International Journal of Computer Science and Engineering Communications,
Volume.4, Issue.2 (2016): Page.1410-1414
www.scientistlink.com/ijcsec

Averting Intruder Attack on Social Network by Data Sanitization

D.Dhivya[1] and R.Venkadeshan[2]
[1]PG Scholar, [2]Assistant Professor,
Computer Science and Engineering,
Chettinad College of Engineering & Technology, Karur, India
dhivya.139@gmail.com[1], venkadengg@gmail.com.com[2]

Abstract: *Online Social Networks offer for social interactions and information sharing among peoples, but it includes security and privacy issues. OSNs allow users to limit access to shared data; OSNs currently do not provide any mechanism to enforce privacy concerns over data associated with multiple users. To overcome this, we put forward an approach which supports the protection of shared data associated with multiple users in OSNs. We are developing an access control model to capture the core of shared authorization requirements, along with a multiparty policy specification scheme and a policy enforcement mechanism.*

Keywords – *anonimizing, elgamal cryptosystem, multiparty access control , Online social network.*

INTRODUCTION

Online social networks (OSNs) such as Facebook, Googleplus, and Twitter are essentially designed to enable people to share personal and public information and make social connections with friends, coworkers, colleagues, family, and even with strangers. In recent years, we have seen unique growth in the application of OSNs. For example, Facebook, one of representative social network sites, claims that it has more than 800 million active users and over 30 billion pieces of content (web links, news stories, blog posts, notes, photo albums, and so on.) shared each month [3]. To protect user data, access control has become a central feature of OSNs [2], [4]. A typical OSN provides each user with a virtual space containing profile information, a list of the user's friends, and webpages, such as wall in Facebook, where users and friends can post content and leave messages. A user profile usually includes information with respect to the user's birthday, gender, interests, education, and work history, and contact information. In addition, users can not only upload a content into their own or others' spaces but also tag other users who appear in the content. Each tag is an unambiguous reference that links to a user's space. For the protection of user data, current OSNs indirectly require users to be system and policy administrators for regulating their data, where users can restrict data sharing to a specific set of trusted users. OSNs often use user relationship and group membership to distinguish between trusted and untrusted users. For example, in Facebook, users can allow friends, friends of friends (FOF), groups, or public to access their data, depending on their personal authorization and privacy requirements. Although OSNs currently provide simple access control mechanisms allowing users to govern access to information contained in their own spaces, users, unfortunately, have no control over data residing outside their spaces. For instance, if a user posts a comment in a friend's space, she/he cannot specify which users can view the comment. In another case, when a user uploads a photo and tags friends who appear in the photo, the tagged friends cannot restrict who can see this photo, even though the tagged friends may have different privacy concerns about the photo. To address such a critical issue, preliminary protection mechanisms have been offered by existing OSNs. For example, Facebook allows tagged users to remove the tags linked to their profiles or report violations asking Facebook managers to remove the contents that they do not want to share with the public. However, these simple protection mechanisms suffer from several limitations.

RELATED WORK

The area of privacy inside a social network encompasses a large breadth, based on how privacy is defined. In [4], Backstrom et al. consider an attack against an anonymized network. In their model, the network consists of only nodes and edges. Detail values are not included. The goal of the attacker is simply to identify people. In systems which include e-mail and messaging networks, one needs to set up the data to protect the privacy of individual users while preserving the global network properties. This is done through anonymization, a simple procedure in which each individual's "name" e.g., e-mail address, phone number, or actual name is replaced by a random user ID, but the connections between the people are revealed. Anonymization is intended to exactly preserve the pure unannotated structure of the communication graph while suppressing the "who" information. In anonymized social networks, passive attacks are carried out by individuals who try to learn the identities of nodes only after the anonymized network has been released. In contrast, an active attack tries to compromise privacy by strategically creating new user accounts and links before the anonymized network is released, so that these new nodes and edges will then be present in the anonymized network. The active attacks will make use of the following two types of operations. First, an individual can create a new user account on the system. This adds a new node to G. Second, a node u can decide to communicate with a node v, this adds the undirected edge (u, v) to G. The goal of the attack is to take an arbitrary set of targeted users w1, . . . ,wb, and for each pair of them, to use the anonymized copy of G to learn whether the edge (wi, wj) in fact exists. This is the sense in which the privacy of these users will be compromised. In a passive attack, regular users are able to discover their locations in G using their knowledge of the local structure of the network around them. While there are a number of different types of passive attacks that could be implemented, here we imagine that a small coalition of passive attackers collude to discover their location. By doing so, they compromise the privacy of some of their neighbors those connected to a unique subset of the coalition, and hence unambiguously recognizable once the coalition is found. This work is not directly relevant to all settings in which social network data is used. This paper ignores details and do not consider the effect of the existence of details on privacy. In [5], He et al. consider ways to infer private information via friendship links by creating a Bayesian network from the links inside a social network. While they crawl a real social network, Live Journal, they use hypothetical attributes to analyze their learning algorithm. This work focuses on social network data classification and inferring the individual's private information. More private information is inferred by applying collective classification algorithm. The system explores how the online social network data could be used to predict some individual private trait that a user is not willing to disclose. For instance, in an office, people connect to each other because of similar professions. Therefore, it is possible that one may be able to infer someone's attribute from the attributes of his/her friends. In such cases, privacy is indirectly disclosed by their social relations rather than from the owner directly. This is called personal information leakage from inference. This system uses a collective classification algorithm for classifying the social network data. It has three components: local classifier, relational classifier and collective inference. Relaxation labeling is used as collective inference method. By applying the collective classification method the system could infer (indirect disclosure) the user private information using the released network data. The system showed that, user's private information can be inferred via social relations and release of personal information in the social network. To protect the individual's private information leakage in social networks, the system either hide our friendship relations or ask our friends to hide their attributes. Compared to this work, we provide techniques that can help with choosing the most effective details or links that need to be removed for protecting privacy. Finally, we explore the effect of collective inference techniques in possible inference attacks. In [6], Zheleva and Getoor proposed several methods of social graph anonymization, focusing mainly on the idea that by anonymizing both the nodes in the group and the link structure, that one thereby anonymizes the graph as a whole. The challenge of anonymizing graph data lies in understanding dependencies and removing sensitive information which can be inferred by direct or indirect means. This work concentrates on hiding the identity of entities, considering the case where relationships between entities are to be kept private. In social network data, based on the friendship relationships of a person and the public preferences of the friends such as political affiliation, it may be possible to infer the personal preferences of the person in question as well.

The process of anonymization involves taking the unanonymized graph data, making some modifications, and constructing a new released graph which will be made available to the adversary. The modifications include changes to both the nodes and edges of the graph. The anonymization of nodes creates equivalent classes of nodes. For the edge data, five different anonymization strategies were used. This work proposed several methods of social graph anonymization, focusing mainly on the idea that by anonymizing both the nodes in the group and the link structure, that one thereby anonymizes the graph as a whole. However, their methods all focus on anonymity in the structure itself. Also, much of the uniqueness in the data may be lost. Through method of anonymity preservation in the proposed model, we can maintain the full uniqueness in each node, which allows more information in the data post release. Online social networks, such as Facebook, are increasingly utilized by many people. These networks allow users to publish details about themselves and to connect to their friends. Some of the information revealed inside these networks is meant to be private. Yet it is possible to use learning algorithms on released data to predict private information. [7] Explored how to launch inference attacks using released social networking data to predict private information. And then devise three possible sanitization techniques that could be used in various situations. Then, the effectiveness of these techniques and attempt to use methods of collective inference to discover sensitive attributes of the data set. This approach can decrease the effectiveness of both local and relational classification algorithms by using the sanitization methods described.

PROBLEM DEFINITION

Online social networks (OSNs) have experienced tremendous growth in recent years and become a defect portal for hundreds of millions of Internet users. These OSNs offer attractive means for digital social interactions and information sharing, but also raise a number of security and privacy issues. While OSNs allow users to restrict access to shared data, they currently do not provide any mechanism to enforce privacy concerns over data associated with multiple users.

PROPOSED SYSTEM

We pursue a systematic solution to facilitate collaborative management of shared data in OSNs. We begin by examining how the lack of multiparty access control (MPAC) for data sharing in OSNs can undermine the protection of user data. Some typical data sharing patterns with respect to multiparty authorization in OSNs are also identified. Based on these sharing patterns, an MPAC model is formulated to capture the core features of multiparty authorization requirements that have not been accommodated so far by existing access control systems and models for OSNs. Our model also contains a multiparty policy specification scheme. Meanwhile, since conflicts are inevitable in multiparty authorization enforcement, a voting mechanism is further provided to deal with authorization and privacy conflicts in our model. The hash-based protocol takes a one-way hash function as its underlying crypto system; its computational costs are extremely low. We have proposed a P2P-based batch authentication framework for OSNs. We have also designed three batch authentication protocols using the one-way hash function, ElGamal proxy encryption, and certificates for different situations and purposes. The hash-based protocol adopts lightweight cryptosystems to reduce the computational costs. To offer higher security properties, the proxy- and certificate based methods are based on asymmetric encryption and signature methods to fulfill the security requirements of sensitive transactions.

Different goals: In conventional group key management protocols, a group is formed for a temporary purpose. The group is dismissed when that temporary purpose is served, and then, the group members lose relationships with other group members. Our social-based batch authentication protocols are designed for authenticating friends in OSNs. Once a group member is authenticated, he/she can help friends for another batch authentication. Such authentications protocols help extend the social network of a user.

Different behaviors: In most group key management protocols, group members are authenticated by the group leader "one by one." That is, n authentication messages are required to authenticate n group members. Then, these members share one common group key for the group communication. In our batch authentication protocols, users are simultaneously authenticated by the requester. That is, one authentication message is required to authenticate n session peers. Then, the requester negotiates one secret key with each user instead of sharing one group key among all users.

POST WALL CREATION

The Website wallpost is the most social network is enabling with photo sharing activities. Protected albums allow users to set their albums with access protection. This is one of the beneficial features from wallpost that who fear with photo scams on photo sharing websites. Photo tagging the option makes the photo search easier after a long period of time. Here reuse can give the names or keywords for photos that related to the photo in better to recognize easily. Although OSNs currently provide simple access control mechanisms allowing users to govern access to information contained in their own spaces, users, unfortunately, have no control over data residing outside their spaces. In this user can add their or interested photos in their wall. This wall posting contains the photo, photo description, tag information are given by the user that details are stored in the OSNs database.

MPAC Model

An OSN can be represented by a relationship network, a set of user groups, and a collection of user data. The relationship network of an OSN is a directed labeled graph, where each node denotes a user and each edge represents a relationship between two users. The label associated with each edge indicates the type of the relationship. Edge direction denotes that the initial node of an edge establishes the relationship and the terminal node of the edge accepts the relationship. The number and type of supported relationships rely on the specific OSNs and its purposes.

MULTIPARTY POLICY EVALUATION

Two steps are performed to evaluate an access request over MPAC policies. The first step checks the access request against the policy specified by each controller and yields a decision for the controller. The accessor element in a policy decides whether the policy is applicable to a request. If the user who sends the request belongs to the user set derived from the accessor of a policy, the policy is applicable and the evaluation process returns a response with the decision (either permit or deny) indicated by the effect element in the policy. Otherwise, the response yields deny decision if the policy is not applicable to the request. In the second step, decisions from all controllers responding to the access request are aggregated to make a final decision for the access request. Since data controllers may generate different decisions (permit and deny) for an access request, conflicts may occur. To make an unambiguous decision for each access request, it is essential to adopt a systematic conflict resolution mechanism to resolve those conflicts during multiparty policy evaluation.

ADVANTAGES OF PROPOSED SYSTEM

1. The proposed framework reduces the communication cost required for authenticating users.
2. Due to their different security properties, the proposed protocols can be realized on a variety of devices such as personal digital assistants (PDAs), mobile phones, and laptops.
3. By incorporating different trust levels, the proposed protocols allow a user with a high trust level to help authenticate other users and achieve the extensibility of a social network.
4. The proposed protocols support a one-to-many authentication, which is the basis of batch authentication, to simultaneously authenticate multiple users. To the best of our knowledge, this paper is the first study that offers one- to-many batch authentication in P2P-based OSNs.
5. Spam classification method is used to filter the message as illegal or good message.

EXPECTED RESULTS

An online social networking site is created. Users can register and login into the site. The user can find friends, share data, pictures etc. One can post data on other’s wall. New groups can be created. Users can upload photos by tagging their friends and also the can set the privacy for the photos being shared. Privacy can be provided as public or private. Data shared in private will be viewed only by the user’s friends. Different inference attacks are launched on the data released in this social network site. The data is usually achieved through the private information leakage by sharing with friends or by other ways. These attacks can be prevented by removing certain details from the node as well as removing some links between the nodes. Classifier technique used will provide higher accuracy in the classification process compared to other techniques. That is mainly by data generalization. More distant the friendship link between two nodes, the more generalized data will be viewed by the friend.

CONCLUSION

We addressed various issues related to private information leakage in social networks. We show that using both friendship links and details together gives better predictability than details alone. In addition, we explored the effect of removing details and links in preventing sensitive information leakage. In the process, we discovered situations in which collective inference does not improve on using a simple local classification method to identify nodes. When we combine the results from the collective inference implications with the individual results, we begin to see that removing details and friendship links together is the best way to reduce classifier accuracy. This is probably infeasible in maintaining the use of social networks. However, we also show that by removing only details, we greatly reduce the accuracy of local classifiers, which give us the maximum accuracy that we were able to achieve through any combination of classifiers.

REFERENCES

[1] Facebook Beacon, 2007.

[2] K.M. Heussner, “„Gaydar‟ n Facebook: Can Your Friends Reveal Sexual Orientation?” http://abcnews.go.com/Technology/gaydar-facebook-friends/story?id=8633224#. UZ939UqheOs, Sept. 2009.

[3] C. Johnson, “Project Gaydar,” The Boston Globe, Sept. 2009.

[4] L. Backstrom, C. Dwork, and J. Kleinberg, “Wherefore Art Thou r3579x: Anonymized Social Networks, Hidden Patterns, and Structural Steganography,” Proc. 16th Int‟l Conf. World Wide Web (WWW ‟07), pp. 181-190, 2007.

[5] J. He, W. Chu, and V. Liu, “Inferring Privacy Information from Social Networks,” Proc. Intelligence and Security Informatics, 2006.

[6] E. Zheleva and L. Getoor, “Preserving the Privacy of Sensitive Relationships in Graph Data,” Proc. First ACM SIGKDD Int‟l Conf. Privacy, Security, and Trust in KDD, pp. 153-171, 2008.

[7] Raymond Heatherly, Murat Kantarcioglu, and Bhavani Thuraisingham, “Preventing Private Information Inference Attacks on Social Networks”, 2013