IMMORTAL RECIPROCAL INTERFACE METHODOLOGY FOR VIRTUAL SOCIAL NETWORKS

V. Pavani*

1Asst. Prof, Dept. of Information Technology, Vignans Nirula Institute of Science and Technology for Women, Palakaluru, Guntur (A.P), India.

ABSTRACT

Virtual social networks (VSNs) have spectacular development in modern days and become candid portals for hundreds of millions of Internet users. These VSNs offer smart ways for digital social communications and information distribution, but also raise a number of security and discretion issues. While VSNs allow users bound contact to common data, they now do not provide any machinery to apply secrecy concerns over data related with several users. To this end, we offer a better way to enable the safety of shared data connected with multiple users in VSNs. We articulate an immortal Reciprocal interface to capture the spirit of reciprocated approval provisions, along with a reciprocated methodology requirement scheme and a methodology enforcement approach. Also, we present a logical demonstration of our immortal interface methodology that permits us to influence the structures of current rational solvers to achieve numerous scrutiny tasks on our model. We also debate a proof of concept methodology of our approach as part of a presentation in Facebook and provide usability study and system appraisal of our method.

Keywords: Social network, reciprocal interface methodology, security model and methodology specification & management.

1. INTRODUCTION

VIRTUAL social networks (VSNs) such as Facebook, LinkedIn, Google + and Twitter are fundamentally intended to allow people to share personal and public data and make social contacts with friends, associates, social group, clan, and even with foreigners. In recent years, we have perceived unexpected growth in the use of VSNs. For example, Facebook, one of distinctive social network sites, claims that it has more than 960 million active users and over 31 billion pieces of content (web links, news stories, blog posts, notes, photo albums, and so on.) shared each month [1, 3]. To protect user data, Reciprocal Interface Methodology has turned out to be a dominant feature of VSNs [2, 4]. A distinctive VSN provides each user with a replicated memory space having profile information, a list of the user’s friends, and webpages, such as a wall in Facebook, where users and friends can post their posts and leave messages. A user profile typically contains information with reference to the user’s birthday, gender, interests, qualifications, job history, and contact info. Also, users not only upload data into their own or others’ spaces but also label other users who appear in the wall. Each label is an overt reference that links to a user’s space. For the shielding of user data, current VSNs ultimately require users to be system and methodology managers for controlling their data, where users can encompass data allocation to a precise set of trusted users. VSNs often use user relationship and group membership to differentiate between trusted and untrusted users. For example, in Facebook, users can allow friends, friends of friends (FOF), groups, or public to contact their data, depending on their personal approval and privacy necessities.

Though VSNs currently provide simple immortal interface methodologies allowing users to rule contact to info contained in their own spaces, users, inopportunely, have no control over data residing outside their spaces. For example, if a user posts a comment in a friend’s space, she/he cannot state which users can view the comment. In another case, when a user uploads a photo and labels friends who appear in the photo, the labeled friends cannot restrict who can see this photo, even though the labeled friends may have different privacy concerns about the photo. To address such a perilous concern, initial protection methodologies have been offered by
existing VSNs. For instance, Facebook permits labeled users to remove the labels 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 methodologies struggle from several limitations. On one hand, removing a label from a photo can only prevent other members from seeing a user’s profile by means of the association link, but the user’s image is still contained in the photo. Since novel interface methodology can not be changed, the user’s image lasts to be revealed to all authorized users. Conversely, reporting to VSNs only allows us to either preserve or remove the content. Such a binary decision from VSN managers is either too wobbly or too limiting, relying on the VSN’s management and need several people to report their appeal on the same content. Hence, it is vital to develop a real and flexible immortal interface methodology for VSNs, obliging the special approval requirements coming from multiple associated users for managing the shared data collaboratively.

Design for profile and relationship distribution

We follow a logical solution to ease accommodating management of shared data in VSNs. We begin by inspecting how the lack of reciprocated immortal interface (RII) for data distribution in VSNs can weaken the security of user data. Some distinctive data distribution designs with respect to reciprocated authorization in VSNs are also identified. Based on these distribution patterns, an RII model is outlined to capture the core types of reciprocated authorization requirements that have not been put up so far by current immortal interface systems and models for VSNs (e.g., [7-9, 11, 16]). Our methods also comprise a reciprocated methodology specification scheme. In the intervening time, as conflicts are foreseeable in reciprocated approval enforcement, an election methodology is further providing to deal with authorization and privacy conflicts in our model.

Additional substantial feature of our explanation is the support of analysis on the RII model and systems. The perfect implementation of an immortal interface methodologies based on the foundation that the immortal interface methodology is valid. Besides, while the use of an RII methodology can greatly enhance the elasticity for adapting data distribution in VSNs, it may possibly decrease the certainty of system authorization costs due to the reason that authorization and privacy conflicts need to be resolved elegantly. Measuring the implications of immortal interface methodologies usually relies on the safety analysis system, which has been applied in several domains (operational systems, faith management [12], and role-based immortal interface [6, 10]). In our methodology, we further more introduce a method to represent and motive about our model in a logic program. Furthermore, we provide a model implementation of our authorization methodology in the context of Facebook. Our trial fallouts prove the possibility and usability of our method.

2. RII FOR VSNs: NECESSITIES AND PATTERNS

We proceed with a comprehensive requirement analysis of RII in VSNs. For now, we discuss some typical distribution patterns occurring in VSNs where numerous users may have dissimilar authorization requirements to a single resource. We exactly analyze three scenarios: profile distribution, relationship distribution, and content distribution—to understand the risks posted by the lack of collaborative control in VSNs. We influence Facebook as the running example in our discussion because it is currently the most popular and characteristic
social network provider. For the time being, we recap that our discussion could be easily extended to other existing social network platforms, such as Google+ [4].

**Profile dissemination:** A beautiful feature of some VSNs is to support social applications written by third-party developers to make additional functionalities built on the top of users’ profile for VSNs [1]. To offer eloquent and beautiful services, these social applications consume user profile properties, such as name, birthday, activities, hobbies, and so on. To make substances more intricate, social applications on present VSN platforms can also consume the profile aspects of a user’s friends. In this case, users can choice specific pieces of profile assets they are willing to share with the applications when their friends use the applications. At the same time, the users who are using the applications may also want to control what info of their friends is obtainable to the applications since it is likely for the applications to accomplish their private profile properties over their friends’ profile properties [13].

**Relationship dissemination:** Another feature of VSNs is that users can share their relationships with other members. Relationships are intrinsically bidirectional and carry possibly sensitive info that associated users may not want to disclose. Most VSNs provide RII machineries that users can control the display of their friend lists. A user, still, can only control one direction of a relationship. Let us reflect, for example, a scenario where a user Karthik specifies a methodology to hide his friend list from the public. But, Anand, one of Karthik’s friends, agrees a weaker methodology that permits his friend list visible to anyone. In this case, if VSNs can solely enforce one party’s methodology, the relationship between Karthik and Anand can still be learned through Anand’s friend list. A relationship distribution form where a user called owner, who has an association with another user called shareholder, shares the relationship with a contactor. In this situation, authorization requirements from both the owner and the shareholder should be considered. Otherwise, the shareholder’s privacy concern may be violated.

**Content dissemination:** VSNs offer built-in methodologies enabling users to connect and share contents with other members. VSN users can post statuses and notes, upload photos and videos in their own places, label others to their contents, and share the contents with their friends. On the other hand, users can also post contents in their friends’ spaces. The shared substances may be connected with multiple users. Consider an example where a photograph includes three users, Karthik, Anand, and Christina. If Karthik uploads it to his own space and labels both Anand and Christina in the photo, we call Karthik the owner of the photo, and Anand and Carol stakeholders of the photo. All of them may agree immortal interface methodology to control over that can see this photo.

3. RIIMODEL FOR VSNs

We honor a RII model for VSNs, as well as a methodology scheme and a procedure assessment methodology for the specification and enforcement of RII rules in VSNs.

3.1 RII Model

A VSN can be denoted by a relationship network, a set of user groups, and a collecting of user data. The relationship network of a VSN is a directed labeled graph, where each node signifies a user and each edge indicates a relationship between two users. The label associated with each edge indicates the type of the relationship. Verge direction denotes that the initial node of a verge launches the relationship and the terminal node of the verge accepts the relationship. The number and type of maintained relationships rely on the specific VSNs and its purposes. Also, VSNs include an important feature that allows users to be arranged in groups [15], [14] or called circles in Google+ [5], where each group has an exclusive name. This feature enables users of a VSN to easily find other users with whom they might share specific interests (e.g., same hobbies), demographic groups (e.g., studying at the same schools), political alignment, and so on. Users can join in groups without any endorsement from other group members. Also, VSNs provide each member a web space where users can store and manage their personal data with profile information, friend list and content.
3.2 RII Strategy Description

To allow a collective authorization management of data distribution in VSNs, it is essential for RII policies to be in place to regulate contact over shared data, on behalf of approval requirements from multiple associated users. Our methodology specification scheme is built upon the proposed RII model.

**Contactor portrayal:** Contactors are a set of users who are approved to contact the shared data. Contactors can be denoted with a set of user names, a set of relationship names (RNs) or a set of group names (GNs) in VSNs.

**Information description:** In VSNs, user data are composed of three types of information: user profile, user relationship, and user content. To enable effective privacy conflict determination for RII, we present sensitivity levels (SL) for data description, which are assigned by the controllers to the shared data items. A user’s judgment of the SL of the data is not binary (private/public), but multi-dimensional with varying degrees of sensitivity.

**Immortal interface methodology:** To summarize the above-mentioned methodology features, we present the definition of an RII methodology as follows:

Definition of RII methodology: A RII methodology is a 5-tuple $P = \langle controller, c \text{ type}, contactor, data, effect \rangle$.

The RII policies

1. “Karthik approves his friends to view his status known by status01 with a medium SL, where Karthik is the owner of the status.”

2. “Anand approves users who are his colleagues or in hiking group to view a photo, winter.jpg, that he is labeled in with a high SL, where Anand is a stakeholder of the photo.”
V. Pavani/ International Journal of Engineering & Science Research

3. “Christina disallows Danny and Sunny to watch a video, play.avi that she uploads to someone else’s spaces with a highest SL where Christina is the provider of the video.”

3.3 Reciprocated Methodology Evaluation

Two steps are done to evaluate a contact request over RII policies. The first step checks the contact request against the methodology stated by each controller and yields a decision for the controller. The contactor element in a methodology decides whether the methodology is applicable to a request. If the user who sends the request goes to the user set derived from the contactor of a methodology, the methodology is appropriate and the evaluation process yields a response with the decision (either permit or deny) indicated by the effected element in the methodology. Otherwise, the response yields deny decision if the methodology is not appropriate to the request. In the second step, decisions from all controllers responding to the contact request are amassed to make a final decision for the contact request. Since data controllers may generate different decisions (permit and deny) for an contact request, conflicts may happen. To make an unmistakable decision for each contact request, it is vital to adopt a methodical conflict resolve methodology to resolve those conflicts during reciprocated methodology evaluation.

A simple solution for deciding reciprocated privacy clashes is to only allow the common users of contactor sets defined by the several controllers to contact the data item. Regrettably, this strategy is too limiting in many cases and may not harvest desirable results for resolving reciprocated privacy conflicts. Reflect an example that four users, Anamica, Anand, Carol, and Danny, are the controllers of a photo, and each of them permits her/his friends to see the photo. Presume that Anamica, Anand, and Carol are close friends and have many common friends, but Danny has no common friends with them and also has a cute weak privacy concern on the photo. In this case, adopting the simple solution for conflict resolution may turn out that no one can contact this photo. Though, it is sensible to give the view permission to the common friends of Anamica, Anand, and Carol.

3.4 An Elective System for Decision Making of Reciprocated Control

Main stream election is a popular instrument for decision making [29]. Stimulated by such a decision-making methodology, we suggest an election scheme to achieve a real reciprocated conflict resolution for VSNs. A distinguished feature of the election methodology for conflict resolution is that the choice from each controller is able to have an effect on the final decision. Our election scheme covers two election methodologies: decision election and sensitivity election.

Assume that all controllers are similarly important; an aggregated decision value (DVag) (with a range of 0.00 to 1.00) from many controllers with the owner (DVow), the contributor (DVcb), and stakeholders (DVst) is computed with following equations:

\[
DV_{ag} = \left( DV_{ow} + DV_{cb} + \sum_{i \in SS} DV_{st}^{i} \right) \times \frac{1}{m},
\]

\[
DV_{ag} = \left[ \omega_{ow} \times DV_{ow} + \omega_{cb} \times DV_{cb} + \sum_{i=1}^{n} \left( \omega_{st}^{i} \times DV_{st}^{i} \right) \right] \times \frac{1}{\omega_{ow} + \omega_{cb} + \sum_{i=1}^{n} \omega_{st}^{i}}.
\]

**Sensitivity election:** Each controller assigns an SL to the public data item to reflect her/his privacy worry. A sensitivity score (Sc) (in the range from 0.00 to 1.00) for the data item can be considered based on following equation:

\[
Sc = \left( SL_{ow} + SL_{cb} + \sum_{i \in SS} SL_{st}^{i} \right) \times \frac{1}{m}.
\]
3.5 Verge Based Conflict Resolution

A basic idea of our method for verge based conflict resolution is that the Sc can be used as a verge for decision making. Instinctively, if the Sc is higher, the final decision has a high chance to deny contact, taking into account the privacy protection of high sensitive data.

3.7 Clash Determination for Diffusion Control

A user can share others’ data with her/his friends in VSNs. In this case, the user is a disseminator of the content, and the content will be posted in the disseminator’s space and visible to her/his friends or the public. Since a disseminator may adopt a weaker control over the disseminated content but the content may be much more sensitive from the perspective of original controllers of the content, the confidentiality worries from the original controllers of the content should be always fulfilled, averting inadvertent revelation of sensitive contents.

4. BALANCED PICTURE AND EXPLORATION OF RII

We adopt answer set programming (ASP), a recent form of declarative programming, to properly represent our prototypical, which fundamentally provide a formal foundation of our model in terms of ASP-based representation. Then, we prove how the correctness analysis and authorization analysis [7] of RII can be approved based on such a rational picture.

4.1 Representing RII in ASP

We present a conversion module that turns reciprocated authorization specification into an ASP program. This interprets a formal semantics of reciprocated authorization specification in terms of the answer set semantics.

4.2 Rational Definition of Reciprocated Controllers and Transitive Relationships

The basic components and relations in our RII model can be directly demarcated with matching predicates in ASP. We have defined UDct as a set of user-to-data relations with controller type ct 2 CT. Then, the logical definition of multiple controllers is as follows:

- The owner of a data item can be represented as:
  \[ OW(\text{controller}, \text{data}) \leftarrow UD_{OW}(\text{controller}, \text{data}) \land U(\text{controller}) \land D(\text{data}). \]

- The contributor of a data item can be represented as:
  \[ CB(\text{controller}, \text{data}) \leftarrow UD_{CB}(\text{controller}, \text{data}) \land U(\text{controller}) \land D(\text{data}). \]

- The stakeholder of a data item can be represented as:
  \[ ST(\text{controller}, \text{data}) \leftarrow UD_{ST}(\text{controller}, \text{data}) \land U(\text{controller}) \land D(\text{data}). \]

- The disseminator of a data item can be represented as:
  \[ DS(\text{controller}, \text{data}) \leftarrow UD_{DS}(\text{controller}, \text{data}) \land U(\text{controller}) \land D(\text{data}). \]

5. EXECUTION AND ASSESSMENT

5.1 Model Execution

We executed a proof-of-concept Facebook application for the cooperative management of shared data, called MController (http://apps.facebook.com/MController). Our model application enables multiple associated users
to specify their approval policies and privacy preferences to control a common data item. It is value noting that our current execution was limited to handle photo distribution in VSNs. Adversely, our approach can be generalized to deal with other types of data distribution, such as videos and comments, in VSNs as long as the stakeholder of shared data is recognized with real methods like labeling or searching.

MControl application structure

A core element of MController is the decision-making module, which procedures contact requests and returns responses (either permit or deny) for the requests. The figure showed system architecture of the decision-making module in MController. To evaluate a contact request, the policies of each controller of the targeted content are imposed first to generate a decision for the controller. Before, the decisions of all controllers are amassed to yield a final choice as the response of the request.
5.2 Participants and Process

MController is a useful proof-of-concept application of reciprocated privacy management. To measure the practicality and usability of our methodology, we conducted a survey study (n = 35) to explore the issues surrounding users’ desires for privacy and discover how we might recover those applied in MController. Exactly, we were interested in users’ viewpoints on the current Facebook privacy system and their desires for more control over photos they do not own. We employed participants through university mailing lists and through Facebook itself using Facebook’s built-in distribution API. Users were given the chance to share our application and play with their friends. While this is not a random sampling, employing using the natural distribution features of Facebook debatably gives a precise profile of the ecosystem.

5.3 User Study of M Controller

For assessment determinations, questions were divided into three areas: likeability, simplicity, and control. Likeability is a degree of a user’s satisfaction with a system (e.g., “I like the idea of being able to control photos in which I am labeled”). Simplicity is a measure how instinctive and useful the system is (e.g., “Setting my privacy settings for a photo in MController is Complicated (1) to Simple (5)” with a 5-point scale). Control is a measure of the user’s apparent control of their individual data (e.g., “If Facebook implemented controls like MController’s to control photo privacy; my photos would be better protected”). Questions were either True/False or restrained on a 5-point Likert scale, and all replies were scaled from 0 to 1 for numerical analysis. In the extent, a higher number indicates a positive insight or opinion of the system while a lower number designates a negative one. To examine the average user awareness of the system, we used a 95 percent confidence interval for the users’ answers. This assumes the population to be mostly normal.

5.4 Performance Assessment

To assess the performance of the policy assessment methodology in MController, we changed the number of the controllers of a shared photo from 1 to 20, and allocated each controller with the average number of friends, 130, which is appealed by Facebook statistics [3]. Also, we considered two cases for our evaluation. In the first case, each controller permits “friends” to contact the shared photo. In the second case, controllers specify “FOF” as the contactors instead of “friends.” In our experiments, we performed 1,000 autonomous tests and measured
the performance of each trial. Since the system performance depends on other processes running at the time of dimension, we had initial inconsistencies in our performance.

6. DISCUSSION

In our RII system, a group of users could conspire with one another so as to influence the final immortal interface decision. Study an attack scenario, where a set of malevolent users may want to make a shared photo available to a wider audience. Supposing they can contact the photo, and then they all label them or fake their individualities to the photo. In addition, they conspire with each other to assign a very low SL for the photo and stipulate policies to grant a wider audience to contact the photo. With a large number of conspiring users, the photo may be disclosed to those users who are not predictable to gain the contact. To stop such an attack scenario from happening, three conditions need to be satisfied: 1) there is no bogus identity in VSNs; 2) all labeled users are real users seemed in the photo; and 3) all controllers of the photo are authentic to specify their privacy partialities.

7. CONNECTED WORK

Immortal interface for VSNs is still a comparatively new research area. Numerous immortal interface methodologies for VSNs have been introduced (e.g., [7-9, 11, 16]). Early immortal interface solutions for VSNs introduced trust-based immortal interface enthused by the developments of trust and status computation in VSNs. The D-FOAF system [11] is mainly a friend of a friend ontology-based disseminated identity management system for VSNs, where relations are related with a trust level, which shows the level of friendship between the users partaking in a given relationship.

8. CONCLUSION

In this paper, we have projected a new solution for cooperative management of shared data in VSNs. An RII model was articulated, along with a reciprocated policy condition scheme and corresponding policy assessment methodology. In addition, we have presented a method for expressing and intellectual about our proposed model. A proof-of-concept application of our solution called MController has been discussed as well, trailed by the usability study and system evaluation of our technique.

REFERENCES


