Building Privacy-Preserving Location-Based Services For Mobile Apps

Singampalli Sankeerthi[1], Pullagura Prasanna Kumari[2]
[1]Assistent Professor, Dept of MCA
[2]Dept of MCA
[1, 2] St. Mary's Group of Institutions, Guntur, Andhra Pradesh, India

Abstract- *Location primarily based Services (LBS) have seen alarming privacy breaches in recent years. whereas there has been a lot of recent progress by the analysis community on developing privacy-enhancing mechanisms for LBS, their analysis has been typically centered on the privacy guarantees, whereas the question of whether these mechanisms is adopted by sensible LBS applications has received restricted attention. This paper studies the relevance of Privacy-Preserving Location Proximity (PPLP) protocols within the setting of mobile apps. we reason popular location social apps and analyze the trade-offs of privacy and practicality with reference to PPLP enhancements. to research the sensible performance trade-offs, we have a tendency to gift AN in-depth case study of A humanoid application that implements Inner Circle, a progressive protocol for privacy-preserving location proximity. This study indicates that the performance of the privacy-preserving application for coarse-grained precision is corresponding to real applications with a similar feature set.*

Keywords- Location Based Services; Location Privacy; Privacy-preserving Technologies;

I. INTRODUCTION

A location-based service (LBS) is a software-level service that uses location data to control features. As such LBS is an information service and has a number of uses in social networking today as information, in entertainment or security, which is accessible with mobile devices through the mobile network and which uses information on the geographical position of the mobile device.[1][2][3][4] LBS can be used in a variety of contexts, such as health, indoor object search,[5] entertainment,[6] work, personal life, etc.[7].LBS is critical to many businesses as well as government organizations to drive real insight from data tied to a specific location where activities take place. The spatial patterns that location-related data and services can provide are one of its most powerful and useful aspects where location is a common denominator in all of these activities and can be leveraged to better understand patterns and relationships.

LBS include services to identify a location [8] of a person or object, such as discovering the nearest banking cash machine (ATM) or the whereabouts of a friend or employee. LBS include parcel tracking and vehicle tracking services. LBS can include mobile commerce when taking the form of coupons or advertising directed at customers based on their current location. They include personalized weather services and even location-based games. They are an example of telecommunication convergence.

This concept of location based systems is not compliant with the standardized concept of real-time locating systems (RTLS) and related local services, as noted in ISO/IEC 19762-5[9] and ISO/IEC 24730-1.[10] While networked computing devices generally do very well to inform consumers of days old data, the computing devices themselves can also be tracked, even in real-time.

There are a number of ways in which the location of an object, such as a mobile phone or device, can be determined.

Control plane locating

With control plane locating, sometimes referred to as positioning, the mobile phone service provider gets the location based on the radio signal delay of the closest cell-phone towers (for phones without GPS features) which can be quite slow as it uses the 'voice control' channel. [4] In the UK, networks do not use trilateration; LBS services use a single base station, with a "radius" of inaccuracy, to determine a phone's location. This technique was the basis of the E-911 mandate and is still used to locate cell phones as a safety measure. Newer phones and PDAs typically have an integrated A-GPS chip.

In order to provide a successful LBS technology the following factors must be met:

Coordinates accuracy requirements that are determined by the relevant service, lowest possible cost, minimal impact on network and equipment. Several categories of methods can be used to find the location of the subscriber. [2][20] The simple and standard solution is GPS-based LBS. Sony Ericsson's "Near Me" is one such example. It is used to maintain knowledge of the exact location, however can be expensive for the end-user, as they would have to invest in a GPS-equipped handset. GPS is based on the concept of trilateration, a basic geometric principle that allows finding one location if one knows its distance from other, already known locations.

Self-reported positioning

A low cost alternative to using location technology to track the player is to not track at all. This has been referred to as "self-reported positioning". It was used in the mixed reality game called Uncle Roy All around you in 2003 and considered for use in the augmented reality games in 2006. [21] Instead of tracking technologies, players were given a map which they could pan around and subsequently mark their location upon. [22][23] With the rise of location-based networking, this is more commonly known as a user "check-in".

To mitigate the attacks, there has been substantial progress on privacy-enhancing LBS [8], [9], [10]. Some approaches separate some parts of the system [11] in order to make it harder for an attacker to gain full white-box access to the service. While these studies address increasingly more powerful attackers, their evaluation has been often focused on the privacy guarantees. At the same time, the question of whether these mechanisms can be adopted by practical LBS applications has received limited attention.

This paper studies the applicability of PPLP in the setting of mobile apps. We categorize popular location social apps and analyze the trade-offs 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 Inner Circle [19], a state-of-the-art protocol for privacy-preserving location proximity. This study indicates that the features of PPLP fit several scenarios of real-world LBS and that the performance of such protocols is, for coarse-grained precision, comparable to real applications. To summarize the main contributions of the paper:

1) We evaluate to what extent a state-of-the-art protocol can be applied to mobile applications without limiting their functionality. The study uses popular location-based social apps from the Google Play Store.

2) We investigate performance trade-offs by performance measurements of an implementation of Inner Circle [19], a state-of-the-art privacy-preserving location-proximity protocol in an Android application. The study compares the performance of the implementation to real-world applications

The paper is organized as follows. Section II studies the applicability of privacy-preserving proximity-testing protocols to real-world LBS by investigating the privacy vs. functionality trade-offs. Section III presents necessary back-ground for the Inner Circle protocol. Section IV describes the architecture of the Android-based implementation of Inner Circle. Section V studies the performance of the protocol and compares it with the performance of the real-world apps. Section VI discusses the related work. Section VII offers concluding remarks.

II. LITECHURE SURVEY

The relevance of research on location-privacy has seen some debate, with studies showing mixed results on whether location-privacy is important to users of LBS or not. Barkhuus and Dey [26] compared the two scenarios of location-tracking services and location-aware services and performed an experimental case study with 16 participants. The participants had more privacy concerns regarding location tracking services compared to location-aware services, but in general were not overly concerned about privacy of their location data. Nevertheless, Barkhuus and Dey recommended focusing on developing services around location-aware concept. In case of location-tracking services, the researchers believe such services can still be acceptable as long as users have the option to turn-off the tracking capability at any time.

Xu and Gupta [27] developed a model to examine the impact of privacy concerns on intention to use LBS. They found that performance expectancy had a positive impact on participants' intention to use LBS and effort expectancy was positive only for inexperienced users, but privacy concerns had no direct effect. Interestingly, privacy concerns negatively impact performance and effort expectancy, thus indirectly affecting user decision to use LBS mobile services. This implies that privacy concerns are relevant to at least a limited extent to user of LBS applications.

Zickuhr [28] studied use of LBS in mobile apps by Americans. The findings show that the use of such applications is rapidly growing, from 55% of Smartphone owners using LBS applications in 2011 to 74% of Smartphone owners using LBS in 2012. Furthermore, taking into account that Smartphone ownership itself quickly grew from 35% of adults in 2011 to 46% in 2012, it is safe to assume that the importance of LBS privacy concerns, even if relevance is currently debatable, will grow in the coming years.

III. RELATED WORK

Privacy-Preserving Technologies

There is significant literature on both protecting users' privacy against internal and external attackers. For internal attackers, there are several generic techniques not tied to LBS. For external attackers on LBS, there are two core tracks [29]. The first idea is to minimize each individual disclosure. For instance, by disclosing distances instead of positions, etc. Secondly, a good countermeasure is to discredit the location data by dividing the plane into a grid, such that many coordinates in a grid-cell are mapped to the same location. The grid cells need to be large enough that the imprecision is sufficient to provide privacy. While the first often allows a service to remain unchanged while providing better protection, the second can provide strict guarantees of how much information the attacker is able to learn.

1) **Generic Privacy-Preservation**: For internal attackers, there are a number of different techniques. One popular strategy is the "k-anonymity model" [30], [31], [32], which hides the user among similar other users. This makes the original user indistinguishable from the rest of the population and thus anonymous. However, all efficient techniques for k-anonymity require a third party to be set up, which again opens up for internal attackers at this new party.

A generic approach to hide sensitive data from service providers is to utilize Secure Multi-party Computation (SMC), which is a research field of considerable size. SMC enables multiple parties to compute on private data without revealing their inputs. The ability to compute functions without revealing inputs allows for private data to remain confidential while being handled by 3rd parties, which completely removes the need for trusting a third party. There are three tracks in the literature that achieve SMC, each with its own large community: Secret Sharing (SS) [33], Garbled Circuits (GC) [34] and Homomorphic Encryption (HE) [22]. SS-based techniques show very promising performance, and are seeing some commercial use [35]. However, they typically require a set of non-colluding servers, which makes it unsuitable when the goal is to not put any trust in the service provider(s). Techniques based on GC have seen promising performance utilizing the Intel Advanced Encryption Standard Instructions through protocols tailored for this particular instruction set. As most mobile devices use ARM processors, it is unlikely that the performance results can be extrapolated to mobile devices. Further, GC offers a one-off solution, where any results (except the output) should not be reused in further computations.

As previously detailed, homomorphic encryption makes it possible to perform mathematical operations on encrypted data. The ground-breaking result by Gentry [23] presented the first Fully Homomorphic Encryption (FHE) scheme, which is capable of computing arbitrary arithmetic formulas. Following Gentry's work, there have been numerous improvements for FHE [36], [37], [38]. However, so far there is no FHE scheme that is comparable in efficiency to schemes that are just additive or multiplicative. There have been many works that utilize homomorphic encryption to create privacy-preserving protocols in areas such as location-privacy and biometric authentication [20], [13], [19], [21], [14].

2) **Privacy-Preservation in LBS**: Puttaswamy et al. [39] present a new technique for location privacy by coordinate system transformations, called LocX. Each user has a secret for which its coordinate system is translated, and a set of friends. The secrets are distributed to each user's friends, such that only the user's friends may understand how coordinates are mapped. A prototype has been developed and it showed that it can be used in commercial applications with minimum overhead. However, unlike other protocols mentioned in this section, the user's exact location is revealed to all users with the secret, which forces the users to limit their social circle to users they trust with their location.

Further, to generate dummy data and present this to the LBS is a viable option to hide the user's location. Zhou et al. [40] propose a system called TISSA. TISSA allows users to choose what data an application can access. In case an application demands access to data that the user is unwilling to provide, the system sends dummy data as substitute, keeping the real data private. The system was tested in Android OS and successfully prevented leakage of information to restricted applications and caused no significant slowdown to performance of the phone. However, using only dummy inevitably prevents the application from functioning properly. Kido et al. [41] propose a system which sends

LBS provider's real user data as mixed with dummy data. As the LBS providers cannot distinguish between real and fake data, the anonymity of the user is preserved. However, the solution causes large communication overhead as all users need to send many additional messages with dummy data for each real query.

There are not many works that provide an in-depth discussion of PPLP on Mobile Devices. Narayanan et al. [12]

provides use cases where LBS mobile applications could be used and how their proposed protocol would relate to such applications. However, it is debatable whether the use cases themselves are realistic examples of LBS use and sufficient proof that the protocol could be applicable enough to be used in general applications.

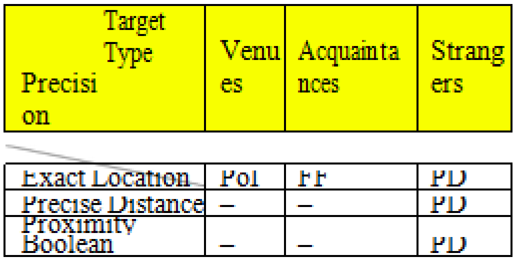
IV. PROPOSAL WORK

The applicability of privacy-preserving proximity-testing protocols to real-world LBS. First, a new set of features for LBS is outlined. These features can be used to assign LBS into a category. A privacy-preserving protocol is able to serve a fixed set of categories.

A. LBS Features and Categories

We identify features and categories to aid the applicability analysis of privacy-preserving protocols for LBS. First, mobile LBS applications vary based on whose location information they provide to the user, herein called the target type feature: venues, acquaintances, and strangers. Second, the applications also vary based on the precision of the location information provided, called the precision feature: exact location, precise distance, or a Boolean proximity result. Using these application features we will determine to what extent a given privacy-preserving mechanism is applicable to each application.

Table I CATEGORIZATIONS FOR LOCATION-BASED SERVICES



Target Type Precision	Venues	Acquaintances	Strangers
Exact Location	PoI	FF	PD
Precise Distance	–	–	PD
Proximity Boolean	–	–	PD

Important to note about the venue target type is that in most cases, a venue’s location is normally not secret. Thus, for most common applications, there is little to gain by using privacy-preserving protocols towards a venue, as in this case the instigator can be told the venue’s coordinates and then run all computations locally. Although there is no need for a privacy-preserving protocol to handle the venue’s position in this case, the privacy of the requester’s location needs to be protected by the implementation as to prevent location leaks to internal attackers such as via the IP address.

We define three app categories: Point-of-Interest based (PoI), Friend-Finding (FF), and People-Discovery (PD) apps. PoI apps are common venue-locator applications, e.g. where people wish to meet each other or find a shop of some kind. Friend-Finding apps are for keeping track of the whereabouts of close friends and family. People-Discovery apps are for locating new people to interact with.

Table I reflects what kinds of applications belong to which category. As expected, the PoI applications disclose the precise location of the venue. This is also the case for Friend-Finding applications, though one could imagine scenarios where users would not want their precise location known even to friends and family, e.g. when buying a gift. Surprisingly, many applications that facilitate interaction between strangers also disclose the exact location of the users to each other.

For any privacy-preserving proximity-testing protocol to be adopted, the application must have proximity precision. Further, it cannot be a venue target type, as then the location can be publicized instead. The services which could most easily adopt privacy-enhancing technologies are thus the Friend-Finding and People-Discovery, both with proximity precision. However, some applications might in their current state reveal more location information than strictly necessary. As such, applicability of a privacy-preserving protocol is grouped into three classes:

Not Applicable: the mechanism sets overly strict limits on the information disclosure to support the features of the application.

Partly applicable: to incorporate the mechanism the application would require minor modifications to its features but would still be able to maintain its core purpose.

Applicable: the mechanism can be incorporated into the mobile application without hampering the functionality of the mobile application.

A CONCRETE PPLP PROTOCOL

Hitherto, we have only touched upon PPLP protocols in general; the enforcement of such is discussed in this section. There are many published works describing how to accomplish different flavors of PPLP [14], [15], [16], [17], [18], [12], [13], and [19]. In this work, Inner Circle by AnonymousAthors [19] was implemented to evaluate efficiency of a recent PPLP protocol on a Smartphone device. Inner Circle is a good representative of state-of-the-art PPLPs as it provides protection against internal attackers while disclosing only location proximity, which is a good countermeasure against external attackers. Further, the authors provide evidence that the protocol could be efficient enough for usage in Smartphone applications. Other protocols, such as the work by Sedenka et al. [13] provides the same security guarantees, but requires the use of multiple cryptographic schemes and has several additional round-trips between the parties as compared to Inner Circle. Reducing the number of round-trips proved a good choice, as this can cause a blow-up in communication, as seen in Section IV.

The mobile application produced in this work uses the Inner Circle protocol [19]. This particular protocol was chosen as it preserves location privacy against both internal and external attackers, while completing in a single round-trip. The key concept used in Inner Circle is, as mentioned previously, homomorphic encryption, which avoids the need for TTP. In recent years homomorphic encryption has became a popular choice for creating privacy preserving protocols and as such, it is a good representation of much of the state-of-The-art technology in location-privacy.

The protocol considers two principals, Alice and Bob, where Alice is the instigator. When Alice wants to query Bob to check if they are in each other's proximity, Alice constructs a location request. The location request encapsulates Alice's coordinates, encrypted under her public key. Bob uses the information in the location request together with his own coordinates to create a location response. A location response is an array which encodes a single Boolean value, which can be decoded using Alice's private key. For the full protocol, the reader is referred to the original paper [19]. For the scope of this work, it suffices to view the protocol as consisting of three steps: request construction, response construction to encode the Boolean result, and response interpretation to decode the Boolean. The encoding step which constructs the lesser than comparison is henceforth referred to as less Than(), while the decoding step where Alice finds out whether Bob is in her proximity is called import(). As shown in Section V, the less than () and import () methods are the more time-consuming operations in the protocol.

The key concept used in Inner Circle is, as mentioned previously, homomorphic encryption, which avoids the need for TTP and in recent years has became a popular choice for creating privacy preserving protocols [14], [20], [21], [13], [19]. Homomorphic encryption allows for computations to be evaluated on encrypted data. Formally, given the plaintext space M and tcipher textext space of a homomorphic scheme C such that encryption is a function E: M! C and decryption is D: C! M, for any arithmetic formula

f : M^k! M^k it is possible to construct g: C^k! C^k such
! !

That D (g (E (m))) = f (m). I.e., for any arithmetic formula in the plain it is possible to construct another formula to compute the same in the cipher texts. There are several flavors of homomorphic encryption. Normally homomorphic encryption signifies Fully Homomorphic Encryption (FHE) schemes [22], [23]. FHE schemes are extremely powerful, and can evaluate any formula as described above, but are rather inefficient. On the other hand, there are schemes that are more limited in what they can compute – such as Additively Homomorphic Encryption (AHE) – but which are far more efficient [24]. The Authors Of [19] present several cryptosystems which can be used to instantiate Inner Circle. In this research we have chosen to use the ElGamal's [25] encryption system using 1024 bit keys since it had a notably fast performance in the original implementation.

Of interest is also how an array is used in Inner Circle to encode a Boolean. Of course, using an array requires much more communication, memory and computational resources. However, due to the limitations of AHE, the authors of Inner Circle found this the most efficient approach. In essence, the array a is the result of a less-than operation. To check if $x < y$, one can check if $9y_i < y : x\ y_i = 0$. The protocol creates the array such that it contains only uniformly random numbers, except for the case when $x < y$, when it contains a single (random) slot which contains the encryption of 0. The decoding step is thus to decrypt the array and check for the existence of a zero. Further, as square roots can not be computed using homomorphic encryption, the square of the distance between Alice and Bob is compared to the square of the radius, which yields an array which is quadratic in r.

V. CONCLUSION

This study furthers the data of however well current crypto logic privacy-preserving protocols apply to real-world mobile apps. To the current finish, we've road-mapped common location-based social maps and known eventualities wherever privacy-preserving location proximity is desired. The class of People-Discovery apps seems to be a particularly promising match. we tend to conclude that the protocol is productively applied to variety of common applications, specifically for those that facilitate conferences in real world between strangers, like meet-up and geological dating apps.

Further, we've enforced Inner Circle, the progressive privacy-preserving location proximity protocol and integrated it in an automaton app. With relevancy performance, we tend to attain the conclusion that Inner Circle on automaton matches real applications at radius values of twenty five and fifty units whereas values at seventy five units and on top of aren't nonetheless among a reach. The common network usage for twenty five units is 143 kilobyte and for one hundred units is 1740 kilobyte severally. With less precise coordinates the protocol will check the radius of one hundred kilometers, mistreatment twenty five unit radius in just four seconds that shows that the protocol is efficient enough for implementation in real applications.

REFERENCES

[1] AngelList, “Location based services startups,” Sep. 2014, https://angel:co/location-based-services.

[2] A. Lella, “Number of Mobile-Only Internet Users Now Exceeds Desktop-Only in the U.S.” https:// www:comscore:com/Insights/Blog/Number-of-Mobile-Only-Internet-Users-Now-Exceeds-Desktop-Only-in-the-U:S, Apr. 2015.

[3] K. Dreyer, “Mobile Internet Usage Skyrockets in Past 4 Years to Overtake Desktop as Most Used Digital Platform,” http://www:comscore:com/Insights/Blog/Mobile-Internet-Usage-Skyrockets-in-Past-4-Years-to-Overtake-Desktop-as-Most-Used-Digital-Platform, Apr. 2015.

[4] D. Coldewey, “”Girls Around Me” Creeper App Just Might Get People To Pay Attention To Privacy Settings,” http: //techcrunch:com/2012/03/30/girls-around-me-creeper-app-just-might-get-people-to-pay-attention-to-privacy-settings/, Mar. 2012.

[5] M. Veytsman, “How i was able to track the location of any tinder user,” http://blog:includesecurity:com/2014/02/how-i-was-able-to-track-location-of-any:html, Feb. 2014.

[6] C. Paton, “Grindr urges LGBT community to hide their identities as Egypt persecutes nation’s gay community,” http://www:independent:co:uk/news/world/africa/grindr-urges-lgbt-community-to-hide-their-identities-as-egypt-

[7] persecutes-nations-gay-community-9757652:html, Sep. 2014.

[8] C. Bessette, “Does Uber Even Deserve Our Trust?” http://www:forbes:com/sites/chanellebessette/2014/11/25/does-uber-even-deserve-our-trust/, Nov. 2014.

[9] J. Krumm, “A survey of computational location privacy,” Personal and Ubiquitous Computing, vol. 13, no. 6, 2009.

[10] M. Terrovitis, “Privacy preservation in the dissemination of location data,” SIGKDD Explorations, vol. 13, no. 1, 2011.

[11] E. Magkos, “Cryptographic approaches for privacy preservation in location-based services: A survey,” IJITSA, vol. 4, no. 2. [Online]. Available: http: //dx:doi:org/10:4018/jitsa:2011070104

[12] N. Talukder and S. I. Ahamed, “Preventing multi-query attack in location-based services,” in WISEC 2010. [Online]. Available: http://doi:acm:org/10:1145/1741866:1741873

[13] A. Narayanan, N. Thiagarajan, M. Lakhani, M. Hamburg, and D. Boneh, “Location privacy via private proximity testing,” in Proceedings of the Network and Distributed System Security Symposium, NDSS 2011. [Online]. Available: http://www:isoc:org/isoc/conferences/ndss/11/pdf/1 3:pdf

[14] J. Sedenka and P. Gasti, “Privacy-preserving distance computation and proximity testing on earth, done right,” in ASIA CCS ’14, Kyoto, Japan - June 03 - 06, 2014. [Online]. Available: http://doi:acm:org/10:1145/2590296:2590307

[15] G. Zhong, I. Goldberg, and U. Hengartner, “Louis, lester and pierre: Three protocols for location privacy,” in Privacy Enhancing Technologies, 7th International Symposium, PET 2007. [Online]. Available: http://dx:doi:org/10:1007/978-3-540-75551-7 5

[16] L. Siksnys, J. R. Thomsen, S. Saltenis, M. L. Yiu, and O. Andersen, “A location privacy aware friend locator,” in Advances in Spatial and Temporal Databases, 11th International Symposium, SSTD 2009. [Online]. Available: http://dx:doi:org/10:1007/978-3-642-02982-0 29

[17] L. Siksnys, J. R. Thomsen, S. Saltenis, and M. L. Yiu, “Private and flexible proximity detection in mobile social networks,” in Eleventh International Conference on Mobile Data Management, MDM 2010. [Online]. Available: http://dx:doi:org/10:1109/MDM: