# POSTER: LocMask: A Location Privacy Protection Framework in Android System

Qiuyu Xiao, Jiayi Chen, Le Yu, Huaxin Li, Haojin Zhu
Shanghai Jiao Tong University
Shanghai, China
{xiaoqiuyu, edjason, yule5100309221, lihuaxin003, zhu-hj}@sjtu.edu.cn

Muyuan Li, Kui Ren
University at Buffalo
Buffalo, NY, USA
{muyuanli, kuiren}@buffalo.edu

## ABSTRACT

The mobile users are facing a serious risk of losing location privacy (e.g., users' location information transmitted by open advertisement network, and the reported event of involuntary tracking of mobile users in popular mobile social apps). In this study, we design and implement LocMask, a system-level solution that provides location privacy protection in Android system. LocMask achieves the tradeoff of the privacy and the utility of location based services by providing the Quality of Protection (QoP) on demand, which sets different privacy protection levels to different locations based on how sensitive these locations are. Motivated by the fact that Top locations (e.g, user's home or office) are more sensitive than less visiting locations, LocMask provides location profile management module that records the user's mobility history and ranks the locations in terms of the user's visiting frequency. With users' location profiles, LocMask can automatically determines the sensitiveness of these locations as well as their corresponding privacy protection level. LocMask is also designed to incorporate various obfuscation techniques. The effectiveness of LocMask is supported by extensive real-world data based evaluations.

## Categories and Subject Descriptors

C.2.0 [**Computer-Communication Networks**]: General—*Security and Protection*

## Keywords

Location privacy; Smartphone security; Android

## 1. INTRODUCTION

As an important tool in facilitating coordination and communication among people, smart phone together with a wide range of apps forms a revealing montage of people's life by recording not just calls made but of medical concerns, political preferences, romantic involvements, financial resources and other sensitive information. Among different privacy issues, location privacy leakage in smartphone is receiving an increasing attention. It has been pointed out that 100 representative ad libraries are used in 52.1% of 100000 apps and 27 of the top 50 libraries requesting user's location data[3]. More seriously, most of the ad libraries don't encrypt their ad requests due to the extra overhead[6]. Thus, the location information of numerous users is public to not only the ad providers but also any network sniffers who can eavesdrop ad traffic between users and ad providers.

Another typical example of location privacy leakage comes from location-based social discovery apps (e.g., Wechat and Skout) which allow the users to discover new friends based on their proximity testing. A recent research [4] shows that attackers can exactly geo-locate the victim by only exploiting the public information of the users. Recent studies have shown that four spatial-temporal points are sufficient to identify the individuals in an anonymized mobility data set[2]. Note that users' location traces can leak much information about the individuals' habits, interests, activities, and relationships as pointed out in [5]. And loss of location privacy can expose users to unwanted advertisement and location-based spams/scams, cause social reputation damage or property loss, and make them victims of blackmail or even physical violence.

In the past years, there are quite a few works proposed for location privacy protection including: k-anonymity, mix-zone and various obfuscation techniques. However, none of the existing works provide a system-level countermeasure for location-privacy protection in smart phone systems such as Android. In this study, we present LocMask, a system-level solution that provides location privacy protection in Android system. LocMask has the following features: 1. Providing the Quality of Protection (QoP) on demand. It is motivated by the following fact. On the one hand, the privacy comes at a cost, and will inevitably reduce the utility of LBS applications. On the other hand, for a specific user, different locations may potentially require different privacy protection levels. For example, the Top 2 Locations of the user (e.g., home or office) are closely relevant to his identity and thus require a high privacy protection level while the public regions (e.g, shopping malls or cinema) need a relatively low privacy protection. 2. Determining the privacy level based on automatic location profile management as well as user's preference. LocMask provides location profile management module that records the user's mobility history and ranks the places in terms of the user's visiting frequency to deter-


*CCS'14,* November 3–7, 2014, Scottsdale, Arizona, USA.
ACM 978-1-4503-2957-6/14/11.
http://dx.doi.org/10.1145/2660267.2662367 .

mine the sensitiveness of these places as well as their corresponding privacy protection level. LocMask also provides flexibility for users to determine their privacy level based on their personal preferences. 3. Being compatible to the existing obfuscation techniques, LocMask will be compatible to rather than be a replacement of the existing obfuscation techniques. In other words, a diversified range of obfuscation techniques can be adopted in LocMask.

# 2. FRAMEWORK DESIGN AND IMPLEMENTATION

In this section, we will introduce LocMask, a novel location privacy protection framework in Android, and explain the strategies behind it.

## 2.1 Design of LocMask

LocMask aims to provide location privacy protection for Android users without significantly reducing the Quality of Protection (QoP) of users. The basic idea of LocMask is assigning different privacy levels to different locations to achieve the balance of the privacy and the utility. To reduce the load of manually setting the value to each location, we correlate the privacy level of each location to the user's visiting frequency, which is motivated from the fact that the locations with a higher visiting frequency are more closely related to the user's identity and thus more sensitive to this user (e.g., Top Locations). In general, LocMask is comprised of the following modules: Privacy Level Setting Module, Location Profile Learning Module and Obfuscation Module.

### 2.1.1 *Privacy Level Setting Module*

As described above, LocMask allows the automatic privacy level configuration for Android users by correlating the privacy level with their location profiles. The existing researchers show that the human's mobility is generally predictable and 94% indiviuals' daily activity is confined to a limited neighborhood of less than 100 km[2]. By obtaining the location profiles of users, the more frequently visiting locations will be set to a higher sensitive level, which leads to a higher privacy protection level and a bigger obfuscation range. In case that the privacy levels do not fully match users' preferences, LocMask also allows the users to set the privacy levels for specific locations or apps.

### 2.1.2 *Location Profile Building Module*

One of the main features of LocMask is to correlate the privacy protection levels of different locations with users' location profiles, which can naturally differentiate the Top locations (office or home) from other less sensitive regions (public regions). Location Profile Building Module is designed to collect users' historical trajectory and then build users' location profiles. We model the trajectory of a specific user $\mathcal{U}$ as a function mapping a time point in $\mathcal{T}$ to the user's location in $\mathcal{R}$ at that time, i.e., $\alpha_u : \mathcal{T} \rightarrow \mathcal{R}$. Thus, if the user traverses $k$ POIs for $k$ different time slots, the real mobility traces of the user $u$ can be denoted as $\mathcal{M} =<< u, t_1, \alpha_u(t_1) >, \ldots, < u, t_k, \alpha_u(t_k) >>$. By collecting a certain duration of users' trajectory, Location profile building module will obtain the location list of the users as well as the possibilities of visiting these locations.

### 2.1.3 *Location Obfuscation Module*

LocMask can support various obfuscation techniques, including: distance-based obfuscation, cloaking techniques, and etc [1]. Obfuscation techniques protect a user's location privacy by deliberately degrading the quality of information about that user's location. LocMask provides a general interface for each obfuscation mechanism to intercept the original locations and return the obfuscated results. With this interface, each obfuscation technique can be easily implemented in Android and existing LBS applications don't need any modification. Moreover, LocMask can incorporate privacy level mechanism into existing obfuscation techniques, which can achieve a balance of location privacy and the QoP of location-based service.

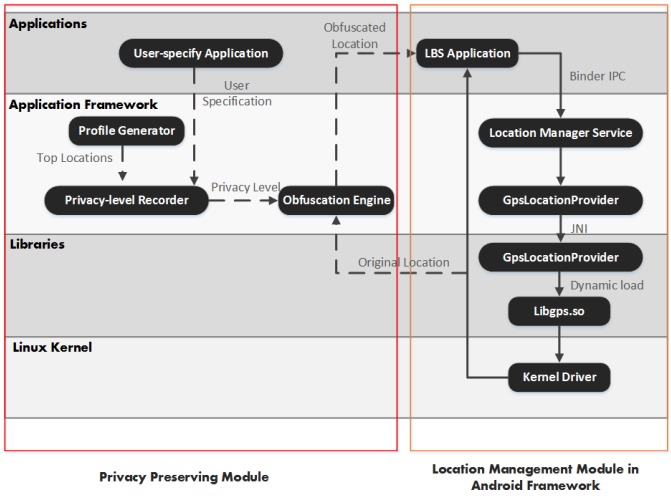



**Figure 1: LocMask Architecture**

## 2.2 Framework Implementation

Based on the strategies discussed above, we designed and implemented LocMask as a location-privacy preserving module in Android system. Figure 1 illustrates the baseline architecture of LocMask, which comprises of four components.

**User-specify Interface:** Provides an interface for users to specify their location sharing preferences. User-specify interface was implemented as an system application in Android as shown in Figure 2. This application can report the LBS apps by scanning the manifest file to find *ACCESS_COARSE_LOCATION* or *ACCESS_FINE_LOCATION* permission. The application can also show the geographic positions in a map. And then users can specify privacy preserving level for LBS apps and geographic positions to meet their requirements.

**Profile Generator:** Collects user's location information and stores user's mobility history in the local database. We implemented a LocationProfile class in Android framework. This class provides methods to execute clustering algorithm in the mobility data set, and then extract user's location profile. Location profile records user's Top N locations, which will be assigned privacy preserving level according to their sensitiveness.

**Privacy-level Recorder:** Saves the privacy preserving level for each geographic position and LBS app. There are four privacy levels in LockMask, which are low, medium,

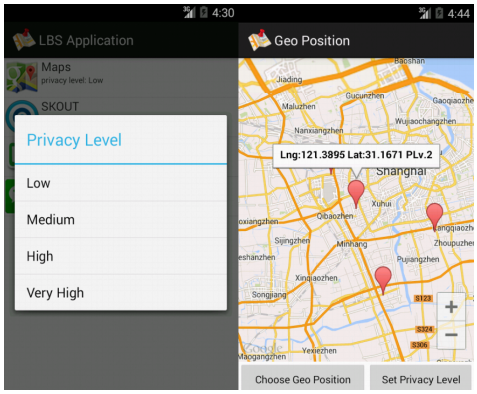



**Figure 2: User-specify Interface**

high and very high. Privacy level information is stored as XML file in the SystemDir of Android file system and will be used to compute obfuscation range in our obfuscating process.

**Obfuscation Engine:** Implements obfuscation techniques and executes obfuscation process. We add a function, ObfuscateLocation(), in LocationManager class. ObfuscateLocation() provides the interface for different obfuscation techniques. Parameters of this function are the original location and the package name of query app, which can be used to query privacy level. We also modified Android location requesting APIs so that whenever they are invoked by a query app, they will call obfuscateLocation() and return the obfuscated result to the query app.

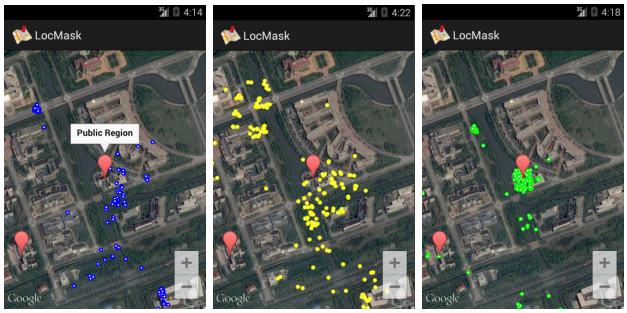
## 2.3 Obfuscation Mechanism

We implemented a hybrid obfuscation method for LocMask. This hybrid method includes two different obfuscation techniques. The first obfuscation technique is introduced in [1]. There are three basic obfuscation operators in this technique, which are *radius enlargement*, *radius reduction* and *center shifting*. LocMask executes obfuscation by randomly combining these obfuscation operators. This obfuscation technique will be selected when privacy level is low or medium (or the LBS has a certain requirement on the precision).

For the privacy level high or very high or LBS only needs a low requirement on the precision (for example, the location based advertisements normally have a low requirement for the precision), LocMask uses a novel obfuscation technique, which let obfuscation results deviate to the public region (e.g, shopping malls or cinema). Users don't want to disclose their real locations in these privacy levels, so LocMask tries to disguise user's location as public region, which is less sensitive and informative. This technique is useful for defending malicious or unwanted location requests.

# 3. EXPERIMENT AND RESULTS

We conducted a 3-week experiment to test LocMask. 15 volunteers attended this experiment by using the modified Android system which incorporates LocMask. In the first 2 weeks, we gathered each user's location data to generate location profile. We also let users specify their location preserving preferences. In the last week, LocMask began to obfuscate each location request according to location profile and user's preferences. Figure 3 shows some original and obfuscated locations of a volunteer. Blue points are original locations. Yellow points are obfuscated results from the first obfuscation technique and green points from the second technique as described in 2.3. We can see that LocMask can successfully obfuscate users' location and protect their location privacy.




(a) Original data (b) Technique 1 (c) Technique 2

**Figure 3: Obfuscation Results**

# 4. CONCLUSION

In this poster, we present a novel location-privacy preserving framework, LocMask, in Android system. Without any change on existing LBS applications, our framework can provide tailored protection for each user. For our future work, we are planning to incorporate other advanced privacy-preserving technics into our framework to get better performance.

# ACKNOWLEDGEMENT

This research is partially supported by NSFC (No. 61272444).

# 5. REFERENCES

[1] C. A. Ardagna, M. Cremonini, S. De Capitani di Vimercati, and P. Samarati. An obfuscation-based approach for protecting location privacy. *Dependable and Secure Computing, IEEE Transactions on*, 8(1):13–27, 2011.

[2] Y.-A. de Montjoye, C. A. Hidalgo, M. Verleysen, and V. D. Blondel. Unique in the crowd: The privacy bounds of human mobility. 3, 2013.

[3] M. C. Grace, W. Zhou, X. Jiang, and A.-R. Sadeghi. Unsafe exposure analysis of mobile in-app advertisements. In *Proceedings of the fifth ACM conference on Security and Privacy in Wireless and Mobile Networks*, page 101ÍC112, 2012.

[4] M. Li, H. Zhu, Z. Gao, S. Chen, K. Ren, L. Yu, and S. Hu. All your location are belong to us: Breaking mobile social networks for automated user location tracking. In *MobiHoc*, 2014.

[5] B. Schilit, J. Hong, and M. Gruteser. Wireless location privacy protection. *Computer*, 36(12):135–137, 2003.

[6] R. Stevens, C. Gibler, J. Crussell, J. Erickson, and H. Chen. Investigating user privacy in android ad libraries. In *Workshop on Mobile Security Technologies (MoST)*, 2012.