PriGuard: A Semantic Approach to Detect Privacy Violation in Online Social Networks

Abstract-Social network users expect the social networks that they use to preserve their privacy. However, in online social networks, privacy breaches are not necessarily. In this proposed, first categorizes to protect the consumer that take place in online social networks. Our proposed approach is based on agent-based representation of a social network, where the agents manage users’ privacy requirements by creating commitments with the system. The proposed detection algorithm performs reasoning using the description logic and commitments on a varying depths of social networks. The proposed detection algorithm performs reasoning using the description logic and commitments on a varying depths of social networks.

Keywords-Social Networks, Facebook, Privacy, Filtering.

INTRODUCTION

Online social systems have become an important part of everyday life. While initial examples were used to share personal content with friend’s. Generally, these systems serve a large number of users; however each user shares content with only a small subset of these users. This subset may even change based on the type of the content or the current context of the user. For example, a user might share contact information with all of her acquaintances, while a picture might be shared with friends only. If say, the picture shows the person sick, the user might not even want all her friends to see it. That is, privacy constraints vary based on person, content, and context. This requires systems to employ a customizable privacy agreement with their users. However, when that happens, it is difficult to enforce users’ privacy requirements.

ADVANTAGES

The aim of the present work is therefore to propose and experimentally evaluate an automated system, called Filtered Wall (FW), able to filter unwanted messages from OSN user walls. To specify Filtering Rules (FRs), by which users can state what contents, should not be displayed on their walls. Both the security and efficiency of our proposed scheme Identified the unwanted Content.

Can’t able to leak the information

Providing intimation through the Email

DISADVANTAGES

In the existing Online Social Networks, provide very little support to prevent unwanted messages on user walls. For example, Facebook allows users to state who is allowed to insert messages in their walls (i.e., friends, friends of friends, or defined groups of friends). However, no content-based preferences are supported and therefore it is not possible to prevent undesired messages, such as political or vulgar ones, no matter of the user who posts them.

Profile Leakages

No filtering Approach

© 2017, IJARIIT All Rights Reserved
Prevention concepts implements
Collusion Attack
Less Intimation

TYPES

- Network scenario
- Filtering rules
- Online setup assistant for FRS thresholds
- Blacklists
- Blocked unwanted message
- Relative frequency
- Mail notification

NETWORK SCENARIO

Given the social network scenario, creators may also be identified by exploiting information on their social graph. This implies to state conditions on type, depth and trust values of the relationship(s) creators should be involved in order to apply them the specified rules. All these options are formalized by the notion of creator specification, defined as follows.

FILTERING RULES

In defining the language for FRs specification, we consider three main issues that, in our opinion, should affect a message filtering decision. First of all, in OSNs like in everyday life, the same message may have different meanings and relevance based on who writes it. As a consequence, FRs should allow users to state constraints on message creators. Creators on which a FR applies can be selected on the basis of several different criteria; one of the most relevant is by imposing possible to conditions on their profile’s attributes. In such a way it is, for instance, define rules applying only to young creators or to creators with a given religious/political view.

ONLINE SETUP ASSISTANT FOR FRS THRESHOLDS

As mentioned in the previous section, we address the problem of setting thresholds to filter rules, by conceiving and implementing within FW, an Online Setup Assistant (OSA) procedure. OSA presents the user with a set of messages selected from the dataset discussed in Section VI-A. For each message, the user tells the system the decision to accept or reject the message. The collection and processing of user decisions on an adequate set of messages distributed over all the classes allows to compute customized thresholds representing the user attitude in accepting or rejecting certain contents. Such messages are selected according to the following process. A certain amount of non neutral messages taken from a fraction of the dataset and not belonging to the training/test sets, are classified by the ML in order to have, for each message, the second level class membership value.

BLACKLISTS

A further component of our system is a BL mechanism to avoid messages from undesired creators, independent from their contents. BLs are directly managed by the system, which should be able to determine who are the users to be inserted in the BL and decide when users retention in the BL is finished. To enhance flexibility, such information are given to the system through a set of rules, hereafter called BL rules. Such rules are not defined by the SNM, therefore they are not meant as general high level directives to be applied to the whole community. Rather, we decide to let the users themselves, i.e., the wall’s owners to specify BL rules regulating who has to be banned from their walls and for how long. Therefore, a user might be banned from a wall, by, at the same time, being able to post in other walls.

BLOCKED UNWANTED MESSAGE

Similar to FRs, our BL rules make the wall owner able to identify users to be blocked according to their profiles as well as their relationships in the OSN. Therefore, by means of a BL rule, wall owners are for example able to ban from their walls users they do not directly know (i.e., with which they have only indirect relationships), or users that are friend of a given person as they may have a bad sopolion of this person. This banning can be adopted for an undetermined time period or for a specific time window. Moreover, banning criteria may also take into account users’ behavior in the OSN. More precisely, among possible information denoting users’ bad behavior we have focused on two main measures. The first is related to the principle that if within a given time interval a user has been inserted into a BL for several times, say greater than a given threshold, he/she might deserve to stay in the BL for another while, as his/her behavior is not improved. This principle works for those users that have been already inserted in the considered BL at least one time.
In contrast, to catch new bad behaviors, we use the Relative Frequency (RF) that let the system be able to detect those users whose messages continue to fail the FRs. The two measures can be computed either locally, that is, by considering only the messages and/or the BL of the user specifying the BL rule or globally, that is, by considering all OSN users walls and/or BLs.

**MAIL NOTIFICATION**

In the mail contribution it enhance the system by creating a instance randomly notifying a message system that should instead be blocked, or detecting modifications to profile attributes that have been made for the only purpose of defeating the filtering system. Automatically user will get a mail notification.

**DETECTION OF PRIVACY VIOLATIONS**

Detection, PRIGUARD uses the domain information, norms, the view information and the violation statements as depicted in A violation statement is identified for each commitment. PRIGUARD checks the violation statements in the system. A commitment violation means that: osn failed to bring about the consequent of the commitment. The creditor agent should be notified about its commitment violations to take an action accordingly.

**PRIGUARDTOOL**

We develop a tool called PRIGUARDTOOL in Java, which implements the PRIGUARD model described in Section 5. Recall that each user is represented by an agent. The execution is as follows: (i) The user’s agent takes the privacy constraints of its user. (ii) Then the agent processes these constraints to generate corresponding commitments. (iii) The agent sends this set of commitments to PRIGUARDTOOL, which generates the statements wherein these commitments would be violated. (iv) Finally, PRIGUARDTOOL checks whether these statements hold in an ABSN view, which would mean a violation of privacy and notifies the requesting agent about the results.

**CONCLUSION**

This paper introduced a meta-model to define online social networks as agent-based social networks to formalize privacy requirements of users and their violations. In order to understand privacy violations that happen in real online social networks, we have conducted a survey with Facebook users and categorized the violations in terms of their causation. We further propose PRIGUARD, an approach that adheres to the proposed meta model and uses description logic to describe the social network domain and commitments to specify the privacy requirements of the users. Our proposed algorithm in PRIGUARD to detect privacy violations is both sound and complete. The algorithm can be used before taking an action to check if it will lead to a violation, thereby preventing it upfront. Conversely, it can be used to do sporadic checks on the system to see if any violations have occurred. In both cases, the system, together with the user, can work to undo the violations. In the implemented PRIGUARD in a tool called PRIGUARDTOOL and demonstrated that it can handle example scenarios from various violation categories successfully. Its performance results on real-life networks are promising.
ACKNOWLEDGEMENT
First and foremost I bow my heads to LORD almighty for blessing me to complete my paper work successfully by overcoming all hurdles.
I express my immense gratitude to our Correspondent Shri. A. SRINIVASAN and Vice Chairman Shri. R. KATHIRAVAN our Secretary Shri. P. NEELRAJ Dhanalakshmi Srinivasan Educational Institutions, Perambalur, for providing the necessary facilited for completion of this paper.
I admit my heartfelt thanks to my honourable Principal DR. ARUNADINAKARAN our Vice Principal Ms. S. H. AFROZE Dhanalakshmi Srinivasan college of Arts & Science for Women, Perambalur, who gave me permission to do my journal.
I profound my sincere thanks to Miss A. KIRUTHIKA M.C.A., M.Phil., Asst. Prof., of the Department of computer science, Dhanalakshmi Srinivasan college of Arts & Science for Women, Perambalur, for encouraging me to do my paper and giving valuable suggestion for completion of my journal.
I am very proud of my parent who encourages me to do the same. I am rendering my heartfelt thanks to my friends, who helped me to complete this paper.

REFERENCES