LocPriS: A Security and Privacy Preserving Location Based Services Development Framework

Gareth Ayres and Rashid Mehmood

School of Engineering, Swansea University, Swansea, SA2 8PP, UK
{g.j.ayres, r.mehmood}@Swansea.ac.uk

Abstract. With the ever increasing pervasiveness of devices with functionality to provide location based services comes the increased importance and reliance upon those services to provide user privacy and security. Many techniques to facilitate privacy and security in mobile and fixed networks have been developed, but surveys of user's show that this area still has a lot of work left to do to satisfy privacy fears and help developers of such services to choose the best techniques to use. In this paper we propose a security and privacy preserving location based services development framework. The framework will allow for future development, visualisation, comparison and analysis of location based services that preserve security and privacy in order to improve user confidence in such technologies.

Keywords: Location Based Service; Privacy; Security; Mobility; Visualisation; Wireless Networks.

1 Introduction

The recent explosion in popularity of mobile devices such as the Apple iPhone and Google Andriod phones has accelerated the use and deployment of Location Based Services (LBS). Such services are keen to help users make use of their location and mobility data in order to enhance or provide functionality. However, this functionality can sometimes come at the cost of privacy.

While LBS's are usually developed with security and privacy measures in mind, these are not always sufficient. Many LBS's come with the ability to turn location tracking on/off, while some come with only assurances of privacy with little or no technical explanation or justification of how privacy is achieved, or to what degree. The level of granularity of location data relative to the level of granularity required for a service to be functional is often never expressed or made transparent enough to users. Previous surveys of the value of location privacy to users have revealed the importance of privacy with regard to location, which is discussed further in this paper along with the result of a local study of user opinions.

Keeping the importance of location privacy and the security of techniques used in mind we have identified the need for a framework to help develop, visualise, test, compare and analyse existing and new ways of preserving location privacy and security in LBS's.

We propose a modular framework that will attempt to address these issues and provide an open source solution to help future researchers as well as developers and users of LBS's.

The remainder of this paper is broken down as such: Section 2 covers background material on LBS's and location privacy techniques. Section 3 provides an overview of related works in the area of network and mobility simulators and frameworks, and. discuses some previous studies of user's opinions on location privacy. Section 4 shows the results of a survey of 502 users carried out at Swansea University and the results discovered. Section 5 introduces our proposed LocPriS framework and its modular architecture while Section 6 will conclude the paper and highlight the future direction of our work.

2 Background Material

2.1 Origins of LBS

One of, if not the first, LBS's to be developed was the E911 system developed by Telecom operators in the early 1970's in collaboration with the US Governments Federal Communications Commission. These telephone systems allowed emergency calls made in some states in the United States to be routed to the appropriate emergency services call room. This is a simple example of a LBS with low granularity of location data, but later this service was enhanced to comply with additional regulations and new technologies such as mobile phones. This resulted in improved granularity of the location data as well as the better functionality of the service by displaying the data on maps [1].

Some of the first LBS's to be developed separately from the E911 system were developed under the vision of context-aware computing by Olivetti Research Ltd. ORL developed a LBS in 1992 that made use of the Active Badge system to inform receptionists where to forward phone calls too. This allowed receptionists to forward calls to the nearest phone to the recipient [2].

The development of the Active Badge system in Cambridge led to an increase in research in LBS's that made use of indoor localisation systems and users wearing a small localisation device. The next major development in indoor localisation did not appear until 1999 when AT&T developed the Active Bat system. Soon after in 2000 the cricket system [3] was also developed with much success.

With significant research in localisation techniques and other issues relevant to LBS's focusing on indoor systems throughout the 1990's until early 2000 the next wave of research was kick started by Microsoft with a paper they published called RADAR [4], which details a number of methods of performing localisation through wireless LAN's. This paper claimed the use of WLANS can provide localisation with an accuracy of 2-3 meters using existing 802.11 equipment.

The direction of research began to shift during the early 2000's from using indoor location tags to existing infrastructure to provide LBS's. The increase in popularity of

GPS during this time as a result of the increase in its accuracy to 20meters from 100meters in 2000 also helped change the direction of research.

In 2005 the combination of the increase in availability of mobile phones with built in GPS, 3G networks and the arrival of Web 2.0 technologies resulted in a revival of LBS research and development. The combination of mobile phones that were location aware through WiFi signatures and AGPS, social networking sites booming and online GIS mapping systems has resulted in a surge of activity in the area of LBS's.

2.2 Location Privacy and Security

Most users of networks in large institutions such as Universities are happy to use computers to browse the internet and communicate with friends and colleagues without considering how private that activity is. They are likely unaware that their internet browsing activity maybe being logged and the chat communications is being sent unencrypted and open to interception by network administrators or other agencies or hackers.

A side effect of the functionality of some LBS's is that users become consciously aware of the fact that their location data is what drives the service and that data is being controlled by a computer somewhere.

Privacy is considered a fundamental human right by the Universal Declaration of Human Rights and most democracies around the world [5] and the security of location data and users privacy must be taken seriously.

One of the first considerations is the granularity of the location data. The granularity of meters could provide more information about a user than the granularity of kilometres [6], depending upon the context of the service. Granularity alone does not provide any real privacy, and is vulnerable to correlation attacks as well as inference and assumptions attacks based on historical data.

The fundamental problems of location data storage and visualisation can be addressed by annonymising the data using pseudonyms. Pseudonymity provides anonymity to location data while maintaining a relationship between the data that is used to help the LBS function. Recording a pseudonym and location as a location data record allows for the movement of a node to be tracked while removing any identifiable data from the record [7]. This adds a level of security to the system that would protect a user if the data was stolen or misused. However it does not offer complete privacy as a user's identity could still be inferred from the history of a nodes movement in some cases.

One solution to this problem is the addition of dummy nodes. Dummy nodes add a level of 'noise' to the LBS that does not affect the quality of the service but helps remove the ability of a possible attacker to infer the identity of a node based on the history of a nodes movements [8, 9]. Other possible solutions to this problem are temporal and special cloaking along with silent periods [9].

Another possible technique to add privacy is the use of mix zones. Mix zones provide a trusted middleware that provides anonymised location information to third-party applications by defining spatiotemporal zones where all users in that zone have

their pseudonyms changed upon entering and leaving, therefore providing a new set of anonymity [10].

Configurable privacy preferences have also become common techniques used to provide privacy in LBS's, giving users the ability to control the volume, granularity or accuracy of location data they reveal.

3 Related Works

There exist a number of simulation and visualisation tools, with different objectives, which come close to meeting some of the objectives of our framework. The tools, simulators and frameworks surveyed can be broken down into two distinctive areas, network simulation and mobility visualisation tools.

3.1 Network Simulations

There are a number of established simulation tools available which address the problem of network/ wireless network simulation. Many of the simulation tools provide the ability to develop other tools built upon them and could be used to fulfil part of the needs of the simulation module of our framework.

There are commercial as well as open source simulators, all with different qualities. One popular open source simulator is NS-2 which is a discrete event based simulator that is very popular in academia for network simulation. NS-2 does not cater well for mobility modelling on its own, and has little in the way of visualisation functionality. There have been developments which attempt to add these features to NS-2, such as iNSpect.

GloMoSim (Global Mobile Information System Simulator) is a network protocol simulation tool that simulates wireless and wired network systems. It is designed using the parallel discrete event simulation capability provided by Parsec. QualNet is a commercial network simulator with many libraries and components. It supports visualization of simulations, and has support for some mobility patterns.

SWANS is a scalable wireless network simulator built on the parallel discrete event based java JiST platform. It makes use of virtual machines to improve speed of simulation. The Georgia Tech Network Simulator (GTNets) also provides limited support for mobility and provides particular attention to protocol simulation and analysis.

3.2 Mobility Visualisation Tools

While most network simulators have added functionality to allow wireless network simulation, some have also added mobility simulation. Mobility simulation is useful for wireless networks of many types, including WLAN, adhoc and sensor networks. A detailed survey paper on the area of mobile area network simulation is [11].

There are a number of mobility simulation tools such as Mobitools, MobiREAL

and MoViTo which all aim to simulate mobility in mobile area networks through the use of mobility patterns. Many have functionality for Vehicular mobility simulation, such as Mobitools, while some aim more at human mobility using probalistic rule-based models such a MobiREAL. Some simulators make use of virtual environments while some make use of GIS systems. Most tools make use of 2D while some also make use of 3D such as ViTaN.

3.3 The Value of Location Privacy

While it is mostly accepted amongst researchers that privacy needs to be built into future technologies regardless of some user's value of it, a number of studies of user opinions on the value of location privacy have been performed. Cambridge University run a survey of their computer science undergraduate students to try to measure the monetary value students place on their location information. The survey was in the form of questions and an auction to determine the value students place on their location data. 74 students filled in the questionnaire.

The results show that students valued their privacy at a median bid of £10. They then doubled that when commercial interest was mentioned. It also showed that students who travelled outside of Cambridge valued their privacy more than those who did not travel far [12].

One of the authors of the Cambridge survey went on to question a sample of over 1200 people from five EU Countries. This also followed the form of an auction to determine the value placed on a month's location data. The survey produced a median value of £20 for a month's location data, but did not find the same correlation between users who travel more and location data value [13].

A survey on location privacy and social networks has been carried out by Intel Research which provided PDA's to 16 non-technical participants in order to retrieve information on how the participants value location privacy when disclosing information to friends, family and colleagues [14].

The Westin/Harris Privacy Segmentation Model was used to classify participant's privacy. The paper found that people were fairly specific about their location 77% of the time. Who was requesting the information had the strongest influence on the participants willingness to disclose. Why a request for information was made was also an important influence. Participants also provided more granular location information to people who were relatively close to them.

Another survey used two distinct types of location data in order to access which is a greater privacy concern in relation to location based services. Location-tracking and position aware location data. The authors claim that users are more concerned by location tracking data than position aware data. They also claim that the sampled users were positive towards location based services as long as they perceive them to be useful [15] .

One survey studies the results from a questionnaire used to determine the importance of two factors – inquirers identity and the users situation at the time of inquiry. It is found that these two factors directly determine the accuracy of disclosed information [16].

4 LBS Privacy Questionnaire

An online questionnaire was sent via email to all users of the Swansea University Wireless Network on 18 March 2010 which ran for 2 weeks. The users of the wireless network consist of members of staff, students and some volunteers. The survey consisted of questions regarding the wireless network, but had a section on location based services and privacy. The questionnaire was anonymous and voluntary, with no incentive offered to participants. 502 people completed the questionnaire, but as answering each question was optional, there are different numbers of responses to some questions.

4.1 Questionnaire Results

There was a fairly even split between participants of the questionnaire on who had used a LBS and who has not. 43% (190) had not, while 41% (181) said they had. Of the participants who had used a LBS, GPS directional assistance was the most popular service 30% (131) with mobile phone applications following with 27% (119).

When asked '*Is privacy an issue you would consider when using a Location Based Service*' the response was that 47% (203) said '*yes*' it was, with 35% (151) saying '*no*' it was not. When asked who they would be happy to share thier location data with (allowing for multiple choices), the response was unsuprising that family (66%) and friends (64%) was selcted most commonly with the extreme options of sharning with nobody (14%) and anybody (14%) being less popular.

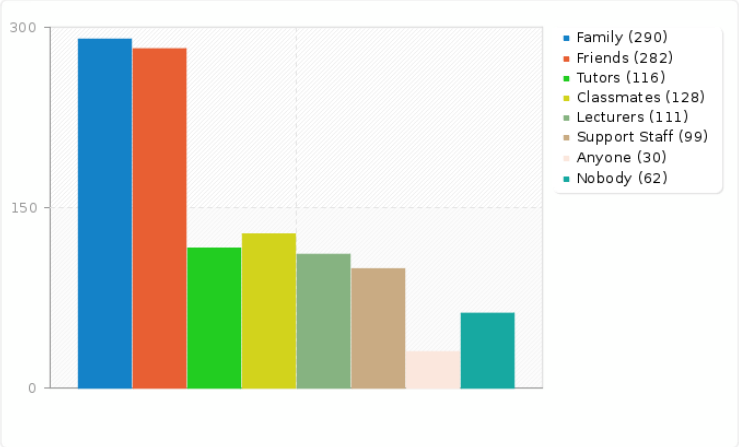

Fig 1 - Who would you share location information with?

Interestingly, when asked '*If technology could guarantee the privacy of your location, would this encourage you to use a Location Based Service?*' the response was that 63% (277) of participants felt it would encourage them with only 9% (40) saying it would not.

5 LocPriS Framework

We propose a modular extensible framework that will provide tools for the development, analysis, comparison and visualisation of LBS's that preserve privacy and security. The framework will also assist in the development and testing of Location Based Services through an exposed API.

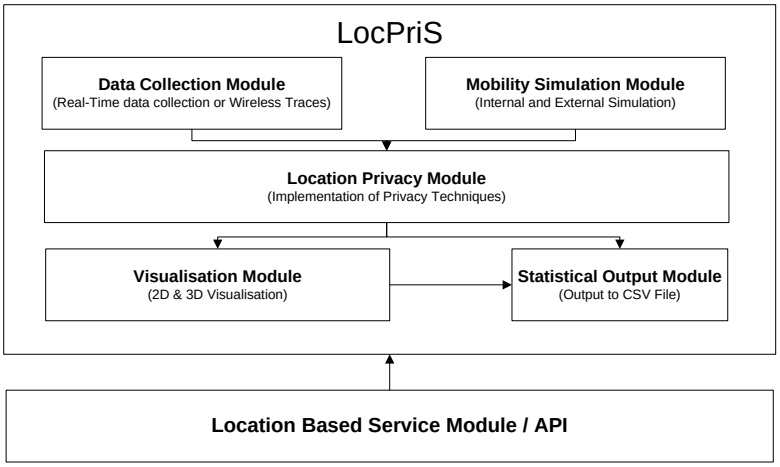

Fig 2 - The modular design of the LocPriS Framework

5.1 LocPriS: Data Collection Module

The Data Collection Module will provide for two main inputs of data:

- **Wireless traces** – Wireless traces are available from a number of archives and institutions, including Dartmouth (Crawdad) and USC. These archives are of different sizes, and do not all contain location linking data, but through linking techniques can used.
- **Real-time data –** Data from the Swansea University wireless network is being recorded in real time through the use of a SNMP traps and custom java/PHP programs. See figure 3 for a system design diagram.

5.2 LocPriS: Mobility Simulation Module

Although the use of real data will be beneficial, the use of simulated mobility data will allow for additional testing and comparison. There are a number of mobility simulators that simulate models such as the random waypoint and walk models which could be used as a single source of data or in conjunction with the implementation or other mobility models in the framework.

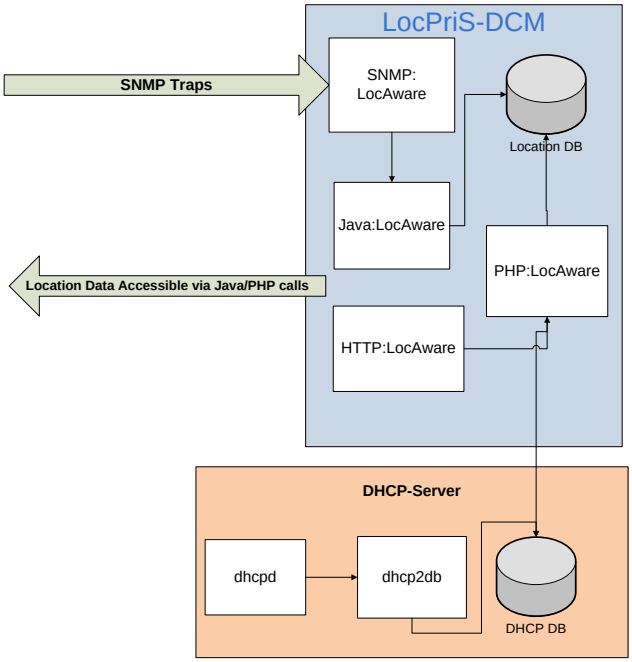

Fig 3 - LocPriS Data Collection Module

5.3 LocPriS: Visualisation Module

Through the use of Java, OpenGL and the Java Monkey Engine it is possible to visualise mobility in 2D or 3D. Visualisation of mobility and then the visualisation of the application of privacy and security techniques will allow for contrasting views of some of the strengths, weaknesses and characteristics of differing techniques. This will aid designers of LBS's as well as users who wish to quickly see the implications of using LBS's.

Through the use of open mapping data it will also be possible to overlay graphical maps on to 2d visualisations as well as allowing for the importing of user designed floor maps and layouts. See figure 4 for a screen shot of the visualisation module.

5.4 LocPriS: Location Privacy Module

As described in the previous sections, there have been a number of privacy and security techniques developed to improve privacy and provide security in LBS's. These techniques will be implemented in this module so they can be applied to sets of location/mobility data. This module will also allow for the development of new novel techniques.

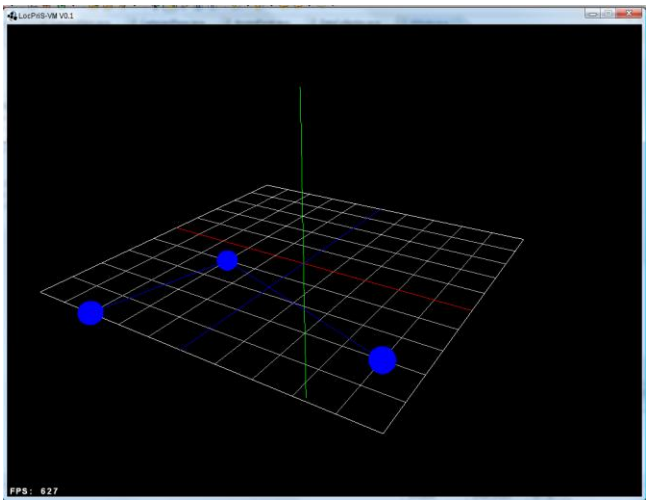

Fig 4 - LocPriS Visualisation Module

5.6 LocPriS: Statistical Output Module

The result of visualisation and application of privacy and security techniques will produce statistical output. This will mainly consist of numerical representation of node locations and movements. This data will be outputted in a CSV file for easy analysis.

5.5 LocPriS: Location Based Services

Through the use of an exposed API it will be possible to develop, test and analyse privacy techniques as well as new services through the use of the LocPriS framework. As has been shown [17], security can be considered a LBS and can be built as a service on the LocPriS framework.

6 Conclusion

Location based services have come a long way since the early inceptions by researchers and service providers, along with significant developments in privacy and security techniques to complement them. While these techniques are bringing some confidence and assurances to users, results from our and other user surveys and questionnaires have shown that there is still work to be done to provide greater privacy and security, and to build the trust of users of LBS's through continued transparency of the application and functionality of such techniques.

User surveys along with the continued growth of the number of devices with LBS functionality have shown that demand for such services is substantial and growing. It is important that the growth of privacy techniques follow this trend to keep up with such growth in order to ensure the continued trust of users in new and exciting technologies.

In this paper we have outlined a framework we believe will help to enhance the development of LBS's that preserve privacy and security. Development of the framework is still in the early stages, with work left to do on each of the modules. The continued development of the framework will result in the production of results from analysis and comparison of privacy and security techniques along with the possibility of development of new techniques and LBS's.

References

1. Woody, L.A., Acker, L., Curran, W., Susi, S., Velazquez, M.: The Impact of the FCC's Position on Wireless E911.
2. Hightower, J., Borriello, G.: A Survey and Taxonomy of Location Systems for Ubiquitous Computing. (2001) 57--66
3. Priyantha, N.B., Chakraborty, A., Balakrishnan, H.: The Cricket location-support system. Mobile computing and networking. ACM, Boston, Massachusetts, United States (2000)
4. Bahl, P., Padmanabhan, V.N.: RADAR: an in-building RF-based user location and tracking system. (2000)
5. Nations, U.: Universal Declaration of Human Rights, General Assembly Resolution 217 A (III),. (1948)
6. Grlach, A., Heinemann, A., Terpstra, W.W.: Survey on location privacy in pervasive computing. Privacy, Security and Trust within the Context of Pervasive Computing. (2004)
7. Chaum, D.: Untraceable electronic mail, return addresses, and digital pseudonyms. Communications of the ACM (1981) 84--88
8. Report, F.: Surviving the privacy revolution.: Deering, S., ICMP Router Discovery Messages, RFC 1256 (2002)
9. Gruteser, M., Grunwald, D.: Anonymous Usage of Location-Based Services Through Spatial and Temporal Cloaking. Mobile systems, applications and services. ACM (2003)
10. Alastair R. Beresford and Frank Stajano, *U.o.C.*: Location Privacy in Pervasive Computing. Pervasive Computing, IEEE (2003) 10
11. S. Kurkowski, T.C., and M. Colagrosso: MANET simulation studies: the incredibles. Vol. vol. 9. SIGMOBILE Mob. Comput. Commun (2005) pp. 50-61
12. Danezis, G., Lewis, S., Anderson, R.: How much is location privacy worth. (2005)
13. Dan, C., George, D.: A Study on The Value of Location Privacy. Privacy in the Electronic Society. 2006, ACM 109--118
14. Consolvo, S., Smith, I.E., Matthews, T., LaMarca, A., Tabert, J., Powledge, P.: Location disclosure to social relations: why, when, & what people want to share. Proceedings of the SIGCHI. ACM (2005) 81-90
15. Barkhuus, L., Dey, A.: Location-Based Services for Mobile Telephony: a study of users' privacy concerns. Proceedings of the 9th IFIP TC13 (2003) 712, 709
16. Lederer, S., Mankoff, J., Dey, A.K.: Who wants to know what when? privacy preference determinants in ubiquitous computing. CHI '03. ACM (2003) 724-725
17. Localization to Enhance Security and Services in Wi-Fi Networks under Privacy Constraints. In Communications Infrastructure. Systems and Applications in Europe, Vol. 16. LNICST (December 2009) pp175-188