Poster: Analysis of User Privacy in Mobile Geo-location sharing: You are not Traveling Alone.

Siva Kumar Sudikonda[1] , Venkata N Inukollu[2]
School of Science and Computer Engineering
University of Houston, Clear Lake
[1]Sudikondas2704@uhcl.edu, [2]Inukollu@uhcl.edu

Abstract
The mobile marketplace is growing apace and so are the privacy attacks on the end-users. Location of the users is one of the most important and fascinating pieces of information to the app developers and in particular to the marketers as it reveals the activity patterns and the habits of the users. In the current smartphone era, The apps based on Location based services (LBS) are ubiquitous and are employed in a variety of contexts, including social networking, businesses and personal life among others, thereby, providing a rich and dynamic user experience. While LBS have great potential for enhancing the economy and thereby increasing the revenue [1], nearly 26% of location based applications have compromised the privacy and security of the user personal information [2].

The idea of this poster is to expose the perils of sharing the physical location when the location is paired with personally identifiable information (PII) such as Mobile number and Email or Device ID. In particular, this research discusses the probability of connecting the geo-location and PII with other attributes such as User Name, Employment details, Education background, Address, Birthdate, Age, Gender, Interests and hobbies[3] of the individual user are presented in the poster.

Keywords: Location tracking, mobile privacy, data risks.

I. INTRODUCTION

Mobile devices have created a great impact on the human lifestyle and the way people communicate. The first generation of mobile phones was only focused on connecting people with a unique subscriber number. With the increasing mobility in urban environments and the portability of mobile devices, the second generation of mobiles are equipped with GPS to provide LBS. However, mobiles with GPS features continuously track the user's physical data and further continue to save the location history, thus raising privacy concerns [4]. Having no or limited end-user's knowledge and perception of threats and mitigations on location security, today it is effortless to find geotagged multimedia files on the social networks. This scenario alarms the necessity to take preventive measures to control and secure the private information of the users saved on the non-trusted servers.

The users of the mobile devices are dependent on the native or third party applications to perform their routine activities such as banking, shopping, navigation, reservations, online payments etc., as many app developers begin to provide their services. Mobile Applications or Apps are software programs specifically designed for usage on mobile devices, such as, smartphones and tablets.

II. APPLICATION BEHAVIOR ANALYSIS

Mobile Application behavioral analysis is a technique primarily devised to identify the risks and malicious conduct of mobile applications that compromise the privacy of the users by accessing the personal data on their mobile phones, including reading the contact information without the permission of the users, reading data from the data cards, and sending the mobile geo-location to anonymous sources among others.

A. Permission Analysis

Mobile platforms choose permissions for apps to secure sensitive data from non-trusted apps and third party developers. The permissions are primarily used to communicate to the users about what the app will access in their mobile phones and how the accessed data will be used.

B. Static Code Analysis

The executable output format of the code is analyzed without dynamically running the application. The objective of the static code inspections is to identify the risky components of the code that allow access to user's

browser history, record phone calls, and read system logs [5].

C. *Dynamic Analysis*

This method is the most effective and yields an accurate behavior of the application in comparison to the permissions and static code analysis. Dynamic analysis reveals the exact data that is transmitted and shared between the mobile client and the application server.

The below statistics indicate the severity of sharing the physical location with the Location Based Services (LBS) apps. The results depict that most of the apps share the location related information with at least one third party domain.

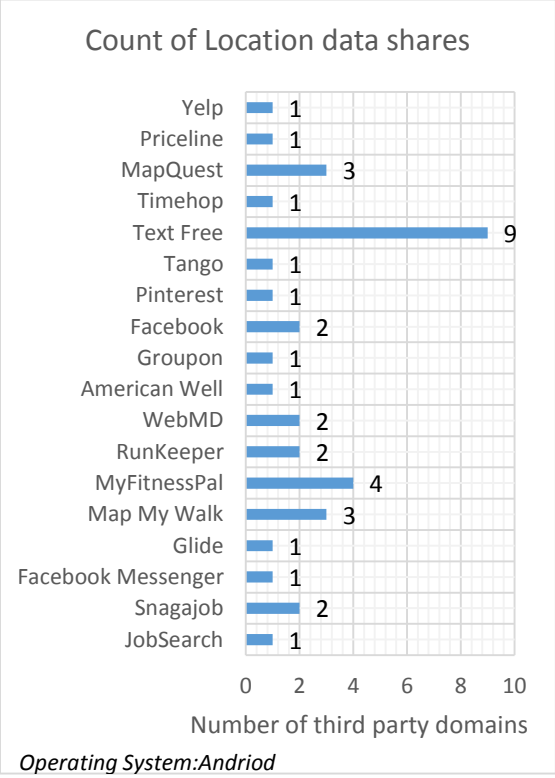

Fig. 1. Number of third party domain shares of the location data by mobile applications in Android OS.

III. OUR CONTRIBUTION

This research has made an effort to explain the direct need of prevention of sharing the Geo-location of the mobile users. In particular the research demonstrates how the user's personal and professional information can be gathered when the Geo- location is paired with any of the PII attributes, including, Mobile Number, Email Id and device ID.

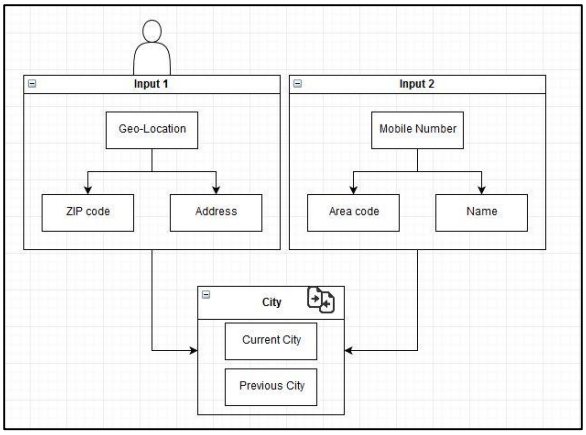

Fig 2. The Relationship between geo-location and Mobile Number attributes

Our approach to identify the personal and professional attributes of the user are presented in the poster. Typically, a combination of Mobile number with the location can reveal the name and address of the mobile user [6]. Mobile Number yields the Area code and the Name of the Subscriber. The Area code along with ZIP code derived from the Geo-location, calculates the evidence of user presence in the current city or the previous city.

IV. FUTURE WORK

Following Dynamic analysis on the LBS applications using Man in the middle Proxy approach, we continue the work by analyzing the sharing of sensitive data by mobile applications in varies categories of apps in market places such as App store and Google play.

V. REFERENCES

[1] **Location-Based Services Report** by Federal Communications Commission, 2012

[2] FPF Finds Nearly Three-Quarters of Most Downloaded Mobile Apps Lack A Privacy Policy by *future of privacy forum*, 2011

[3] Zang, J., Dummit, K., Graves, J., Lisker, P., and Sweeney, L., "Who Knows What About Me? A Survey of Behind the Scenes Personal Data Sharing to Third Parties by Mobile Apps," *Proceeding of Technology Science*, October 30, 2015.

[4] Rashmi, B., Samantha, L. R., and Dharma, P. A., "GPS: Location-Tracking Technology," *Proceeding of IEEE Computer*, 2002.

[5] Neil DuPaul. Static Code Analysis. Vera code

[6] Krumm, J., "Inference attacks on location tracks", *Proceedings of Pervasive*, 2007.