A Role and Trust Access Control Model for Preserving Privacy and Image Anonymization in Social Networks

Nadav Voloch, Priel Nissim, Mor Elmakies, Ehud Gudes

▶ **To cite this version:**

Nadav Voloch, Priel Nissim, Mor Elmakies, Ehud Gudes. A Role and Trust Access Control Model for Preserving Privacy and Image Anonymization in Social Networks. 13th IFIP International Conference on Trust Management (IFIPTM), Jul 2019, Copenhagen, Denmark. pp.19-27, 10.1007/978-3-030-33716-2_2 . hal-03182609

HAL Id: hal-03182609

https://inria.hal.science/hal-03182609v1

Submitted on 26 Mar 2021

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Distributed under a Creative Commons Attribution 4.0 International License

A Role and Trust Access Control model for preserving privacy and image anonymization in Social Networks

Nadav Voloch[1], Priel Nissim[1], Mor Elmakies[1] and Ehud Gudes[1,2]

[1] Ben-Gurion University of the Negev
P.O.B. 653 Beer-Sheva 8410501 Israel
[2] Achva Academic College
Shikmim Mobile Post 79800 Israel
voloch@post.bgu.ac.il

Abstract. Over the last decade Online Social Networks (OSN) privacy has been thoroughly studied in many aspects. Some of these privacy related aspects are trust and credibility involving the OSN user-data conveyed by different relationships in the network. One of OSN major problems is that users expose their information in a manner thought to be relatively private, or even partially public, to unknown and possibly unwanted entities, such as adversaries, social bots, fake users, spammers or data-harvesters. Preventing this information leakage is the target of many OSN privacy models, such as Access Control, Relationship based models, Trust based models and many others. In this paper we suggest a new Role and Trust based Access Control model, denoted here as RTBAC, in which roles, that manifest different permissions, are assigned to the users connected to the Ego-node (the user sharing the information), and in addition, every user is evaluated trust wise by several criteria, such as total number of friends, age of user account, and friendship duration. An interesting extension of the model of image anonymization is also given, where a user that has a certain role with a proper permission can access a partial instance of the data, if a sufficient trust level is not achieved. These role and trust assessments provide more precise and viable information sharing decisions and enable better privacy control in the social network.

Keywords: Social Networks Privacy, Access control, Trust-based privacy models.

1 Introduction

Online Social Networks (OSN) privacy models have been a source of many researches over the past couple of years. Some of which focus on handling the OSN information sharing instances as an Access Control system, in which there is a selective restriction of access to the network's resources. The permission to access a resource is the main concern of the different models. The decision of giving a certain user authorization to such a resource is usually made by several criteria, based on many different factors.

Access Control models have different variations, some are more widely used than others. [1] presents a new model for privacy control based on sharing habits on which, we have preliminary based our research. This model controls the information flow by a graph algorithm that prevents potential data leakage.

This paper presents a new privacy model for access control in an OSN, in which the decisions of permission granting combines both pre-defined roles and trust-based factors derived from user-attributes, such as total number of friends, age of user account, and resemblance attributes between the two users. Similar attributes have appeared in a previous work ([2]), which deals with information-flow control, and creates a model for adversary detection. However, in this paper we present specific parametric values for these attributes, which are experimentally based. The model's extension of a partial data visibility is used here in an implementation of image anonymization, in which a certain role that inherently has a permission of seeing images, can see a partial (relatively blurry) image if he does not gain the necessary minimal Trust value for getting the full permission.

The rest of this paper is structured as follows: Section 2 discusses the background for our work, with explanations on the related papers it relies on, Section 3 describes and defines our model thoroughly with several examples of its operation and presents its preliminary evaluation. Section 4 is the model's extension of partial data visibility for image anonymization in the OSN. Section 5 discusses the model and concludes it.

2 Background and related work

Access Control models, and specifically ones describing OSN privacy, have been studied extensively over the past decade. A major problem, existing especially in OSN, is an information flow to unwanted entities, violating the privacy of individuals. The main Access Control model used in OSN is Role-Based Access Control (RBAC) that has many versions, as presented in [3], and limits access by creating user-role assignments. The user must have a role that has permission to access that resource.

The most prominent advantage of this method is that permissions are not assigned directly to users but to roles, making it much easier to manage the access control of a single user, since it only must be assigned the right role.

To this model an addition of the Trust factor is done in [4], and it is based on the network users' interaction history, which could be problematic in assessing relatively unknown new connections. In this paper we circumvent this problem by adding independent user attributes to this estimation. An example of using RBAC specifically in Facebook is done in [5], that describes the use of roles in it and the possible breaches that can occur due to the flexible privacy settings of the network. [6] present a model named IMPROVE-Identifying Minimal Profile Vectors for similarity-based access control. It elaborates on this specific subject, and gives a 30-item list of attributes, some direct and some derived, that define the user information in an OSN. We have based our Role and Trust Based Access Control (RTBAC) model on the above works, and it is presented in the following section. The novelty of our model is that the relationships and their strengths do not determine Access Control directly , but are used along with other characteristics to compute the trust of an OSN user in accordance with a specific Ego-user.

3 OSN Role and Trust Based Access Control (RTBAC)

3.1 The RTBAC model

The basic idea of the model is that besides the general roles given to different users, each user will be given a certain level of trust, and permissions to different data instances will be authorized only if the trust level passes a certain threshold. In this manner, the generalization disadvantage of RBAC can be solved, and better data distribution can be achieved. We should first emphasize the way, relative to a specific Ego-user, RBAC is generally used in an OSN. A user may belong to multiple hierarchic roles, but all of them are on a single path (as seen in [7]). Therefore, when a user, and an Access chosen for it, is the lowest in the hierarchy it has the maximal set of permissions per role. We denote this role as *R (U, Ego)*, but we will use just *R* as a short notation. The main contribution of RTBAC is the way Trust is computed.

Trust is computed by assigning values of credibility and connection strength to the different users, based on the criteria presented below. A minimum trust value threshold is the core condition of accessing a specific permission. The purpose of combining trust is to provide an additional stage of screening besides the RBAC roles. Another advantage of the model is that the combination of trust elements allows dynamic assignments of permissions to users over time, meaning their trust level can be dropped, and vice versa. The formal definition of the RTBAC model instance is as follows:

An RTBAC instance is a tuple <*u_id, R, P(R), UTV, MTV, P(U)*> where:

- *u_id* – the identification of a user connected to the Ego-node.
- *R* – the assigned user role of *u_id*, same as in RBAC
- *P* –An access permission to an OSN data instance
- *B (P, R)* - the preliminary access Permission *P* of the assigned role *R*
- *UTV*-, the User Trust Value for *u_id*, that will be explained in the following part, values range between 0 and 1
- *MTV (P, R)* - the Minimal Trust Value of role *R* for permission *P*, that will be explained in the following part, values range between 0 and 1
- *B (U, P)* - the final access decision for *u_id U* for permission *P*

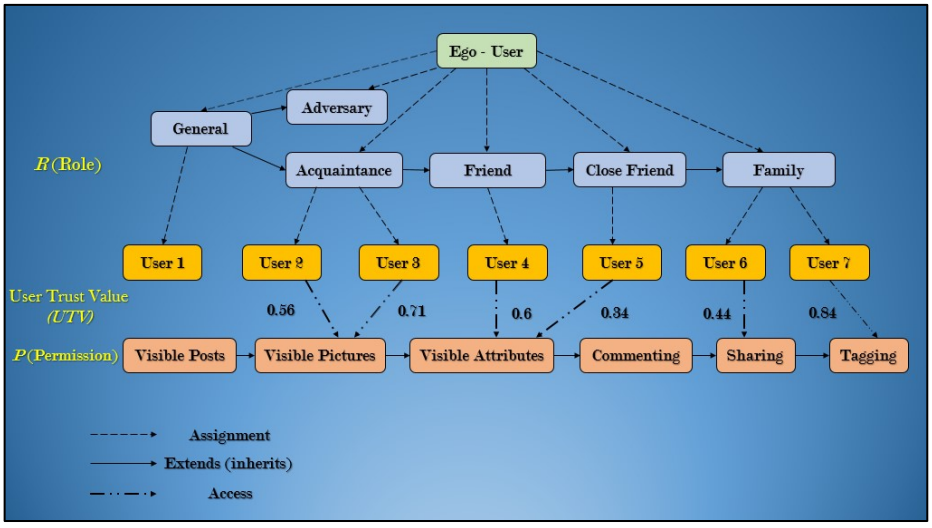

Fig. 1. RTBAC model example of 7 users. Users 6 and 7 have a "Family" role, but only User 7 achieves a trust value > 0.745 and gets the "Tagging" permission.

In Fig.1 we can see an example for the model's structure – The Ego-user is the user sharing the information. There are 7 other users in the system in this example, that obtain different roles. In this example, we give a minimal trust value (*MTV*) of 0.745 for a family member role to access the permission of "Tagging". This value can be altered per role and per permission in other cases. An Example of the trust decision making can be clearly seen in User 6. Users 6 and 7 have a "Family" role, but only User 7 achieves a trust value > 0.745 and gets the "Tagging" permission that User 6 does not obtain.

3.2 Criteria choice for Trust estimation

The choice of the attributes, for determining the level of trust for the model, is based on the criteria mentioned in the above sections, and the two main categories of criteria for our model are:

- **Connection strength (*c*):** the connection strength of users is determined by characteristics that indicate their level of closeness such as Friendship Duration (FD), Mutual Friends (MF), Outflow/Inflow Ratio (OIR) and Resemblance Attributes (RA). The notation given to these factors is *c*. For example, c_{MF} is the value for the Mutual Friends attribute.

- **User credibility (*u*):** the user credibly criterion assesses the user attributes that convey his OSN reputation and trustworthiness. These are Total number of Friends (TF) and Age of User Account (AUA) calculated from the time the user joined the OSN, and Followers/Followees Ratio (FFR). The notation given to these factors is *u*. For example, u_{AUA} is the value for the Age of User Account attribute.

3.3 Calculating Trust parameters' values

Setting the values for the Trust variables is done in this model in a scale of 0 to 1, since the decision of sharing information with a certain user is defined as a probability variable, 0 being no sharing willingness at all, 1 being definite sharing willingness.

All the parameters' values presented in this section are based on an experimental evaluation we have performed and is discussed in more detail in section 3.5 of this paper.

Table 1. Threshold values for trust attributes

TF	*AUA* (months)	*FD* (months)	*MF*
245	24	18	37

The threshold values for TF, AUA, FD and MF are presented in Table 1, FFR is defined as a ratio by default, as well as OIR, while if one of these values is larger than 1, it is calculated as 1 for the model.

For the c_{RA} value we take into consideration 10 of the users' attributes, based on the researches presented above (e.g. IMPROVE [6]), that resemble the Ego-user's attributes that are gender, age (range), current educational institute, past educational institute, current workplace, past workplace, current town, home-town, current country, home-country.

Let us denote the following factors:

- TA_{ego} is the total number of non-null attributes (from the 10 attributes mentioned above) of the Ego-user. The values of these attributes must be defined by non-null values.
- $TRA_{ego,\ other}$ *is* the total number of non-null resembling attributes (from the 10 attributes mentioned above) of the Ego-user and the other user. The values of these attributes must be defined by non-null values.

Now we can define c_{RA}:

$$c_{RA} = \frac{TRAego,other}{TAego} \tag{1}$$

This value cannot be larger than 1, since the maximal number of common attributes could be the total number of Ego-user's attributes at most. Now we can assess the access permission decisions by defining the total values of user credibility and connection strength in a manner of averaging the different factors noted above.

$$u = \langle WiUi \rangle = \frac{\sum_{i=1}^{|u|} WiUi}{\langle W \rangle |u|} = \frac{WuTF + WuAUA + WuFFR}{5.24 \cdot 3} = \frac{5.37uTF + 5.2uAUA + 5.16uFFR}{15.72} \tag{2}$$

$$c = \langle WiCi \rangle = \frac{\sum_{i=1}^{|c|} WiCi}{\langle W \rangle |c|} = \frac{WcMF + WcFD + WcOIR + WcRA}{5.52 \cdot 4} = \frac{5.93cMF + 5.1cFD + 5.7cOIR + 5.34cRA}{22.8} \tag{3}$$

These weights (W_i) were the survey results for the significance (weight) of every attribute-factor (U_i or C_i) in u and c. They could theoretically be altered by other user-preferences or future results.

We can now conclude the definition of the model's User Trust Value (*UTV*), taking into consideration that there are 7 attributes: 4 connection attributes and 3 user attributes (marked as $|c|$ and $|u|$):

$$UTV = \frac{c\cdot|c|+u\cdot|u|}{|c+u|} = \frac{4\cdot c+3\cdot u}{7} \quad (4)$$

The Minimal Trust Value (*MTV*) set in this model is based on the Trust-based dynamic RBAC model presented above and is altered per role and per permission by the user-preferences if such exist, or by an OSN administration policy, if such exists for these specific cases. It is important to state here that the users were not asked directly about the parameter values, but those were derived from the experimental evaluation that will be described in the following part of this paper. A certain user can set its own trust threshold dependent on his privacy preferences.

The values presented here are validated by the experimental evaluation but are subject to flexible changes by necessity.

In Table 2 we can see an example, portrayed in Fig.1, where there is a difference between two users that have the same role, but not the same *UTV*, thus not getting the same permission. The *MTV* set for this specific role and permission (Family - Tagging) is 0.745, and User 6 achieves a *UTV* value of 0.44 and does not get the permission, whilst User 7 achieves a *UTV* of 0.84, thus gets the permission.

In the following parts we will see the model's algorithm, and the experimental evaluation done for determining its different parameters.

Table 2. Difference in *UTV* between same-role users

User	*WuTF*	*WuAUA*	*WuFFR*	*WcRA*	*WcFD*	*WcOIR*	*WcMF*	***u***	***c***	***UTV***	***MTV***
6	0.44	0.33	0.89	0.4	0.67	0.13	0.22	**0.55**	**0.36**	**0.44**	**0.745**
7	0.78	0.59	0.91	0.8	0.86	0.96	1	**0.76**	**0.91**	**0.84**	**0.745**

3.4 The model's algorithm

The decision algorithm is depicted in algorithm 1:

Algorithm 1. PermissionDecisionOfRTSBAC (User *U*, Role *R*, Permission *P*)

Input: Minimal Trust value: *MTV(P(R))*
Output: The decision of granting or denying access.

```
if P(R(U)) = 1                    // permission belongs to role
        if UTV (U) ≥ MTV(P(R)) // UTV: pre-calculated, set as attribute
                Grant Access
        else
                Deny Access
else
        Deny Access
```

3.5 Experimental assessment and real OSN data estimation of Trust

As mentioned above, the experimental evaluation of the model's trust parameters consisted of two parts:

A. A validation of the parameters by a survey of 282 OSN users that were asked for the importance of various attributes in their decisions to grant various permissions to their private data. The survey included the quantifiable attributes of user credibility and connection strength. For all these attributes, the request was for the needed threshold value of Trust of a certain user. For example, an average of 245 total friends (TF) and above was considered as a trustworthy user, to which we can share information. The results of the most important ones are presented in Table 1. Two more aspects were examined in the survey: the importance (weight) of every one of the Resembling Attributes (RA) on a scale of 1 to 10, and the importance of every one of the model's Trust attributes.

B. In the second experimental evaluation we attempt to validate the trust computation in a real OSN dataset that included 162 user nodes and their attributes, all were friends of a single ego user. This dataset of user nodes was checked for the model parameters' Trust quantifiable attribute values mentioned in the previous parts. The nodes' *UTV* was calculated by the formulas presented above, and the average *UTV* achieved by the 162 users was 0.745. When we set the *MTV* threshold to 0.5, we get that only 3 users were denied access. The ego user confirmed that these three users should not have been in his friends' role.

4 The model's extension – partial access for data anonymization

Our model's algorithm enables the complete access of information to highly trusted users or blocks it completely to undesirable ones. In this section we suggest an extension of the model such that the information access is generalized or anonymized based on the user's trust level and distance from the Ego-user. We demonstrate this idea using image anonymization, but it can also be applied to text, profile attributes and other information instances, similarly. The main idea of the model's extension of partial access is that a certain instance of data is not fully seen or unseen but can be partially scaled in its appearance. This option gives a wider information access, with the benefit of secure data anonymity. In image anonymization this feature helps reducing data leakage from facial recognition algorithms, vastly used in OSN and other Web applications. In Fig.2 we can see the manifestation of such a partial access, where the Ego-user's profile picture is anonymized in the access granting seen in Fig.1. For the given scenario we assume the value of 0.7 as the *MTV*, and the permission handled is the "visible pictures" that User 2 and User 3 obtain. User 1 does not see the image at all (left part of Fig.2) since it does not have a fitting Role (he is "General" and the relevant Role is "acquaintance"). User 2 has a fitting Role but has a *UTV* of 0.56, hence he gets a blurrier image (middle part of Fig.2) then User 3 obtains. User 3 has the fitting Role and the needed Trust value (*UTV*=0.71), thus he gets the full image (right part of Fig.2). It is important to state here that this extension of the model is relevant only to these permissions that logically enable partial access. Permissions of "sharing" or "tagging" are binary by nature, hence cannot allow a partial access model.

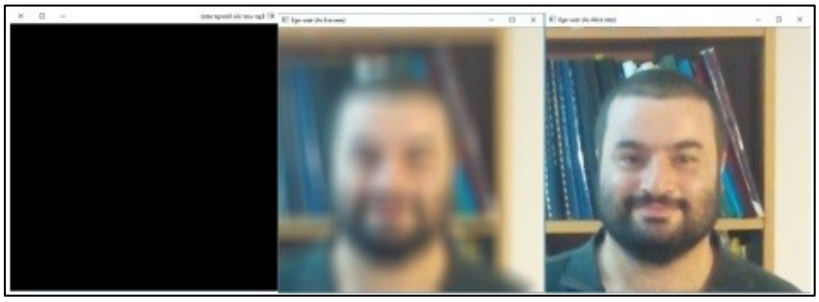

Fig. 2. Visibility of profile picture as seen by the users of Fig.1, with a threshold *MTV* of 0.7 Left: User 1, Middle: User 2, Right: User 3.

5 Discussion and conclusions

In this paper we have presented an Access-Control model for privacy in OSN. The novelty of our RTBAC model is its combination of User-Trust attributes, based on real OSN characteristics, in an RBAC, that usually grants permissions solely to roles, and by that improving the privacy features of the network. In this manner, it is better than current Role-based models, in which members of the same role (e.g. family or close friend) have the same set of permissions, disregarding their relationship with the Ego-user and other users, and not taking into consideration their dynamic behavior. Our model makes this permission's decision dynamic in time, since these attributes can change during time: The user gains or loses friends, its age of user account grows over time, etc. In addition, the model's extension of data anonymization is an important feature, that helps reducing the data leakage for OSN users, giving the OSN a better privacy infrastructure.

Acknowledgments

The authors would like to thank Eyal Pickholz for his assistance in the part of the model's extension of image anonymization and its software implementation. We also thank the BGU cyber center for supporting this project.

References

1. Levy, S., Gudes, E., & Gal-Oz, N. "Sharing-habits based privacy control in social networks". In IFIP Annual Conference on Data and Applications Security and Privacy 2016, Springer, Cham. pp. 217-232.
2. Gudes E., Voloch N. "An Information-Flow Control model for Online Social Networks based on user-attribute credibility and connection-strength factors", CSCML 2018, 2nd International Symposium on Cyber Security Cryptography and Machine Learning.
3. Sandhu, R. S., Coyne, E. J., Feinstein, H. L., & Youman, C. E. "Role-based access control models". Computer, 29(2), 38-47. 1996.
4. Lavi, T. and Gudes, E." Trust-based Dynamic RBAC." In Proceedings of the 2nd International Conference on Information Systems Security and Privacy (ICISSP) 2016, pp. 317-324.
5. Patil, Vishwas T., and R. K. Shyamasundar. "Undoing of privacy policies on Facebook." IFIP Annual Conference on Data and Applications Security and Privacy. Springer, Cham, 2017.
6. Misra, G., Such, J. M., & Balogun, H. "IMPROVE-Identifying Minimal PROfile VEctors for similarity-based access control". In Trustcom/BigDataSE/I SPA, 2016 IEEE (pp. 868-875). IEEE.
7. Facebook help: roles, https://www.facebook.com/help/323502271070625/