ u = \text{ExtractMin}(Q) \]
\[ u = \{ u \} \rightarrow s \]
for each \( v \in \text{adjacent}(u) \)
if \( d[u] + w(u, v) \)
\[ d[v] = d[u] + w(u, v) \]
\[ u[v] = u \]
\[ u = \text{return up}^* \]
\[ w, u = \{ u(v), u \} \cup u^* \]
\[ u = u(v) \]
while \( u \neq s \)
\[ \text{return up}^* \]

In the above algorithm \( V \) represents vertex, \( E \) represents Edge, \( UPL \) represents User Upper Limit preferences where \( UPL = [h_0, h_1, \ldots, h_n] \) and user target states \( st \) and Application transition graph \( G = (V, E) \). The below is the algorithm for defining relationships and implementing cryptography in a generalized sense:

\[ A \leftarrow \text{ABEKeyGen}(u, \text{AKS}, \text{AA}) \]
\[ C \leftarrow \text{TEncrypt}(u, \text{TKey}, \text{A}) \]
\[ u \leftarrow \text{SSout}(u, \text{TPK}, C) \]
\[ A \leftarrow \text{ABEKeyGen}(\text{APK}, \text{AKS}) \]
\[ C \leftarrow \text{ABEEncrypt}(\text{APK}, A, \text{AS}) \]
\[ u \leftarrow \text{SSout}(u, \text{TPK}, C) \]
\[ \text{AssignRightsToIdentity}(\text{u.rights}, \text{TPK}, r, 0) \]

In the above algorithm \( u1, u2, \text{attrs}, \text{rights} \) are attributes, \( \text{AS} \) stands for access structure and \( r \) denotes resources used to define relationship set. \text{ABEKeyGen}, \text{TEncrypt}, \text{ABEEncrypt}, \text{chACL}, \text{AssignRightsToIdentity}, \text{get} \) are methods implementing the algorithm.

The below is the figure representing the sequence diagram for representing the user and third party server interaction:

![Sequence diagram of user interaction with the third party.](image)

We have developed and implemented this application in educational institute where it is being used by faculty and students in intranet and some of the screens represent the solution space for the problem space is:
The application we designed is an XML RPC server which uses PHP and Apache with a MySQL database as a backend and the service implemented is the storage API. The below are the outputs produced by weka tool which depicts the different attributes of a social networking site such as Address, Age, Interests, Birthday, Occupation, Likes, Movies, Sports.

![Figure 8 attributes mined using WEKA tool]

6.CONCLUSION
In this paper we have presented an framework that controls a for social networks developer applications that enables users to specify profile attribute preferences and requires applications to be designed so to be personalized based on users profile preferences it also provides a privacy enabled solution that is in line with social network ethics and allows users to add useful and entertaining applications to their profiles which are also called as the third party applications where we have modeled the applications as finite state machine with transition labeling indicating the generalization level required to enable application state transitions. We defined the reduced application transition system that only includes the state transitions possible with a given user generalization vector and also by implementation of cryptography that is implementation of trusting the Social networks with data and also shown how ABE and traditional public key cryptography can be combined to provide the flexible, user-defined access control needed in social networks.

References

AUTHOR
SYED AZHARUDDIN has completed his B.Tech degree in Computer Science & Information Technology (2006-2010) from Nizam Institute Of Engineering & Technology, AP and is pursuing his M.Tech degree in Software Engineering at Lords Institute Of Engineering & Technology, A.P. He is also working as Security Delivery Specialist at IBM Global Technology Services Pvt Ltd.

MOHAMMED OSMAN has completed his B.Tech degree in Computer Science & Information Technology (2006-2010) from Nizam Institute Of Engineering & Technology, AP and is pursuing his M.Tech degree in Software Engineering at Lords Institute Of Engineering & Technology, A.P.

Ms Shahana Tanveer has completed her M.Tech degree in Computer Science Engineering(2009-2011) from Jawaharlal Nehru Technological University Hyderabad, B.E. degree in Computer Science Engineering(1998-2002) from Gulbarga University and working as associate professor in the CSE department at Lords Institute Of Engineering & Technology, A.P.