Hide me if you can. Location Blurring on FxOS

Marta Piekarska*
Security in Telecommunications
Technische Universitat Berlin

Abstract

Mobile phones become part of our daily life. Currently there are over two million applications in various Market Places. More and more of those require access to the location of a user in order to enhance her experience. However, if the information on where the device is might pose privacy threats. Geolocation may be used for targeted malware spreading, phishing, as well as posing a threat to the user’s physical security. In this paper we present a solution to the problem which allows the user to choose how precise her location is, on per-application basis. We implement our solution as a part of an emerging web-based OS, namely Firefox OS. The user can choose the granularity of the information given to the apps on several levels: precise, random, defined, as well as rounded to the city and country. Our solution is flexible, and does not influence services which require full precision like the lost phone trackers.

Keywords: location blurring, geolocation, mobile operating systems

1 Introduction

Location based services use the information about the geographical position of a mobile device to enhance the quality of experience (QoE) of a user. The integration of the Global Positioning System receivers(GPS) into the mobile devices made the task easy. No matter if the information is collected for valid, or not so good reasons, it always can be subject to interception and leakage. Because of that most mobile operating systems ask users to give their consent to reveal the location of their device. On Android this decision has to be made during the installation phase, when the list of permissions is shown, and one has to make a binary choice of either accepting all or rejecting them, thus not installing the app. On iOS when an application attempts to access the address book, calendar, location services and photo library a pop-up appears on the screen asking for the consent of the user. However, granting GPS access to the camera application that every photo will contain location data even when moved to e.g. social media.

2 Background

Any app for Firefox Operating System(FxOS) is a web app, meaning it uses HTML5, JavaScript, CSS or any other open Web technology. All system calls, including storage access, are done through the Web APIs. Additionally, there is a second mechanism that divides applications into three trust groups: certified, privileged, and web. The more trusted the app is, the bigger is the group of APIs it can access. Every time an app calls an API, system will consult the Manifest file to check if it was listed and if the type of the App (certified, privileged or web) is sufficient to grant the rights. Depending on the type of the API the access is either granted, or set to ‘prompt’. In the first case, if the app successfully passes through the Marketplace, it gets implicit access to the API. If, however, the API access will impact the privacy of a user, or the decision is simple (i.e. he can be expected to understand, what will be the impact of his choice), she will be prompted to choose.

3 Related Work

To address the privacy concerns of location based services several approaches have been proposed in academia. However, none of them made it to the real world system, be it because of the complicated design or political reasons. We believe that most interesting are the Orient Platform [Dunne et al. 2008], the CASPER [Mokbel et al. 2006], and the recent paper from Wolinsky et al. [Wolinsky et al. 2013].

4 Proposed solution

The solution we are proposing is a simple tweak to the original design of the FxOS web API architecture. What is important it only changes what the apps can see, and not the way the GPS works. This is important in cases of emergency like locating of a stolen device or- even more important - locating of a lost or hidden person. This also does not influence the way the service provider records the position of the users during a phone call. As depicted in the Figure 1 normally on FxOS, the app calls the GeolocationAPI. This forwards the request for location to the GPS driver, which activates the GPS receiver. Once the positioning is finished the result is delivered to the webAPI, which then hands the information to the app that requested it. In our solution the process is altered at a very late stage. Once the webAPI receives the position of the device it checks the granularity of the information set for the calling app. It then adjusts the information accordingly and returns the altered result to the application. In FxOS there is no other way to obtain the position other then with the use of the geolocationAPI, which means that the app cannot find out if the received information was changed in any way. Nor can it request more precise data.

5 Conclusion

The proposed scheme is a simple solution to the privacy concerns of the users, yet it does not influence the usability. It is fully adjustable, which makes it very flexible and easy to use. Because the solution does not interact with the GPS sensors themselves it should not collide with any laws. Most importantly this will be the first location blurring service that will be part of a vanilla OS, which makes it not only an important addition to the end-users privacy, but also a good compromise between security and usability.

References
