IEEE NETWORK®
THE MAGAZINE OF GLOBAL INTERNETWORKING

EDITOR'S NOTE

Security and Privacy in Mobile Social Network

Xuemin (Sherman) Shen

Social networks extending the social circles of users have become an important integral part of our daily lives. With social networking tools, we are able to easily share information, images, and videos with our friends, and search for desirable service information with recommendations. As reported by ComScore, social networking sites such as Facebook and Twitter have reached 82 percent of the world's online population, representing 1.2 billion users around the world. In the meantime, fueled by the dramatic advancements of smartphones and the ubiquitous connections of Internet, social networking is further becoming available to mobile users and keeps them posted on up-to-date worldwide news and messages from their friends and families anytime, anywhere. The *eMarketer* estimates that up to 46 percent of mobile users will access their social networks with smartphones in 2014, while this number was merely 16 percent in 2010. It is envisioned that, with the growing number of smartphone users, a pervasive and omnipotent communication platform, the mobile social network (MSN), will become mainstream where smartphone users have extensive methods, from browsing over the Internet to querying nearby peers to obtain desired information.

The boom of mobile social network fosters a large volume of promising and smart mobile applications. Apple Inc. has greatly increased the number of mobile applications from 800 in July 2008 to over 825,000 in April 2013. Nowadays, as many smartphone users indulge themselves in enjoying various mobile social applications, they can no longer live or work effectively without using the applications. Despite the tremendous benefits brought by the MSN and applications, the MSN still faces many security and privacy challenges. Since applications normally require the access of users' personal information to serve users better, security and privacy preservation have not been paid much attention in many application designs. For example, in most social applications, users need to register with personal profiles, such as name, birthday, home address, and phone number, which are very likely to be disclosed due to the lack of protection. In the United Kingdom, the number of complaints and alleged crimes associated with Facebook and Twitter has increased by 780 percent in the last four years, resulting in about 650 people being charged in 2012. Besides, *Internet Safety* states that 29 percent of Internet related sex crimes in 2012 originated from the social networking sites. As the mobile applications enable smartphone users to interact with social networks pervasively, there will be more severe security and privacy concerns for users. In the following, three unique security and privacy issues in mobile applications are discussed: information leakage, location privacy, and trust relation.

Information Leakage in Autonomous Mobile Applications

Autonomous mobile applications enable smartphone users to query neighboring users and local service providers for the desired information through short-range wireless communications such as Bluetooth and near field communication (NFC). Autonomous mobile applications are easy to set up and have much prac-

tical value in our daily lives. A smartphone user can launch a local information search to consult other users nearby, who in turn will ask their friends, and so on, until the information is found. A smartphone user may search for a good restaurant by revealing her personal preferences to nearby users. If a smartphone user is looking for a carpool service, she may reveal her destination to local users who may then provide services to her if their destinations are in the vicinity. Also, patients can launch an application for healthcare purposes (e.g., to find others with similar symptoms or experiences). In all these applications, users are required to reveal their personal information (i.e., restaurant preferences, travel destinations, and symptoms) to others. Such information is highly privacy-sensitive, and malicious attackers may track a target user's behavior if they obtain the information. The current effective solution is to require a trustworthy mediator over the Internet to help the information requester receive the desired and accurate information from an information responder. However, autonomous mobile applications do not have such an Internet mediator, and it is very difficult to find a third user who has a well established trust relationship with both the information requester and the information responder in physical proximity. As such, lightweight and energy-efficient authentication schemes and secret handshake protocols need to be integrated into the applications. Smartphone users should interact only with other authenticated users in autonomous mobile applications to prevent information leakage.

Location Privacy in Location-Based Applications

In addition to voice service available for any cellular telephone, smartphones distinguish themselves with powerful computing resources and, most significantly, their capability to understand their surrounding environments through many built-in sensors. As a result, location-based applications have become very popular. In such applications, selected information is downloaded from the Internet to assist location-based activities. Such applications are widely supported by either social network giants such as Facebook, or specialized service providers such as Foursquare and Loopt. The main idea is as follows. The GPS chip in a smartphone detects its location coordinates, which are then reported to Internet service providers for downloading information related to local services. However, such a process raises a serious privacy issue: the continuously disclosed location coordinates reveal where, when, or even what the smartphone user has been doing. If the location information of a user is revealed to malicious attackers, the attackers will know when the user is not at home and can break into the user's house to commit criminal activities. To prevent any abuse of location information, smartphone users have to often manually switch on and off the localization function to self-control the access of their location information. Another solution is to use cryptographic pseudonyms for mobile users such that the user's behaviors and locations cannot be easily linked. Another solution is to blur the location with an area of the vicinity or mix their identities with nearby other users. However, the former is energy-consuming, while the latter may degrade the application performance in terms of accuracy of services. Therefore, dealing with location privacy is very critical in location-based applications.

Trust Relation in Mobile Applications

The trust relation is fundamental to mobile applications, and affects user experiences of the applications. Mobile applications can only be adopted by smartphone users if they have trust in the Internet service providers, local service providers, and other smartphone users. While smartphone users enjoy conveniences brought by mobile applications maintained by Internet service providers, they realize that more and more personal information is revealed and start questioning how the service providers keep the collected personal information (e.g., whether or not the service providers will disclose the information for other purposes without proper consent). Doubts about trustworthiness will bother users in launching mobile applications. Furthermore, the trust relation of customers toward service providers is influenced by many social factors. The trust relation of new customers toward a service provider is tightly related to reviews from previous customers. Some mobile applications enable customers to quickly exchange their reviews. Strong recommendations from close friends can effectively strengthen the trust relation. However, in reality, the reviews can be forged, and customers do not want to reveal their identities in the recommendation process. So far, how to build the trust relation among smartphone users in mobile applications remains a challenging issue.

A trust relation also exists among users based on their common social communities. Users in a common community often have a certain trust level with each other, as they either share some common interests or recognize each other to some extent. With the initial trust relation, smartphone users can carry out local social activities via mobile applications, and further strengthen the trust relation. In such a trust establishing process, mobile applications are vulnerable to notorious sybil attacks where an attacker manipulates bogus identities or abuses pseudonyms to compromise the effectiveness of systems. Especially in the MSN, as smartphone users often adopt multiple pseudonyms to protect their location privacy, it is very challenging to restrict sybil attackers who legally have multiple pseudonyms but maliciously use them. In addition, sybil attacks can be extended to the mobile domain and be launched by mobile users anytime, anywhere. It is a complex task to promptly detect such attacks, due to difficulty in monitoring and characterizing their behaviors in a mobile environment.

In conclusion, although the MSN brings tremendous benefits to our daily lives, it introduces serious and emerging security and privacy issues that permeate the cyber and physical space around us. In the presence of many new and unique research challenges, long-term efforts in multi-disciplinary research are necessary. I hope that you enjoy reading this Editor's Note, and find it interesting and helpful.