Advances in Engineering Research (AER), volume 148
3rd Workshop on Advanced Research and Technology in Industry Applications (WARTIA 2017)

Research on Privacy Protection of Mobile Social Network and Dynamic Trust Model

Yuan Zhou, Yaofeng Miao, Jiangyan Sun

School of Engineering, Xi'an International University, Xi'an, 710077, China

Keywords: Privacy protection, Mobile social network, Dynamic trust model

Abstract. With the development of mobile internet and the expansion of human interaction and communication requirements, mobile social networks are beginning to influence people's lives. Social networks have been widely used, but the problem of trust has always been the bottleneck that restricts the further development of social networks. In this paper, a dynamic trust model in mobile social networks is constructed. The paper gives a privacy protection scheme of mobile social network based on dynamic trust model, from the perspective of the basic idea of scheme, the key technologies of scheme and the process description of scheme to provide some references for the relevant researchers.

Introduction

With the rapid development of mobile internet, more and more users to participate in the internet, which leads to personal privacy information more and more exposed to the internet security. The problem of user privacy protection becomes more and more serious. Therefore, the protection of information, especially the privacy information protection under mobile internet, has become the focus of research in recent years. Access control is one of the important measures to protect information resources. It plays an important role in the protection of user privacy. Traditional access control mainly includes discretionary access control and mandatory access control. Among them, autonomous access control is an access control service, which controls access rights through the access of the user body to the system resources. Mandatory access control is the system force subject or user obeys a certain access control policy, which is the object created by the system to the user, and the user must obey it according to the rules. The main function of social networking services is to build an online communication community for users with the same entertainment and interests. These services are generally based on the internet or mobile internet, providing people with a variety of communication and contact convenient interactive channel. Interpersonal relationships in the real world, such as friends, relatives, classmates and colleagues, are generally strong and not easy to change greatly. But in most social networking services, anyone can join in and leave at will, so social networking services are highly dynamic. Social networking services offer great convenience to users, so more and more users are joining them, which is even more powerful than the size of social networks. Large amount of users and complex types of user groups make traditional sociological analysis methods not applicable here. Computer technology should be used to build models for analysis.

Dynamic Trust Model in Mobile Social Network

Concept of Dynamic Trust Model. With the rise of new Internet technologies, social networking applications based on Web2.0 technology are gaining popularity and growing rapidly because of their usability and entertainment. Social network is a virtual platform based on real interpersonal relationship and expanded the social network in real life. It has a high degree of dynamic, many users, rich content, anonymous features, good friend circle characteristics, you can see that the study of

social network security is indeed necessary. The major threats in social networks include privacy leaks, phishing, and so far, security measures for social networks are not perfect. With the rapid development of the Internet, Internet based applications have become more comprehensive and fast. The social network has big development in their number and scale, but also to other industries continue to penetrate the field of electronic commerce has now, and social networks are inseparable, the main reason is the social network contains many real relationships, make full use of the trust relationship can help users to effectively filter the redundant information, increase the success of the sale the rate of. The virtual nature and online payment of network transaction make it easy to have security problems, that is, network transaction risk. To make the transaction proceed smoothly, it is the most important problem to establish the trust between the two sides of the transaction. The higher the degree of trust, on behalf of the user to the entity more trust, if in the electricity supplier domain to buy goods, when many businesses have the same commodity, users tend to choose high trust merchants as interactive object. We set the range of confidence to [0,1], and if there is no experience in the past, there is no corresponding degree of trust. After many transactions, the normal user's trust degree is close to 1, and the malicious user's trust degree drops to less than 0.5.

Factors of Trust Degree. Since users often have fewer objects to interact with the system and no interaction experience with many interacting objects, the trust is in the default state, and it is inaccurate to make decisions only by degrees of trust. You can get advice from friends by consulting your friends, choosing reliable recommendations, and then combining them to make decisions, which can reduce the risk of user transactions. The range of credibility is also [0,1], and the trust level and the degree of trust are the same. The meaning of trust and credibility is different. Trust refers to a user's ability to judge the ability of other entities. The index of the user's choice of the transaction object is often the degree of trust. Reliability refers to the degree of trust of a user's recommendation information from a friend, and the index of the user's choice of recommendation information is often credibility. Refers to the action and purpose of the user in the interaction. In online trading, the interactive context includes transactions, reviews, recommendations, and commodity values. Among them, the size of commodity value has an important connection with the purpose of user interaction. When the value of the goods is low, it is more likely for users to brush credit with the merchants, so it is unreasonable to judge the value of trust only by the number of successful transactions. Therefore, considering the effect of interactive behavior of trust in the trust degree calculation, different weights for different value of the commodity trading, commodity value is higher, the greater the weight distribution of goods; the lower the value, the smaller the weight distribution.

Calculation of Trust Degree. The direct trust between the user A (root user) and the user N (target user) is related to the past interaction times, the evaluation information and the time and interactive behavior of the computation. We construct the following table.

Table 1. The Rank Division of Interactive Behaviors

Category	Weight	Description
V (vital)	4	Very important interaction
I (important)	2	Important interaction
O (ordinary)	1	Ordinary interaction
S (secondary)	0.5	Secondary interaction
T (thumbnail)	0.1	Very little important interaction

As can be seen from the previous table, we assign appropriate weights to different interaction behaviors. To some extent, we can distinguish the influence of different interaction behaviors on trust. The direct trust degree of A to N is D (A, N):

$$D(A,N) = \frac{\sum_{k-1}^{K} E_k(A,N) \times f_k \times w_k(A,N)}{\sum_{k-1}^{K} f_k}$$

In the above formula, f is the attenuation function, and its range is [0,1].

In social networks, users communicate with each other and communicate with each other. The user decides whom to interact with. After the interaction, the two sides evaluate each other and update their trust. The root user calculates the trust of each target user and chooses one of them according to their strategy to interact with each other. The size of the trustworthiness is the standard of whether the root user chooses the recommended information to recommend the user feedback.

The trust degree of the root user A to the target user N is calculated by combining the direct trust degree and the reputation value of the A to the N as a criterion for whether the A chooses the N to interact. The weighted average method is used to calculate the trust degree of A to N. The formula is:

$$T(A,N) = \propto \times D(A,N) + \beta \times I(A,N)$$

Privacy Protection Scheme of Mobile Social Network Based on Dynamic Trust Model

Basic Idea of Scheme. Privacy protection should ensure that the private information of the root user is not completed by the target user, and the efficiency of the system should be maintained within the acceptable range of the user. Because users have different requirements for information security, this paper introduces trust into privacy protection, and uses access control technology to protect users' privacy information. In the first scheme by the root user according to the sensitivity of the information to divide the different sensitivity level, then the root user according to the formula to calculate the trust degree of the target user, the target user's trust level corresponding to obtained by the trust degree, according to the trust level to determine whether the need to limit the target users to access their private information. With the rapid development of digital communication and information technology, all kinds of intelligent terminals, mobile Internet presents a spurt of development, greatly facilitate the people's lives, to bring a more rich and colorful way of life. The information exchange between users is more frequent, and it also brings more information sharing, and forms a large amount of online data. Illegal collection of user privacy data by criminals in the network is also very common, to bring trouble to people's life, even may pose a threat to people's life and property, privacy protection problem has become one of the biggest problems facing the rapid development of mobile internet. Root users evaluate trust objects that they want to interact with. According to the computing method of trust in mobile social network, the trust degree of target user is calculated by root user. Therefore, in the mobile Internet environment, how to effectively protect the user's privacy information has important practical significance, but also one of the current research hotspots. Considering the location and real-time characteristics of mobile Internet, the position and time states are introduced, and the dynamic method in mobile Internet environment is given.

Key Technologies of Scheme. Access control is to prevent access to certain information by irrelevant users or to prevent the use of certain important functions by restricting access rights of other users. Access control is the subject's different authorization access to the object itself or its service resources according to the control policy. Access control is an important means to ensure the confidentiality and availability of the system. The main purpose of the access control is to restrict the unauthorized access to the object, and to ensure that the data is used within the legal scope. Access control can be divided into two levels: physical access control and logical access control. Physical access control refers to the requirements of personnel, hardware, equipment and so on, and the logical access control is implemented at the level of data, system, authority and so on. The government, banks, troops and other confidentiality requirements of the site, the information security requirements of the two considerations. Access control can be divided into two categories: discretionary access control and mandatory access control. Discretionary access control refers to the user has the right to access the object created, and can make these permissions to other users or be granted permission to withdraw; mandatory access control refers to the control of unified system mandatory for objects created by the user. Access control, as a technical means of security services, has important significance in distributed security system. Access control technology has been paid much attention by information security researchers both at home and abroad, and it is of great value to study access control technology. The user has the right to access the objects he or she created, such as files, data tables, etc.,

and can grant access to other users or recover their access rights. A principal that allows access to an object makes a control policy for access to that object, usually by restricting access to the object executable through the access control list.

Process Description of Scheme. Privacy protection trust will change with time, users and other factors change based on the process from the root user to the target user interaction request issued to the end protection strategy after computing the trust, security classification determination. The whole process can be divided into the following 4 stages: the sensitivity of the users to the information classification, the security level of the target users, the comparison of judgments, and the provision of resources to interact with each other. The sensitivity of the root user to the information is generally different. The users with low sensitivity have low demand for information protection, and the users with high sensitivity need to implement strong protection measures. Since users may have different sensitivity requirements for information at different times, it is necessary to perform sensitivity classification after each interaction request is made. The security level of the target user is also a basis for the privacy of the root user. The root user according to indirect recommendation information directly interaction history and friends past calculation of the target user's trust, which can be used in the above formula is calculated according to the calculated trust of the target user security level evaluation. From the point of view of the mobile social network's confidentiality, integrity and availability of the three angles, analyze the security demand of mobile social networks, and the privacy protection scheme is discussed in this chapter can play a role in the network. The purpose of users to use social networks is to share information and communicate with their friends. Usually, the higher the frequency of user information, the more likely it is to get the attention of its friends. We enjoy the social network to bring us convenience, but also to ensure the safety of user privacy information. After the root user gets the security level of the target user, he compares his information sensitivity with the security level of the target user, and decides whether or not to provide his information to the target user for interaction. If the root user's sensitivity to the information is less than the target user's security level, the target user can obtain the root user's information, otherwise, the access is not available.

Conclusion

As a popular industry in mobile internet applications, social network has a large user scale and plays an important role in people's daily life. Therefore, it is of great significance to study the security of mobile social network. In different social networks, a user may register with different identities, which means that the user has different social connections in different social networks. It is the research direction of this paper how can we protect the Privacy Protection in this circumstance.

Acknowledgements

This research was financially supported by the Key Research and Development Program (General Program) of Shaanxi Provincial science and technology Department (Program No. 2017GY-094), the Key Research and Development Program (General Program) of Shaanxi Provincial science and technology Department (Program No. 2017GY-062) and the Special Scientific Research Program Funded by Shaanxi Provincial Education Department (Program No. 17JK1102).

References

[1] Shao Jianyu, Chen Fuzhen, Qin Pengyu, Cheng Jiujun. Research on Access Control Method Based on Dynamic Trust Degree in Mobile Internet Environment [J]. Netinfo Security, 2016(8): 46-53.

[2] Chen Danwei, Yang Sheng. Dynamic trust level based ciphertext access control scheme [J]. Journal of Computer Applications, 2017,37(6): 1587-1592+1615.

[3] Zhu Lirong, Chen Ningjiang, He Peicong, Liang Xiaoyu, Xie Qiqi, Huang Ruwei. A cloud user behavior authentication system based on dynamic trust management [J]. Journal of Guangxi University (Natural Science Edition), 2015, 40(6): 1485-1493.

[4] Jiang Weijin, Xu Yuhui, Guo Hong, Xu Yusheng. A multi-dimensional evidence dynamic trust computing model based on multi-agent [J]. Journal of Shandong University (Natural Science), 2015, 50(1): 1-11+19.