Improvement techniques over Location privacy

Longjam Velentina
Student Mtech CSE
Integral University

Prof Rizwan Beg
Professor
Integral University

Dhrub Shankar Ray
Assistant Professor CSE dept
Integral University

Abstract:

Over the past years pervasive computing has gained a significant progress. At the same time, maintaining location privacy is also one of the most challenging issues in the pervasive environment. So here in this paper we proposed an improvement technique using the concept of layered proxies for privacy over the already existing techniques like temporary pseudonyms, dummy locations, and trusted proxies. Also we have highlighted some limitations of the previous method.

Keywords: Location Privacy, Prevasive computing, temporary pseudonyms, dummy, Location anonymization.

I. Introduction:

According to the universal declaration of human rights [1] everyone has the right to privacy, over many years computer security researchers developed a number of sophisticated "privacy enhancing technologies (PET)" to minimize the personal data leaked by everyday online interaction. Our work follows to the protection of privacy, preventing other parties form learning ones current or the past location based on the frequent change of pseudonyms and the trusted proxies. However today's location aware services like GPS, Friends Finder, wireless technology embedded watch. All these application reached into deep into the private sphere of one's life.

II. Location Privacy:

Location privacy is the ability to prevent others from learning one's current and the past location [2]. Also a system that can obtain the position data can invades location privacy.

Location Based Services:

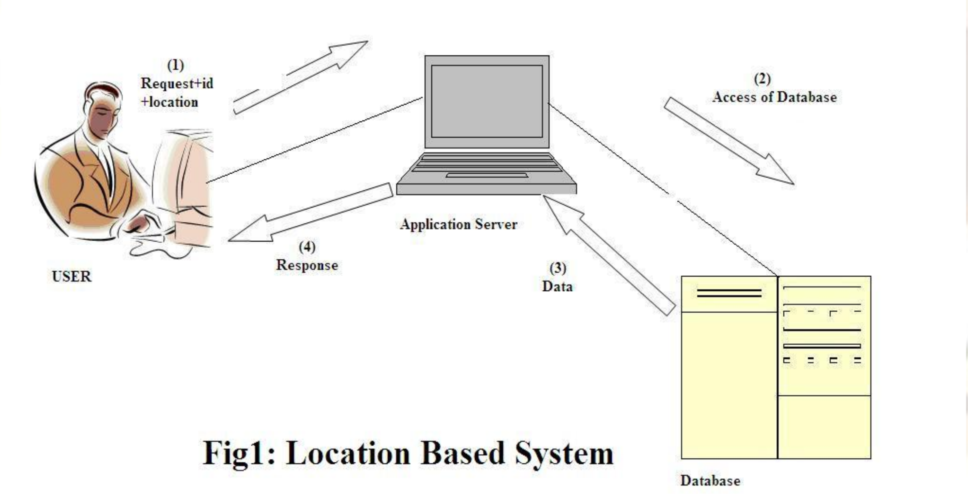

Fig1: Location Based System

Fig 1 shows location based services and it exploits knowledge about where the users are located.

1. The user sends the service request with its ID and the position data to the service provider.
2. The service provider accesses the database and sends the response.
3. User receives the reply message.

In this paper we would like to create a module, in which user could avail "the location based services (LBS)" without revealing the correct id and the actual position of the user. So location privacy in such services or the application most challenging factor is that user could avail the services only when sending request comprises at least of the user-id and the true position data of the user.

III. Related works:

Researchers on privacy led to numerous solutions. Like targeting the location data and try to enhance user privacy by cloaking or blurring location information through reducing the resolution of provided data in terms of time and space.

1. The most interesting scenario for their location-based services privacy solution is the so called intermediary scenario [4]. Here, a location intermediary collects localisation information

from different sources, such as mobile operators or GPS coordinates that are sent by the clients directly. Thus, location intermediary acts as location broker for the application provider which offers some clear advantages such as unified access to different location sources, enhanced quality through correlation of multi-source location information, simplification of the process handling service providers and facilitation of user-to-user location-based services between different mobile operators. The user's privacy is protected by the use of distinct pseudonyms for mobile operator and application provider. The matching between different pseudonyms can only be performed by the location intermediary. However, the heavy use of asymmetric cryptography requires high computational effort, which might be awkward for low power mobile devices.

2. The user provides its location data together with a timestamp and the associated pseudonym to the location service [5]. A third party service provider cannot retrieve location data from the location service without knowledge of the used pseudonym. When a user wants to subscribe a service he has to disclose the pseudonym to the third party provider. By changing the used pseudonym a user can easily deny further access to his location once he has finalised service usage.

IV. Location privacy for the location aware applications:

Protecting the privacy user could use the benefits of location aware application services. Here user accesses the services of the application server through a middleware [2] e.i the trusted proxy.

Simple location privacy using trusted proxy:

Here user request id/ ticket from the trusted proxy for the communication with the application server and the proxy server send the id. So whenever user would be requiring for the services it will use this ID for the services.

1. User sends the request for the Id to the trusted proxy.
2. Trusted proxy reply with the Id to the user.
3. User sends the service request, location with its Id to the proxy server.
4. Proxy server send the service request with temporary pseudonyms to the application server
5. Application server will send back the responds to the proxy server.
6. Proxy server sends the response to the user referring the Id.

While in the other approach temporary pseudonyms is created using the cryptographic technique [6] for hiding the id of the user.

1. User will send the service request with dummy the locations [7] and temporary pseudonym to the trusted proxy.
2. Trusted proxy will forward the service request with the dummy location to the application server.
3. Application server will send the response to proxy server.
4. Proxy server will send back response to the user.

Counter measures in this model is using of only a single trusted proxy. It can easily leak the security of the location, if the proxy server is pressurized. Here are some of problem of using this model:

i) We need to ensure that the proxy server always remain a trusted, one sometime this is not possible.

ii) Single proxy server can be pressurized to give the identity of the user.

V. Improvement over location privacy using layered proxies:

Here in our model we use layers of proxies more than 2. Each proxy server can create temporary pseudonym of own for each id send to it. Proxy server can keep on forwarding the pseudonyms along with the request and the dummy locations [7] to the next proxy server until request is received to the application server. Here too the user will send the request to the proxy server using temporary pseudonyms to the first trusted proxy and this proxy server will again act as a user to the next proxy server so the first proxy server will send request, along with pseudonyms coated /layered with the new pseudonyms created by the first proxy server. On receiving the request and the temporary pseudonyms the second proxy server will create a new pseudonyms layering over the old one. This process will keep on rolling until it reaches the application server. Application server on receiving the request it will send back the response to the proxy server from which it has received the request. Each proxy server keep on forwarding the response, after decoding the pseudonyms it has created while receiving the request.

Let us consider number of proxy server use is 3 and named it as Proxy1, Proxy2, Proxy3 and its corresponding pseudonyms P1, P2, P3.

1. User created pseudonym (P) and send the request along with the dummy locations and pseudonym (P) to the proxy server (Proxy1).
2. Proxy1 will again create pseudonyms (P1) over the received pseudonym forming layered pseudonyms. It will send the request

to Proxy2 along with the pseudonyms (P1) and the dummy locations.

3. Proxy2 create the pseudonyms (P2) over the received pseudonyms forming a coated/layered pseudonym. Proxy2 forward the request to Proxy3 with the pseudonym (P2) and dummy locations.
4. Proxy3 following the same procedure it send the request, pseudonym (P3), dummy locations to the application server.
5. Application server will send the response to the Proxy3 along with the pseudonym (P3) it received.
6. Proxy3 will decode the pseudonym it has created and send the response and Pseudonym (P2) back to Proxy2.
7. Proxy2 will decode the pseudonym (P2) it created and removed the layer it covered and the send the response along with P1.
8. Proxy1 will continue the same process send the request and P back to the user.

This technique provides a better secure procedure for those of unfaithful proxy server. In this model if one proxy is unfaith than it cannot break the security until all the other proxy servers are unfaith, which is quite difficult for an attacker to break it. Here we cannot fix the number of proxies but we can set it according to the privacy's priority of the user. If the privacy priority is very high number of proxy server must be increased ie Privacy priority is directly proportional to the No. Of proxy servers.

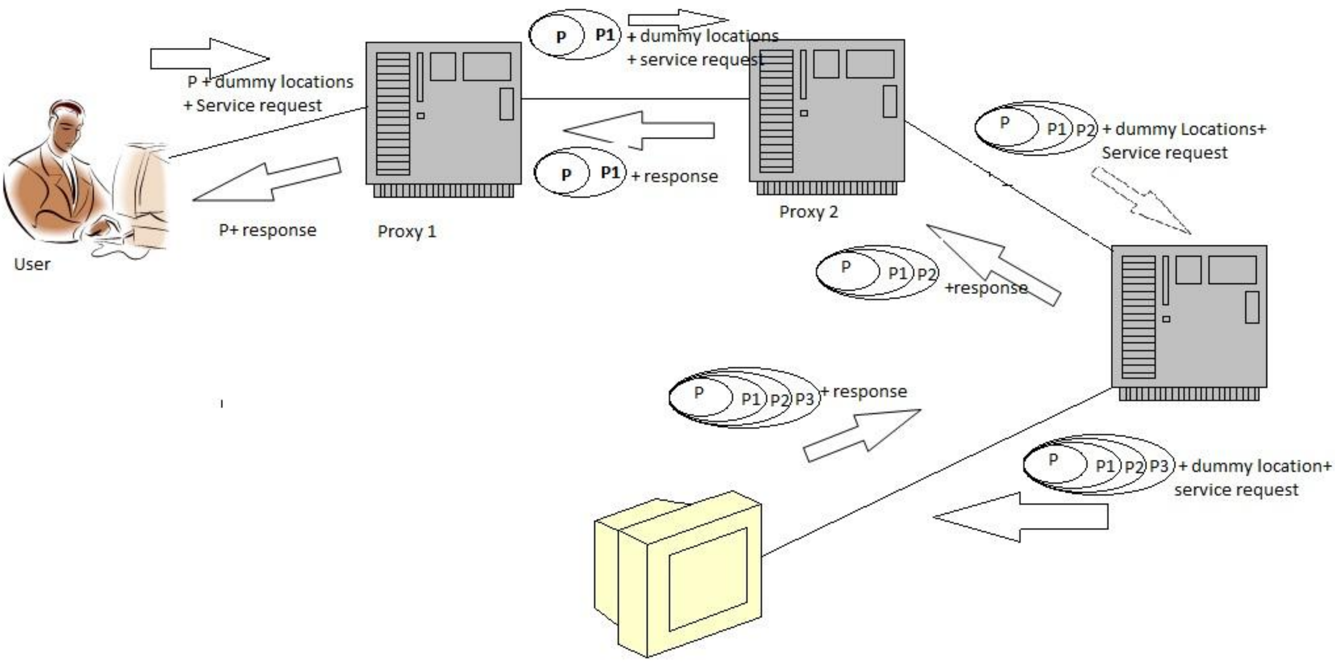

Fig: 2 Location privacy using layered proxies.

VI. Some of the improvements to be mentioned are:

1. A single unfaithful proxy server cannot harm the security of the location privacy.
2. Pressurizing a single proxy server cannot uncover the privacy as it would require pressurizing the entire proxy server included in the communication.

VII. Conclusion:

In our paper we presented a more secure model for location privacy using layers of proxy server making it more complex and secure while breaking the security about the location privacy. To break the security needs to decode the pseudonyms use in all the proxy servers. So the more is the number of proxy server the more is the complex for decoding.

VIII. References

[1] United Nation, Universal Declaration of human Rights, General Assembly Resolution 217 A (III), 1948; www.un.org/overview.

[2] A. R. Beresford and F. Stajano. Location privacy in pervasive computing. *IEEE Pervasive Computing*, 2(1):46–55, 2003

[3] H.kido,Y.Yanagisawa and T.Satoh. An Anonymous Communication Technique using Dummies for Location-based Services.

[4] K¨olsch T., Fritsch L., Hohlweiss M. & Kesdogan D.: Privacy for Profitable Location Based services, Proceedings of the 2nd Intl. Conference on Security in Pervasive Computing, Lecture Notes in Computer

Science (LNCS 3450, pp.164-179), Springer, Berlin, Germany, 2005

[5] Rodden, T., Friday, A., Muller, H. & Dix, A. (2003), A Lightweigth Approach to Managing Privacy in Location-Based Services, Technical Report Equator-02-058, University of Nottingham and Lancaster University and University of Bristol, 2002

[6] D. Chaum. "Blind Signatures for Untraceable Pay- ments." *Proc.* Crypt0 *'82*. 1982.

[7] Tun-Hao You, Wen-Chih Peng, Wang-Chien Lee, “Protecting Moving Trajectories with Dummies”, www.cs.nctu.edu.tw