Privacy-Preserving Location-Proximity for Mobile Apps

Abstract:

Location Based Services (LBS) have seen alarming privacy breaches in recent years. While there has been much recent progress by the research community on developing privacy-enhancing mechanisms for LBS, their evaluation has been often focused on the privacy guarantees, while the question of whether these mechanisms can be adopted by practical LBS applications has received limited attention. This paper studies the applicability of Privacy-Preserving Location Proximity (PPLP) protocols in the setting of mobile apps. We categorize popular location social apps and analyze the tradeoffs of privacy and functionality with respect to PPLP enhancements. To investigate the practical performance trade-offs, we present an in-depth case study of an Android application that implements InnerCircle, a state-of-the-art protocol for privacypreserving location proximity. This study indicates that the performance of the privacy-preserving application for coarse-grained precision is comparable to real applications with the same feature set.

Introduction:

Location Based Services (LBS) have seen a tremendous growth in recent years. A single resource lists over 2900 services at the time of writing . The growth is boosted by the increasing spread of mobile devices, as Internet usage by mobile devices has come to dominate over desktop both by the number of users and time spent . Thanks to these developments, LBS-based mobile applications (or apps) have come to be a lucrative and thriving market. LBS in mobile applications lets users accomplish a variety of tasks, such as planning a route from one location to another or obtaining information about entertainment venues in the vicinity. By obtaining the location of their users, LBS are able to provide a personalized experience to their users. Unfortunately, location disclosure endangers the privacy of the user, opening up for a plethora of attacks. These attacks are typically classified into external and internal. The most intuitive kind of attacks are external,

where the attacker has a black-box view of the system and can act as an ordinary user. External attacks have been seen in many widely used applications such as Foursquare, Tinder and Grindr . These attacks often rely on techniques to precisely position users based on multiple distance queries. In these situations, the service provider is a Trusted Third Party (TTP) while the information being disclosed among users needs to be limited. Secondly, internal attackers have full access to the system, such as the LBS providers themselves. The smartphone app Uber, connecting passengers with private drivers, has been the subject of much privacy debate. Uber and its employees have been allegedly involved in privacy-violating activities from stalking journalists and VIPs to tracking one-night stands Given how powerful they are, internal attackers are significantly harder to protect against.