ATLANTIS PRESS

Advances in Engineering Research (AER), volume 148

3rd Workshop on Advanced Research and Technology in Industry Applications (WARTIA 2017)

Research on Key Technologies of Privacy Protection in Mobile Social Network

Yaofeng Miao, Yuan Zhou, Zhihui Liu

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

Keywords: Privacy protection, Mobile social network, Security technologies

Abstract. With the development of mobile internet technology and the popularity of smart mobile terminals, mobile social network has become an increasingly social revolution. Mobile social networks not only provide users with more personalized services, but also bring privacy leaks. This paper analyzes the main types of information leakage in mobile social networks, and proposes the key technologies of privacy protection in mobile internet social networking, including suppressing publication technology nearest neighbor technology and false trajectory technology to provide some references for the relevant researchers.

Introduction

Mobile social networks originate from the traditional social networks. It is an extension of traditional social ideas in mobile terminals such as smart phones and tablet computers. It realizes the innovation based on traditional social network, positioning system can provide users with real-time, in the actual, personalized service, and further realize the interpersonal relationship in the online transfer line, highlighting the authenticity of the characteristics of mobile social network. Mobile social network inherits the features of traditional social network, such as diversity of content services, large user groups, self-organization, diversified forms of communication and strong interactivity. At the same time, with the development of Internet technology, the continuous upgrading of smart terminals and the continuous improvement of wireless coverage, mobile social network has derived some new features. Access to online services based on mobile terminals. The popularity of intelligent mobile terminals and the upgrading of Internet technology have brought about the mobile features of mobile social networks, including the mobility of devices and the mobility of networks. Mobile social applications to achieve permanent online through the mobile Internet users, if the cellular mobile network will open the mobile phone information received text, pictures, video and other forms of language, the new browsing circle of friends. Different classification standards also show the privacy of mobile social applications hidden security problems. From the operator classification, the major operators in the pursuit of economic interests, the pursuit of the market, the pursuit of the number of users, easy to appear some quick behavior; from the functional perspective, a mobile social network service provides greatly satisfy the user's entertainment, communication and access to information needs. On the other hand, with continuous practice, the user's social relations, personal basic information, daily life and other privacy are exposed.

Current Situation of Privacy Leaks of Mobile Social Network

Leak of User's Basic Information. Mobile social network user's basic information including basic personal information users in the registered account, such as mobile phone number, email, personal names, personal pictures, the information is the basis for user access to services. Social networking and mobile social network social idea to encourage users real name registration, on the one hand, improve the efficiency of communication between users, increase the strength and structure of the social network user viscosity, on the other hand also increased the risk of leakage of user

privacy. Social applications and mobile social applications always hope that users can provide more complete personal information to achieve the application of intelligent upgrade, personalized service purposes, increasing the strength of the user network connection. And users fill in false information will also affect their use of social applications function and use effect. Such as mobile phones, only in the accurate completion of the name, educational background and other information, to achieve the purpose of looking for students, friends. A social networking profile continues to improve, the basic personal information scattered in the network constantly enrich will cause the user is accurately and quickly, human flesh search personal communication mode has become a variety of advertisers to target communication space has become distributed spam messages. At present many social applications and mobile social applications through mobile phone verification code in the form of access to the user's personal information effectively, this behavior largely led to the disclosure of user mobile phone number, e-mail and other information, and suffered from spam and advertising harassment.

Leak of User's Position Information. The location information of the mobile social network to fill the lack of traditional user's body in a social network, which brings the return of the authenticity of interpersonal communication, on the other hand also increased the burden of user privacy protection. At present, based on the rich experience of terminal, mobile social applications almost all support users to share feelings, whenever and wherever possible, photos and other personal information, and with accurate location information. At the same time, the application also allows users to achieve through the position information of strangers dating experience. Compared with the simple location-based services, mobile social location information is based on social and mobile features, and achieve precise positioning, which is more likely to expose the user's personal privacy. First, the exposure of accurate location information increases the risk of user tracking. An attacker can quickly locate the location, even the exact location, based on the location information of the user. Therefore, accurate positioning which greatly affect the user's personal safety; secondly, according to the position information of the frequency of related users, such as home address, address, and the usual habit activities address is easy to accurately guess, it also increases the risk of live in the reality of life and user factors; finally, according to the position information to strangers dating also increased form factors affecting users' personal safety and privacy protection. Because WeChat, unfamiliar street strangers and other social applications to meet friends, and suffer personal and property losses of the actual case is not a minority. With the development of location-based services, location-based service based on situational awareness has become the focus of attention because of its ability to provide users with more humane services. Researchers need to collect many mobile location data to provide richer contextual information. However, location data conferences disclose privacy information about the user's habits, interests and hobbies. On the other hand, location-based services, such as social media, require users to disclose their location information in many cases.

Leak of User's Trajectory Information. The mobility features of mobile social networks facilitate the daily life of users, and the emergence of lower class names, to a large extent, illustrates the impact of mobile social networks on the current society. Track information not only refers to the user's data track data, but also refers to a special location information which is based on the mobility and consists of the user's multiple location information. Here, we focus on trajectory information as special location information. At present, the user through the mobile terminal positioning discontinuity is not uncommon, many users are accustomed to a new place, which is related to the positioning and publish relevant information. In fact, when users use positioning at different times and different times to obtain relevant experience, the user's trajectory has been formed, and has become an important part of the user's personal privacy. Trajectory privacy mobile social networking users to a certain extent is to reproduce the life trajectory of the user, not the law of the trajectory of leakage of user privacy index is low, accurately infer and predict user attackers usually cannot be the next step or the next trip. However, the regular trajectory can easily disclose the trajectory information of the user's daily life, and can easily infer other relevant information of the user, such as daily arrangements, physical health, personal interests, hobbies and so on. To protect the privacy of users,

information security needs to be processed before the location data is sent to other data analysts. The main consideration is that the data analysis method is unreliable, and the data security is not affected while the data security is guaranteed.

Key Technologies of Privacy Protection in Mobile Social Network

Suppressing Publication Technology. The main idea is to suppressing publication of some sensitive information in the information track position, so even if the attacker gets lucky real track information of the user, but because of the lack of user sensitive location information in the information track, so relatively can also reduce the attacker for privacy threat to a certain extent. However, if the sensitive location is completely suppressed and not released, it will inevitably affect the quality of service of the user. For example, the query service in this location is very important to the user. To solve this problem, this paper for the sensitive position taken in selective trajectory information replacement strategy, choose a non-sensitive position to replace the sensitive position, and the distance between the two positions should be within the acceptable range. This can not only satisfy the service quality of users, but also ensure the security of the user's track privacy effectively. Cut off the connection between the path information and user identity information, even if an attacker to obtain a complete track information, but if not, the track information associated with a specific user, then the attacker can give users privacy threats. The protection of sensitive position trajectory information, the attacker to obtain only a complete path information, lack of position sensitive information related to user privacy, also will not cause too much of a threat to user privacy. Prevent the attacker from getting background information to obtain user's track privacy information. In the track privacy protection, if effectively solve the above problems, it basically achieves the goal of privacy protection of the user track. Any trajectory privacy protection algorithm should be established under certain preconditions, and must be directed against a specific attack model.

Nearest Neighbor Technology. The nearest neighbor technology is the core idea if a majority of the most adjacent samples in the feature space of the samples belonging to a certain category, the sample also belong to this category, and has the characteristics of the sample category. In determining the classification decision, the method determines only the category of the sample to be divided according to the category of the nearest one or a few samples. The nearest neighbor matching method is only related to very few adjacent samples in class decision making. The nearest neighbor matching method mainly depends on the sample around the adjacent finite, rather than by the method of discriminant domain to determine the category, so cross or overlap more for the domain of the test samples set, the nearest neighbor matching method is more suitable than other methods. Based on user history trajectory data learning, mobile characteristics can establish the corresponding model to describe the user, in the online service stage, according to the current location information of the user, for the future location of the probability of a certain moment to make predictions; or in the off-line phase, according to the non-blank information node offline sample data the completion of the blank position information. Maintain a large to small priority queue at a distance, used to store nearest neighbor training tuples. Random selected from training tuple as nearest neighbor tuple initial, calculated to test this tuple distance, the tuple labeling and distance training in the priority queue traversal training tuples, calculate the training and testing of the tuple distance, the distance and the maximum distance in the priority queue is compared. Traversing the next tuple. Removes the largest distance tuples in the priority queue and stores the current training tuples into priority queues. Calculates the majority class of the priority queue and takes it as a class of test tuples. Test tuple, after testing, calculate error rate, continue to set different values, training, and finally take the minimum error rate.

False Trajectory Technology. False location technology is often used to protect user's location privacy, query for privacy protection in the single point position, the use of false location technology is a kind of user location information of the true generalization means for constraints of false selection of position is not too large, if the anonymous region formed within the guarantee the spatial scope of

user acceptance can be. Similarly, the false track method can also be used in the user's track privacy protection. The more the number of false track information generated by the user, the protective effect on trajectory privacy better, but too many false trace information is bound to increase the system computation and affect the quality of user service. The number of false usually trajectory information set by the user's own privacy protection degree to decide the number of false generated trajectory information, user privacy protection effect on the trajectory of the better, but too many false trace information is bound to increase the computational overhead and system user service quality. The number of false track information is usually determined by the privacy protection set by the user itself. Mobile social applications of strangers making friends, it greatly expanded the scope and number of user's weak connection. If users open the location function, they may be positioned and searched by countless strangers. If this time the user is negligent of setting up personal privacy, that means exposing their privacy to thousands of strangers. The large number of relationships in mobile social networks has greatly affected the security of user privacy. Users must be aware of the existence of this weak link and set up relevant personal information in a timely manner. The structural differences between the track and the real track of the false of the attacker, false and true information of an attacker to identify the true trajectory information is more difficult. Therefore, when generating false trajectory information, we should try to ensure that the false track information has the same structure as the real trajectory information. For attackers, the more similar the structure between the false track information and the actual trajectory information, the more difficult the attacker is to identify the true trajectory information. Therefore, when generating false trajectory information, we should try to ensure that the false track information has the same structure as the real trajectory information. Thus, in the false track privacy protection method, the selection of false location may affect the effectiveness of the algorithm.

Conclusion

With the rapid development of mobile technology and the popularity of smart portable devices, mobile social networks are more and more accepted by most mobile users. As people enjoy the convenience of mobile social networks, they are also faced with a series of security problems. This paper puts forward the solution of the privacy protection to the users. Although the scheme plays a role in protecting the privacy information of users to some extent, there are many problems that need to be further explored in the search of more lightweight algorithms.

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] Zhang Bowen, Chen Jing, Du Ruiying. Personalized trajectory privacy-preserving scheme for mobile social networks [J]. Application Research of Computers, 2017, 34(3): 871-874.

[2] Li Fengyun, Li Jinshuang, Xue Lifang, Sun Xinran. Privacy Protected User Proximity Computing Protocol in Mobile Social Networks [J]. Computer & Digital Engineering, 2015, 43(10): 1723-1728.

[3] Luo Entao ,Wang Guojun. A Novel Friends Matching Privacy Preserving Strategy in Mobile Social Networks [J]. Journal of Electronics & Information Technology, 2016, 38(9): 2165-2172.

[4] Chen Wen. Real-time Absence Privacy Protection in Mobile Social Network [J]. Computer Engineering, 2015, 41(5): 159-162+168.