2016 International Conference on Computational Modeling, Simulation and Applied Mathematics (CMSAM 2016)
ISBN: 978-1-60595-385-4

A Multi-dimensional Vector Based Access Control Model for Social Networks

Ying-jun ZHANG[1], Kai CHEN[2] , Yi YANG[3], Yu-ling LIU[1], Xue-fei JIA[4] and Yi-feng LIAN[1]

[1]Trusted Computing and Information Assurance Laboratory, Institute of Software, Chinese Academy of Sciences, China

[2]Institute of Information Engineering, Chinese Academy of Sciences, China

[3]Beihang University, China

[4]Information Security Certification Center, Beijing, 100020, China

Keywords: Access control, Social networks, Multi-dimensional vector.

Abstract. The rapid updates of messages and users' information in social networks make it very difficult to efficiently identify unauthorized users and further hard to protect messages. Existing mechanisms for security protection usually have high overhead. In this paper, a multi-dimensional vector based access control model is used to solve these problems. Firstly, multi-dimensional vector for each user is constructed. Then based on a novel access control model proposed in this paper, the vector in social networks is utilized to judge whether an access request is permitted. At last, we give some examples to verify our methods.

Introduction

Nowadays, more and more people use social networks for contact, relax and so on. For example, a lot of users like to use twitter to post their messages or photos. Then users, including both their friends and strangers, can forward the messages to more people. Personal information also exists in the social networks, such as users' interests, locations, etc. Although it is very convenient to post messages in social network, such users' private information could be leaked. If the information is utilized by malicious users, it can be very harmful.

Access control is an effective method to solve these problems and protect users' information. For example, we can define who can access users' private information or forward messages. Most of the access control methods in social networks are based on relationship [6] or rules [5]. Although they can work well to limit those who can access the messages, there are still some problems as follows:

- Lack of updating users' information in real time. As we know, information in social networks, such as the number of followers/followings and the number of posted massages/photos, can be updated in a highly frequent way. Using this information, we can leverage these kinds of real-time information for better access control. For example, we can detect Sybil users and other related potential attackers [14,12] for blocking their accesses. But the existing access control methods do not pay attention to the useful information.
- Lack of updating policies whose importance can be changed with time. In social networks, the time information is very important. People pay more attention to the mostly updated information. Some messages will lose the importance as time goes by, in which the strictness of access control policies can be lower. So we can define the policies according to time period.
- Low efficiency. The process of constructing of relationship graph and judging the relationship is time-consuming. Considering users' friends are updated frequently, if an operation (e.g., forward) is executed several times, the process of judging privileges from the graphs will be very complex. Another issue is that some information is restricted, which cannot be fully accessed. For example, we can only view 100 followers of a user instead of all the followers in

Sina Weibo. Under this limitation, the access control is not efficient and only has partial effect, which will impact the use of social networks.

To solve these problems, we construct a new access control model based on multi-dimensional vector. In this model, we pay more attention to public information, which can be gotten easily for access control, and provide an efficient method to protect users' information.

The Construction of Multi-dimensional Vector

The multi-dimensional vector Φ is used to express users' information, in which we focus on public information that is accessible to everyone (e.g., the number of followers, followings, photos and messages).

$\Phi=\{\varphi\}$, $\varphi=<\alpha_1, \alpha_2,\dots, \alpha_n>$,$\alpha_i$ is one kind of information about the user. In this paper, $\alpha_i \in N$, which is a number and can be directly compared. For example, we can defineα_1 as the number of followers, α_2 as the number of followings, α_3 as the number of the posted messages, α_4 as the number of the posted photos, α_5 as the number of the forwarded messages, and so on. In the next section, we will use these vectors as an example to present our model.

In order to put more weight on some specific α_i (which may be more cared by a user), we can define the weight factors (Ψ) for elements in the vector. The weight factors can be gotten using machine learning or defined by users Then we can compare the value of the vectors.

$\Psi=\{\psi\}$, $\psi=<\beta_1,\beta_2,\dots,\beta_n>$, $\beta_i \in R$ is a weight factor for each vector element α_i. How to chooseψ is considered and determined by the user. For example, a famous person may have a lot of followers. In order to allow the normal user to access his message, the weight factor of followers may be small. Then we can reduce the gap between normal users and famous users.

The value of the vector distance can be defined as$\Theta=\{\theta\}$, which is the product of the vectors and their weight factors. And we use$Y=\{\gamma\}$ to compare the two vectors. The definition of γ is based on Jaccard distance [13]. $\gamma_i=(\alpha_i-\alpha_i')/(\alpha_i+\alpha_i')$. Then the value of vector is defined as $\Theta=\gamma \times\Psi$, $\theta(\varphi1,\varphi2)=|\gamma_1\beta_1+\gamma_2\beta_2+, \dots, +\gamma_n\beta_n|$.

Example 1:

$\varphi A=<125,97,1326,53,190>$
$\varphi B= <5,256,3210,2,2193>$
$\varphi C= <15982,329,8540,2321,942>$
$E(\Psi, \varphi A) \rightarrow\psi1=<0.4, 0.1, 0.1, 0.3, 0.1>$
$E(\Psi, \varphi B) \rightarrow\psi2=<0.1, 0.1, 0.4, 0.1, 0.3>$
$E(\Psi, \varphi C) \rightarrow\psi3=<0.1, 0.2, 0.25, 0.35, 0.1>$
$\gamma(A,B)=<0.92, 0.21, -0.42, 0.93, -0.84>= -\gamma(B,A)$
$\gamma(A,C)=<-0.98, -0.54, -0.73, -0.96, -0.66>= -\gamma(C,A)$
$\gamma(B,C)=<-1.0, -0.12, -0.45, -1.0, 0.4>= -\gamma(C,B)$
$\theta(C,A)=0.98*0.4+0.54*0.1+0.73*0.1+0.96*0.3+0.66*0.1=0.5097$
$\theta(B,A)=(-0.92)*0.4+(-0.21)*0.1+0.42*0.1+(-0.93)*0.3+0.84*0.1=-0.2991$
$\theta(B,C)=(-1.0)*0.1+(-0.12)*0.2+(-0.45)*0.25+(-1.0)*0.35+0.4*0.1=-0.4335$

In Example 1, Alice is a normal user, and her vector can be expressed asφA. Bob is a malicious user, who always sends spam. His vector can be expressed asφB. As in the example, we can see that the malicious user has few followers. But he pays attention to lots of people so that he can forward messages easily. We also note that he posts few of his own photos, and always forwards many spam messages, like the advertisements. Cathy is a famous writer, who has a lot of fans, and his vector can be expressed as φC. So the famous user always has a lot of followers, and posts many messages and photos by himself. Then we define $\Psi=\{\psi1,\psi2,\psi3\}$ in this example, in order to distinguish different kinds of users. After that, we calculate the vector distance among every two users.

Access Control Model in Social Networks

We define the model as M= (φs, φo, O, θ, T). Φs is the vector of subject, Φo is the vector of the object, O is the operations of the subject, θis the value of the vectors' distance, T is the time period. In addition, '-' in the model means NULL.

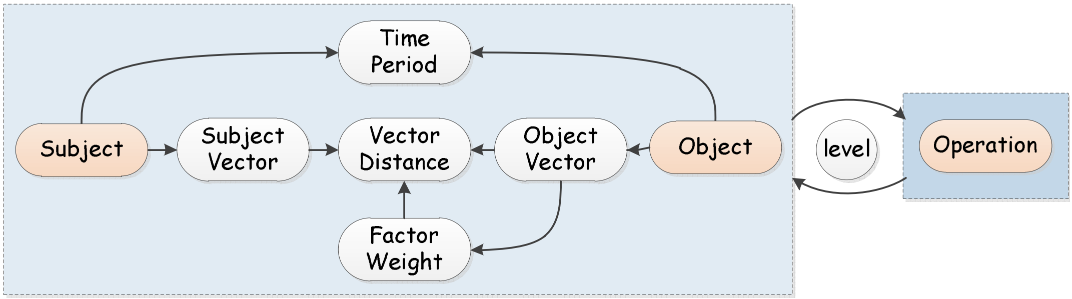

Figure 1. The Multi-dimensional Vector Based Access Control Model in Social Networks.

The operations O in social networks include traditional operations and special operations. Traditional operations include view, modify, delete and so on. Special operations include forward, comment, favor and so on. So we have to define O=<type, depth> (e.g., <forward, 2>). "Type" is the operation and "depth" is the number of times which means the same operation on the same message.

The time period T can be defined as the interval between current time and the time when the message is posted. Considering the practical use, we define the time in the grain of a day. T=D(now)-D(message). The function D is used to map the exact time to the day. Then we can define different access control policies according to different time periods, which conform to the timeliness in social networks.

Next we will introduce the details of our access control model in figure 1. First, we construct the subject vector and object vector from subject and object. We use V(Subject)→φs and V(Object) →φo to define the process. Second, we choose a suitable factor weight from the setΨ, which is based on the vector of object. We express it as E(Ψ, φo) →ψ.Thirdly, we will calculate the vector distance from subject to object. In this process, we first compute theY, and then compare two vectors to get the vector distance. Next, we get the time interval between the subject and object. At last, we compare the privileges several times according to the operation' level. The level means how many times the operation is implemented by different users. Now, we give some examples.

Example 2:

M1=(φA, φA, <post,->, -, -)
M2=(φs, φA, <forward,1>, 0.5,-)
M3=(φs, φA, <forward, 2>, 0.2, 30 days)
M4=(φs, φA, <comment,1>, 0.3,-)
M5=(φs, φA, <favor, 2>, 0.1, 7 days)
M6=(φs, φC, <favor, 1>, 0.4, 7 days)
M7=(φs, φC, <forward, 1>, 0.2, 90 days)

In Example 2, firstly, we get the factor weight according to object vector. In M1, Alice wants to post a message by herself, which does not have any restriction. In M2, if a user wants to forward Alice's message directly, the value of the user's vector should be equal or greater than 0.5. In M3, if a user wants to forward Alice's message from a forwarded message of another user, his vector value should be equal or larger than 0.2 and the time period between the user and Alice should be more than 30 days. In M4, if a user wants to comment Alice's message, his vector value should be larger than 0.3. In M5, if a user wants to favor Alice's message from the indirect message forwarded by the other one, his vector value should be equal or larger than 0.1 and the time period should be more than 7 days. In M6, if a user wants to favor Cathy's message, his vector value should be greater than 0.4 and the time period should be more than 7 days. In M7, if a user wants to forward Cathy's message, his vector value should be larger than 0.2 and T should be more than 90 days.

Access Request

When a user wants to access another user's messages, the access request R has to be judged according to policies defined as above. R=(Ur, Uo, O, t), Ur is the user starting request; Uo is the object which Ur wants to access; O is the operation type and level; t is the current time.

The process of judging is similar to Figure 1. In order to describe it more clearly, we use some examples in Figure 2.

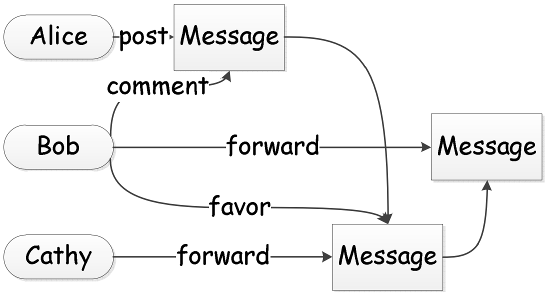

Figure 2. The example of access request in social networks.

Example 3:

R1=(Alice, Alice, <post,->, 2015/3/3)
R2=(Cathy, Alice, <forward,1>, 2015/3/3)
R3=(Bob, Alice, <comment,1>, 2015/4/3)
R4=(Bob, Cathy, <favor,2>, 2015/4/3)
R5=(Bob, Cathy, <forward,2>, 2015/4/3)
R6=(Bob, Cathy, <forward,2>, 2015/11/3)

In Example 3, Alice wants to post a message on 2015/3/3, which is permitted according to M1. In R2, Cathy wants to forward Alice on the same day. Then we compute the vector distance, which is larger than 0.5. So the request is allowed. In R3, Bob wants to comment on Alice's message. According to M3,$\theta(B,A)=0.2991$, which is smaller than 0.3. So the request is denied. In R4, Bob wants to favor Cathy's message which is forwarded from Alice. So the operation's level is 2. According to M5 and M6, $\theta(B,A)=0.2991>0.1$,$\theta(B,C)=0.4335>0.4$; and the time is suitable. So the access is allowed. In R5, according to M3 and M7, Bob wants to forward Cathy's message, which is forwarded from Alice.$\theta(B,A)=0.2991>0.2$, $\theta(B,C)=0.4335>0.2$, but the time period is too short. So R5 is denied, and R6 is permitted.

Related Work

Traditional access control models such as discretionary access control [1], mandatory access control [2], role based access control [3] and attribute based access control [4]) do not satisfy the relationship-based architecture in social networks, which makes them incapable or inefficient to support millions of users in social networks.

Some new access models such as rule-based access control model [5] and relationship-based access control model [6] are proposed to handle the problem of large number of users. D-FOAF [7] is an access control model based on trust-level. This level is assigned a value for comparison. B. Ali et. al [8] proposed a trust-worth access control model by giving subjects and objects different levels. B. Carminati et. al [5] proposed a rule-based access control model based on the depth and trust-level of relationship. Based on this, the authors also proposed privacy enhancing model [10], [11]. Fong et.al [6] proposed ReBAC model based on relationship. In [9], using the public information as attributes will be very slow in the control process. However, these models cannot provide flexible definition and high-efficient judgment. In this paper, the multi-dimensional vector based access control model is a new access control methods in social networks, which can effectively solve these problems.

Summary

In order to provide an efficient access control model in social networks, we propose a multi-dimensional vector based access control model. First, we construct the multi-dimensional vector and define the distance between two vectors. Then we give the new access control model. After that, we introduce how to judge the access request. At last, we give some examples to illustrate it.

Acknowledgement

This research was financially supported by the National Natural Science Foundation of China (NSFC) (Grant No.U1536106, 61303248, 61402456), National High Technology Research and Development Program of China (863 Program) (No. 2015AA016006), Youth Innovation Promotion Association CAS, and strategic priority research program of CAS (XDA06010701). Key Lab of Information Network Security, Ministry of Public Security (C15604).

References

[1] Trusted Computer System Evaluation Criteria, United States Department of Defense. December 1985. DoD Standard 5200.28-STD.

[2] Bell D. Elliott, La Padula, Leonard J, ”Secure computer systems: unified exposition and multics interpretation”, DTIC Document, 1976.

[3] Sandhu R S, Coyne E J, Feinstein H L, et al, ”Role-based access control models”, Computer, 29(2), pp. 38-47, 1995.

[4] Zhang X, Li Y, Nalla D, ”An Attribute-based access matrix model”, Proceedings of the 2005 ACM Symposium on Applied Computing, pp.359-363, 2005.

[5] B Carminati, E Ferrari, A Perego, ”Rule-Based Access Control for Social Networks”, On the Move to Meaningful Internet Systems 2006: OTM 2006 Workshops, LNCS 4278, pp. 1734-1744, 2006.

[6] P W L Fong, ”Relationship-Based Access Control: Protection Model and Policy Language”, CODASPY’11, pp. 191-201, 2011.

[7] SR. Kruk, S. Grzonkowski, A. Gzella, et al. D-FOAF: Distributed Identity Management with Access Rights Delegation[C]. ASWC 2006, LNCS 4185, 2006. 140-154.

[8] B. Ali, W. Villegas, M. Maheswaran. A trust based approach for protecting user data in social networks[C]. Proceedings of the 2007 conference of the center for advanced studies on Collaborative research, 2007. 1-4.

[9] Jun Panga,Yang Zhanga, ”A new access control scheme for Facebookstyle social networks”, Computers and Security, 2015.

[10] B. Carminati, E. Ferrari. Privacy-aware collaborative access control in web-based social networks Proceeedings of the 22nd annual IFIP WG 11.3 working conference on Data and Applicat ions Security, LNCS 5094, 2008. 81-96.

[11] B. Carminati, E. Ferrari, A. Perego. Enforcing access conntrol in webbased social networks, ACM Transactions on Information and System Security, 2009, 13(1):1-38.

[12] Kang Kai, Zhang Yingjun, Lian Yifeng, Liu Yuling, “ A Compound Approach for Sybil Users Detection in Social Networks“, Computer science (in Chinese), Vol. 43, No. 1, pp. 172-177, 2016.

[13] Jaccard, Paul (1901), "Étude comparative de la distribution florale dans une portion des Alpes et des Jura", Bulletin de la Société Vaudoise des Sciences Naturelles 37: 547–579.

[14] Gang Wang, Tristan Konolige, Christo Wilson, Xiao Wang, Haitao Zheng and Ben Y. Zhao,“You are How You Click: Clickstream Analysis for Sybil Detection”, Proceedings of the 22nd USENIX Security Symposium, 2013.