PRIVACY-PRESERVING LOCATION SHARING SERVICES FOR SOCIAL NETWORKS

ABSTRACT:

Using social Networks, such as FourSquare, millions of people interact with their surroundings through their friendsand their recommendations. Without adequate privacy protection, however, these systems can be easily misused, e.g., to track usersor target them for home invasion. In this paper, we introduce LocX, a novel alternative that provides significantly-improved locationprivacy without adding uncertainty into query results or relying on strong assumptions about server security. Our key insight is to applysecure user-specific, distance-preserving coordinate transformations to all location data shared with the server. The friends of a usershare this user's secrets so they can apply the same transformation. This allows all location queries to be evaluated correctly by theserver, but our privacy mechanisms guarantee that servers are unable to see or infer the actual location data from the transformeddata or from the data access. We show that LocX provides privacy even against a powerful adversary model, and we use prototype.

INTRODUCTION

This new functionality comes with significantly increased risks to personal privacy social networks operate on fine-grain, time-stamped location information. For current services with minimal privacy mechanisms, this data can be used to infer a user's detailed activities, or to track and predict the user's daily movements. In fact, there are numerous real world examples where the unauthorized use of location information has been misused for economic gain physical stalking, and to gather legal evidence. Even more disturbing, it seems that less than a week after Facebook turned on their popular "Places" feature for tracking users' locations, such location

data was already used by thieves to plan home invasions. Clearly, mobile social networks of tomorrow require stronger privacy properties than the open to-all policies available today.

EXISTING SYSTEM

Existing systems have mainly taken three approaches to improving user privacy in geo-social systems: introducing uncertainty or error into location data relying on trusted servers or intermediaries to apply an onymization to user identities and private data relying on heavy-weight cryptographic or private information retrieval (PIR) techniques. None of them, however, have proven successful on current application platforms. Techniques using the first approach fall short because they require both users and application providers to introduce uncertainty into their data, which degrades the quality of application results returned to the user. In this approach, there is a fundamental tradeoff between the amount of error introduced into the time or location domain, and the amount of privacy granted to the user. Users dislike the loss of accuracy in results, and application providers have a natural disincentive to hide user data from themselves, which reduces their ability to monetize the data. The second approach relies on the trusted proxies or servers in the system to protect user privacy. This is a risky assumption, since private data can be exposed by either software bugs or configuration errors at the trusted servers or by malicious administrators. Finally, relying on heavy-weight cryptographic mechanisms to obtain provable privacy guarantees are too expensive to deploy on mobile devices, and even on the servers in answering queries such as nearest-neighbor and range queries.