2008

Cross Domain Privacy Protection for Location-Based Services

Oliver Jorns
Ftw. Telecommunications Research Center, jorns@ftw.at

Gerald Quirchmayr
University of Vienna/University of South Australia, gerald.quichmayr@univie.ac.at

Cross Domain Privacy Protection for Location-Based Services

Oliver Jorns
Ftw. Telecommunications Research Center
Donau-City Strasse 1, 1220 Vienna, Austria
Jorns@ftw.at

Gerald Quirchmayr
Institute of Distributed and Multimedia Systems,
University of Vienna, Liebiggasse 4/3-4,
1010 Vienna, Austria
Gerald.Quirchmayr@univie.ac.at

School of Computer and Information Science,
University of South Australia, SA-5001 Adelaide,
Australia
Gerald.Quirchmayr@unisa.edu.au

ABSTRACT

Network operators gradually open their interfaces to formerly hidden services that foster the development of a new class of mobile applications which are operated by 3rd party providers and take into account context information such as the user's location. As a result, the inclusion of the network operators' infrastructure provides many new possibilities and the potential to change the way in which mobile devices are used in everyday life. However, this development raises important issues such as the protection of the users location information and privacy while using location-based services. In this paper we illustrate a service architecture together with a novel and flexible privacy enhancing mechanism that allows the realization of the highly postulated pay-as-you-go model for location-based services. We further specify mobile applications that operate on the exchange of location information even between different network operators while still meeting mandatory legal requirements.

Keywords

privacy, pseudonyms, anonymity, location-based services, identity management, federation of network operators.

INTRODUCTION

While only a decade ago the focus of legislation was on the protection of privacy, it has over the past years dramatically shifted towards enabling law enforcement access to data collections and towards preventing violent and economic crime. Recently, the intensified public and scientific discussions worldwide, primarily those regarding the possible abuse of collected data, have led to a widespread loss of consumer trust in distributed IT systems that are vital for an effective law enforcement and for an efficient economy. Typically, these discussions revolve around the safeguarding of data in banking systems (The Financial Crime Branch - HM Treasury 2002; Lichtblau, 2006), airline passenger information systems (European Digital Rights, 2006) and international financial transaction systems, such as SWIFT (Federal Deposit Insurance Corporation (FDIC), 2007). While the collected information is important in certain contexts, it is also increasing the exposure of individuals to abuse. The widespread sloppyness in the handling of personal data by different industry sectors and by some government agencies in the US and Europe has increased the reluctance of consumers and citizens to provide any other information than what they are obliged to by law or the bare minimum required for a purchase or for access to a service. There even is a tendency to abandon the use of services that lead to the collection of larger amounts of personal data. At the same time compliance requirements on companies and government agencies are growing, resulting in a situation where they are caught in between the necessity to collect more and more data to fulfill these requirements and an increasing reluctance of consumers and citizens to provide personal information. A very typical representative of this increasingly problematic situation is the latest legislation which European mobile phone operators are currently confronted with. While it is highly desirable to better support law enforcement agencies in their efforts to prevent serious crime, the cost of the systems for businesses and the fears of consumers are steadily growing. It has in some cases reached a level at which consumers refuse new services out of fear the data possibly collected about them through the services might be open to abuse. As an abundance of cases has shown, this fear is not unjustified. With a steady stream of serious blunders being reported in the media, it is obvious that consumers and citizens are starting to distrust IT-based products and services. An uneasy feeling that has

previously been limited to the Internet is now mobile end user devices and navigation systems. The legal obligation to collect data and store it for a certain amount of time is reinforcing the already negative attitude of consumers and citizens.

The increasing legal and commercial pressure on operators

As mentioned in the introduction, one of the worst affected industry sectors are the providers of mobile services. The European Data Retention Directive (EU, 2006) does for example clearly state that Member States of the European Union are obliged to introduce legislation that forces service providers to retain highly personal data, such as the origin and the destination of all outgoing or incoming connections and their duration. With this information the complete communication profile of a person can be built, including all telephone and e-mail contacts. While this information is an extremely valuable base for law enforcement officers investigating criminal networks, it gives innocent users the feeling of their lives being monitored permanently. From the recording of connection headers (e.g. called numbers, email recipients, and server logins) and the duration of a phone call to the recording and analysis of the content of a communication it is only a small step. For service operators this means a twofold challenge, because they are being burdened with the collection, storage and making available of this information to law enforcement officers, while at the same time having to assure the safeguarding of this information against unauthorized access. Consequently, the already existing challenges of protecting personal data at the level prescribed by legislation such as the European Data Protection Directive (EU, 1995) are multiplied. Some of the nightmare scenarios for a mobile phone operator would be the unauthorized access to the collected data and the abuse of this data by own staff or by law enforcement officers who get authorized access.

The outcome is a double challenge: While the resulting investments in the affected mobile phone operators systems are considerable and do therefore increase the commercial pressure in an already highly competitive market, consumers do at the same time become reluctant to use new services out of fear that their personal data might be abuse. The way out of such a vicious situation can only come via an approach that enables the operator to fulfill the imposed legal requirements while at the same time providing a level of anonymity that makes the user feel safe enough.

Some of the major challenges an operator is confronted with and interesting questions an operator needs to answer are:

- Organizational challenges, conflicting goals in different areas of legislation, implementation cost, technological challenges.
- Analysis of and planning for expected and unexpected new legislation, implementation, operation of solutions.
    - Can and should a solid framework for dealing with the coming challenges be built?
    - Is an adequate process in place?
    - Requirements modeling, requirements tracking, development, implementation and operation.
- The need for appropriate organizational and technological solutions is quite obvious.
- Anonymity will soon be gone completely. Does *pseudonymity* help in the light of rapidly vanishing consumer trust?

As the full implementation of data retention legislation in Europe is not too far away, these questions need to be dealt with more urgently than some of the operators are aware of.

Interfaces towards 3rd Party Application Providers

One strategy network operators face to hold against the constantly growing market pressure is to provide interfaces to allow access to previously hidden services such as location, messaging or presence services to name only a few. To enable service providers to access network operators' services fosters the development of large-scale context-aware applications. The most prevailing subset of this kind of applications is also known as location-based services. They build the focus in this paper. Regarding open network interfaces, the standardization efforts of the Parlay (2008) group represent one example that aims to promote the use of network service operators' resources. However, interfaces that bring together the formerly separate telecommunications and Internet worlds also introduce new risks. Even worse, bringing together these two different worlds means that operators have to cope with a different scale of complexity and possible threats that multiply each other. As a result, these new kinds of threats are likely to be worse than if these domains remained separated. One decisive question that has to be considered is how to provide adequate privacy protection for users, the associated data and system components. In order to better understand the risks users and especially network service operators have to anticipate, we continue the discussion by illustrating the core privacy principles and concepts that are necessary for the sucessful realization and implementation of location-based services and applications.

Privacy Concepts

The notion of privacy is hard to define and there is probably no clear answer to the question what privacy actually is. Nevertheless, there are different definitions of privacy that reflect the different aspects such as the context and environment.

In this respect (Electronic Privacy Information Centre EPIC, 2008) mentions one writer's statement „*in one sense, all human rights are aspects of the right to privacy*". Meanwhile there are four different privacy concepts identified. These concepts are not self-contained but rather interrelated and include:

- *Information Privacy*: regards all means that are necessary to provide rules that govern the collection and handling of personal data also referred to as S*ensitive Personal Data* by the Data Protection Act (Parliament of the United Kingdom, 1998) and includes credit information, medical and government records as well as racial or ethnic origin, political opinions and religious believes to name only a few. The sum of all these rules and activities is also known as *Data Protection.*
- *Bodily Privacy*: concerns the protection of people's physical selves against invasive procedures such as genetic tests, drug testing and cavity searches
- *Privacy in Communication*: covers the security and privacy of mail, telephones, email and other forms of communications
- *Territorial Privacy*: concerns the setting of limits on intrusion into the domestic and other environments such as the workplace or public space. This includes searches, video surveillance and ID checks.

In the course of the discussion about privacy (Penders, 2004) excludes *Privacy of Communication* and *Bodily Privacy* from further discussion since his aim is rather to explain privacy in the light of (mobile) telecommunication services which reflects our aim quite well. Thus, we also exclude these two concepts from further discussions and concentrate rather on *Information Privacy*, which also covers the confidentiality of traffic data.

Beside the transmitted content data, communication in mobile networks also generates so-called traffic data that directs the content from a sender to the receiver and enables the communication. In telecommunication systems traffic data is also called signaling-data. It controls communications in telecommunication networks. This includes the establishment and control of a communication connection and the management thereof.

Another important aspect with respect to traffic data is location data. It represents indispensable information for the operation of today's mobile networks. Every mobile device that connects to a network first determines the base station of which the received signal strength is the best. If the holder of the mobile device moves it switches from one base station to another. This is called *handover*. Since every base station has a certain position, the location of each connected mobile device is known by the network operator. The location information is stored in a central database called *home location register* (HLR). The European Union defines location data as follows „location data means any data processed in an electronic communictions network, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communicaiton service." which describes the aforementioned technical aspects in telecommunications systems quite well.

PRIVACY RESEARCH FOR LOCATION-BASED SERVICES

Today, location information forms the basis for many commercial location-based services and applications. In the US market the driving force for this development was the E911 mandate. It obliges network operators to provide location information within certain time in case of emergency. Whereas the E911 finds general approval, most people are sceptical or even mistrust in technologies of commercial location-based services (Barkhuus and Day, 2003). However, studies show that some of the people who were initially concerned about revealing thir location may change their mind and finally reveal their location information to almost everyone (Barkhuus, 2004). It is obvious that in any case reasonable solutions are required to guarantee users that their location and real world identity are sufficiently protected, even if they are not aware of any possible threat. The implementation of privacy measures may also reduce costs through data reduction that in turn can be made visible to users and result in a higher loyalty of customers.

Research in the field of privacy for location-based services has originated a number of solutions that aim at giving users control over who they allow to receive their actual location information. A basic classification leads solutions such as those proposed by (Gruteser and Grunwald, 2003; Yee, 2005) with a focus on the definition, distribution and enforcement of privacy policies. Other solutions such as proposed by (Cheng, 2006) is based on the concept of k-anonymity and tries to enhance the users privacy by cloaking or blurring location information through reducing the resolution of provided data in space and time.

The solution we present in this paper is based on pseudonyms that veil the real identity of users towards service providers. In the following we continue with a discussion about pseudonyms, show how the pseudonym generation scheme works and explain how users may query the system by the use of pseudonyms. Furthermore, we demonstrate the exchange of sensitive location information over the boundaries of the network providers without privacy interferrence. These questions are currently one of the most challenging issues designers of location-based systems face. Finally, we give an overview about the current implementation of the system.

Protection of Real World Identities with Pseudonyms

Depending on the requested service by the users, we distinguish two kinds of pseudonyms. One identifies the user who is at the same time the requester, the second kind of pseudonyms is used to denote another person, those in the buddy list. Technically, both kinds of pseudonyms are equal.

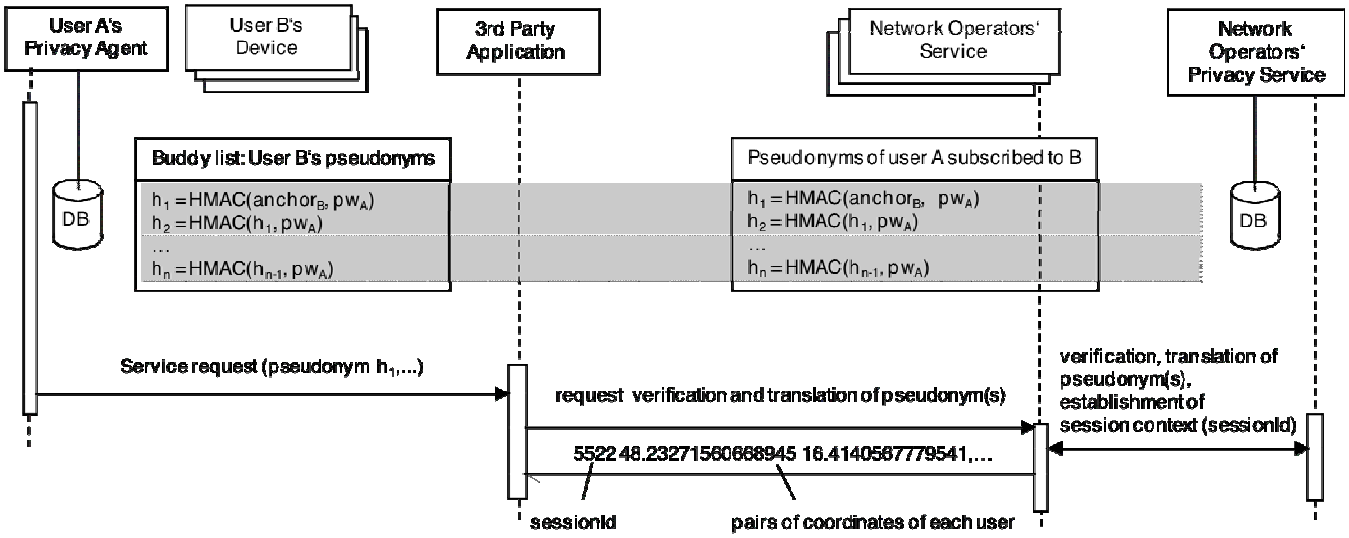

Figure 1. System Architecture and Pseudonym Generation Scheme

The use of pseudonyms allows abstracting from any information that could unveil the identity of a mobile user. However, this also imposes some requirements that have to be considered carefully. The most important one is that the use of static or long-term pseudonyms cannot provide sufficient privacy protection. In this respect, even if different static pseudonyms are used for different applications, it is still possible to unveil the respective identity of users (Beresford A.R. and Stajano F., 2003).

To provide sufficient privacy protection the use of changing pseudonyms is obligatory. Our scheme allows the generation of chains of pseudonyms. Each single pseudonym in a chain distinguishes from its successor and further from any other pseudonym generated by any other chain. Figure 1 shows two tables, one contains the chain of hash values that are generated by the client whereas the other table shows the correspoinding chain that is administered by the network operator's privacy service. For each request, the respective next pseudonym h_{n+1} is generated and sent to the application. The distinction whether the user sends a self-identifying pseudonym, only a single or a list of pseudonyms where each one denotes a particular buddy is, from the applications point of view, obsolete. From a technical point of view all pseudonyms are generated equally. The the application cannot deduce the underyilng real world identity from any received pseudonym.

In the example depicted in Figure 1, the user sends only one hash value h_1, which, in this case, denotes one certain buddy. Upon receipt the network operators' location service forwards the pseudonym to the privacy service which first checks the validity and then translates it. Therefore, the privacy service first looks in the database if it finds the received pseudonym. Each pseudonym is linked to one or several user identifiers. In the case when the location service sends the requests, the privacy service returns the associated MSISDN(s) of the particular user(s). Now, the privacy service computes the respective next pseudonym $h_2 = HMAC(h_1, pw_A)$ and stores it in the database.

For long-term localisaiton processes, the privacy service further creates and stores a sessionID. This is also stored by all the other involved services such as e.g. the location service and the application. It allows assigning incoming location updates to anonymized users. Finally, for long-term processes also the client receives the sessionID, which enables him to later terminate the process and prevent that they run forever.

Beside the capability to administer sessions, users can also send their location information directly to the location service. Therefore, the location service relates the MSISDNs with the actual position of the users. Apart from that, users initiate location updates in the same way as it is done for service requests, as part of message *updateLocation(.)*. For security reasons, pseudonyms that are identified as other than self-identifying are blocked.

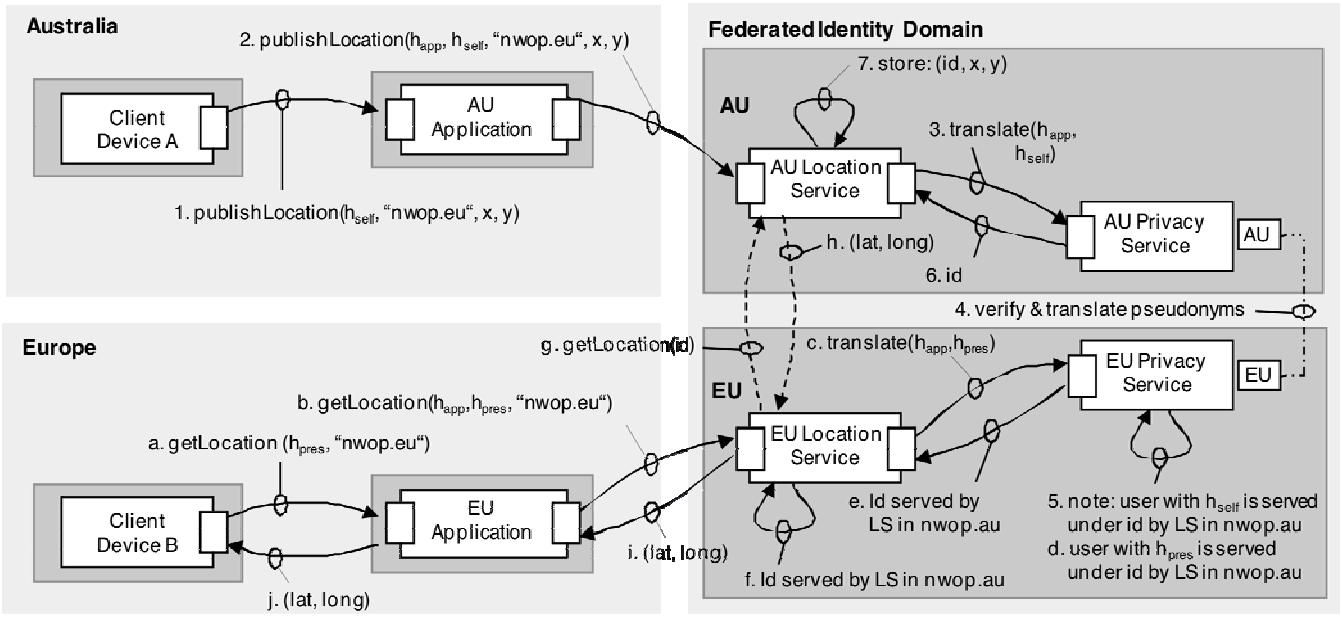

Figure 2. Location update and single location request across different network domains

Depending on the respective localization strategy at hand, the location service may switch between different modes to improve the freshness and accuracy of the location information. Finally, as soon as the location of some user changes the location service sends asynchronous location updates to the application. In case of long-term sessions, the location service queries the position of each involved user that is administered under the particular session and then sends a list of coodinate pairs to the application. As depicted in Figure 1, asynchronous messages contain the session identifier and the coordinate pairs of each particular user. Therewith it is guaranteed that the application has no more information than continuous changing pseudonyms that cannot be linked to coordinate pairs.

The whole service architecture, the pseudonym mechanism and the interworking of each single service that is based on this composition demonstrates only the case when all involved users share the same network operator. However, the most interesting setting is international roaming. In this context the growing fear of becoming victims of identity theft is one explanation why only few customers use advanced services and limit themselves to mere phone calls. Therefore, one focus of this paper is to look at a way how to establish a pseudonym-based privacy protection scheme that can operate in an environment that is dominated by distributed federated systems (Jøsang and Pope, 2005; Jøsang et al. 2005).

EXCHANGE OF LOCATION INFORMATION OVER DIFFERENT NETWORK DOMAINS

This section discusses how the proposed pseudonym generation mechanism can further be used to exchange location information even over different network operator domains. As an example we assume two different network operators, one in Australia and the other one in Europe. Figure 2 shows two users denoted as A and B. One is currently booked in the network domain of the Australian operator; the second one uses the Europan network. We further assume that user A roams in the Australian network and thus both, user A and B have the same European home network provider. Other constellations such as e.g. that the users not use different network operators but are within the same geographical area are conceivable. In our scenario user A is located in Australia but wants to provide his location to user B in Europe. A sends location information via the AU Application to the Australian location service. The *publishLocation(.)* request contains the user's self identifying pseudonym h_{self} and the domain information of her home network operator "nwop.eu". The so-called application pseudonym h_{app} in message 2 is a self-identifying pseudonym and allows the AU privacy service to identify the AU application. This is important to distinguish registered from unknown applications. Since the self-identifying pseudonym h_{self} of user A cannot be translated by the AU privacy service but knows that her home operator is "nwop.eu", it forwards the pseudonym h_{self} as part of message 4 to the EU privacy service.

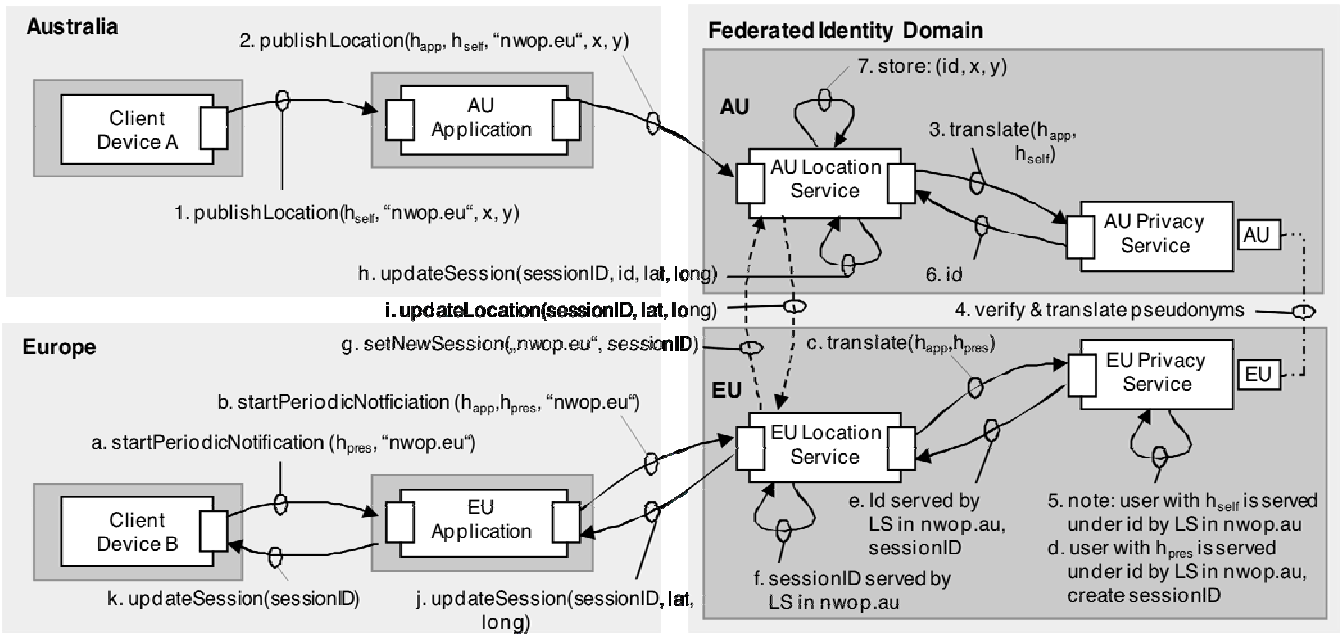

Figure 3. Periodic notifications about location updates across different network domains

To avoid that subsequent location updates by user A require further verification and translation requests of pseudonyms for the AU privacy service, the EU privacy service notes that user A is served by the AU location service (see message 5). Therefore, an identifier indicates that the AU location service serves the location information of users on behalf of another domain. The identifier and the coordinates are stored together by the AU location service in message 7. In order to request the location of user B (*getLocation(.)*), message a. contains among the domain information the pseudonym h_{pres} that denotes user A. Upon receipt of message b. which contains additional information h_{app} of the EU application, the EU location service requests for verification and translation of both pseudonyms from the EU privacy service. Since the location information is now served by the AU location service (message d.) the EU privacy service returns the identifier and the domain information of the responsible AU location service (message e.). Now, the EU location service receives the location information with the identifier (message f.) from the AU location service, which is then propagated back to user B.

Long-term processes

For long-term localization processes each clients, service and application is required to administer a session identifier. The use of sessions allows for notification of location changes even over different domains. Based on the previous explanations about how location information is exchanged over different domains for a single blocking *getLocation(.)* requests, we now discuss how location information is exchanged in the same environment for long-term localization processes. Messages 1 – 7 depicted in Figure 3 are initiated by user A to update the current location. This procedure is equal to the messages already described in Figure 2. All subsequent messages (a. *startPeriodicNotification(.)*) initiate a long-time localization process for user B. Such processes are administered under a certain sessionID that is created by the respective privacy service. It is further propagated to the EU location service (message e) and as the AU location service receives the contact point for location updates from user A, the new session is now also administered by the AU location service. Messages g. and h. induce the update of the sessionID whereas by message i. the location information is sent to the EU location service. Subsequent location update notifications are only sent in case the location of a user changes. Finally, messages j. and k. deliver the location information to the application and inform user B about the sessionID it needs for the management of sessions.

IMPLEMENTATION

At this stage we have implemented the core services including the location and the privacy service. For the localisation of mobile devices we use a webservice interface provided by a local network operator. The whole middleware platform is implemented on a JBoss application server (JBoss.org, 2008). In order to be able to test mobile applications also with many users we extended the location service in such a way that it does not only query the network for the actual location of mobile devices but also provides recorded GPS locations that are stored in GPX (GPX, 2008) files. The left side of Figure 4 shows

four sessions with the user names and coordinates. The map on the right side shows the actual position of each user. The current implementation allows to manage multiple sessions, compareable to the situation when different mobile users start tracking sessions in parallel. Furthermore, by use of the pushlets-framework (Pushlets.com, 2008) for the location service, location changes are instantly updated by the browser (Jorns and Quirchmayr, 2008).

Figure 4. Management Interface of the Location Tracking Platform

Our implementation provides all described functions, such as asynchronous notifications about location changes, session management and the pseudonym functionality for privacy protection. However, the system provides only those functions that are needed to exchange location information within one domain but cannot handle handle cross-domain location exchange.

CONCLUSIONS AND FUTURE WORK

The protection of privacy becomes increasingly important because of a significant shift towards enabling law enforcement access to data collections. As a result mobile network service operators are currently in a controversy situation. The effort of law enforcement agencies to prevent crimes obliges mobile network service operators to collect more data of their customers which results in a situation where customers even start to refuse services. For network service operators the problem becomes even worse if they try to sell services such as location-based services that are generally considered as to be intrusive. To overcome these deficiencies the need for solutions that provide privacy is evident. In this paper we have proposed the use of a simple but effective privacy enhancing mechanism that is based on the notion of pseudonyms. It allows users to anonymously request services even from untrusted services without the need to reveal sensitive data. The proposed service architecture makes use of this pseudonym mechanism and at the same time allows the realization of the higly postulated pay-as-you-go model. Another important aspect we have considered in this paper is how to exchange location information of users across different network domains. To overcome typical constraints of existing proprietary Telco solutions, such as the inability to request location information of users that are either not subscribed to the same network operator or roaming, we propose an extension of our architecture that incorporates the use of pseudonyms and allows the implementation of location-based services over different network domains. This enables the worldwide use of the pay-as-you-go model.

At this stage our system does not support the use of privacy policies that allow users to express certain decisions under which location data can be accessed, transmitted and processed by other parties. Hence, one of the next steps will be the extension of the privacy service by a definition of appropriate privacy policies as introduced in (Zeiss and Jorns, 2008). The current implementation of the system shows the feasibility of the underlying pseudonym generation scheme. The whole implementation is run in a virtual machine on a standard PC with 3.4GHz CPU. In the future we plan to extend the system by the proposed cross-domain aspects. Since the system resources are absolutely not exhausted so far we expect that once each service is operated on a dedicated server, the scalabilty and performance of the system will still be given, even if the number of users is very high. Of course, some critical services such as the location service will be subject to a critical analysis. Implementations for mobile devices will have to be evaluated with regard to performance and applicability.

REFERENCES

1. The Financial Crime Branch - HM Treasury (2002) THE UK'S ANTI-MONEY LAUNDERING LEGISLATION AND THE DATA PROTECTION ACT 1998 GUIDANCE NOTES FOR THE FINANCIAL SECTOR, April 2002, URL: http://www.hm-treasury.gov.uk/mediastore/otherfiles/money_laundering.pdf
2. Erich Lichtblau (2006) Controls on Bank-Data Spying Impress Civil Liberties Board, NYT, November 29, 2006, URL: http://www.nytimes.com/2006/11/29/washington/29nsa.html
3. European Digital Rights (2006) EU-US agreement on passenger data transfer annulled, June 7, 2006, URL: http://www.edri.org/edrigram/number4.11/pnr
4. Federal Deposit Insurance Corporation (FDIC) (2007) Bank Secrecy Act and Anti-Money Laundering, August 24, 2007, URL: http://www.fdic.gov/regulations/examinations/bsa/index.html
5. EU (2006) Directive 2006/24/EC of the European Parliament and of the council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending (EU, 2002), *Official Journal on the European Communities L 105/54*
6. EU (2002) Directive 2002/58/EC of the European Parliament and of the council concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), *Official Journal on the European Communities L 201/37*
7. EU (1995) Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data, *Official Journal of the European Communities L 281/31*
8. Parlay (2008), The Parlay Group, URL: http://www.parlay.org
9. Electronic Privacy Information Centre (EPIC) (2008) The public voice (last accessed 13.2.2008), URL: http://thepublicvoice.org
10. Parliament of the United Kingdom (1998) Data Protection Act (c.29), URL: http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_1
11. Penders J. (2004) Privacy in (mobile) telecommunication services. *Ethics and Information Technology*, 247-260
12. Barkhuus, L. and Day, A. K. (2003) Location-Based Services for Mobile Telephony: a study of users' privacy concerns, ACM Press, Interact 2003, Zurich, CH
13. Barkhuus, L. (2004) Privacy in Location-Based Services, Concern vs. Coolness, Workshop paper in Mobile HCI 2004 workshop: Location System Privacy and Control, Glasgow, UK
14. Gruteser, M. and Grunwald, D. (2003) Anonymous Usage of Location-Based Services Through Spatial and Temporal Cloaking, Proceedings of First ACM/USENIX International Conference on Mobile Systems, Applications, and Services (MobiSys), San Francisco, CA
15. Yee, G. (2005) Using privacy policies to protect privacy in UBICOMP, in *Proceedings of the IEEE 19th International Conference on Advanced Information Networking and Applications (AINA 2005 – Volume II)*, 633-638
16. Cheng, R., Yu, Z., Bertino, E. and Prabhakar S (2006) Preserving User Location Privacy in Mobile Data Management Infrastructures, 6th Workshop on Privacy Enhancing Technologies (PET'06), Cambridge, UK
17. Jøsang, A. and Pope, S. (2005) User Centric Identity Management, in *Proceedings of the Asia Pacific Information Technology Security Conference*, AusCERT'2005
18. Jøsang, A., Fabre, J., Hay, B., Dalziel, J., Pope, S. (2005) Trust Requirements in Identity Management, Conferences in Research and Practice in Information Technology Series, in *Proceedings of the 2005 Australasian workshop on Grid computing and e-research*, 99-108
19. JBoss.org (2008) JBoss Enterprise Application Platform (last accessed 15.5.2008), URL: http://www.jboss.org/
20. GPX (2008) the GPS exchange format (last accessed 15.5.2008), URL: http://www.topografix.com/gpx.asp
21. Pushlets.com (2008) A HTTP-based publish/subscribe framework (last accessed 15.5.2008), URL: http://www.pushlets.com
22. Zeiss J. and Jorns O. (2008) Context-Based Privacy Protection for Location-Based Mobile Services using Pseudonyms, The 2nd International Workshop on Privacy-Aware Location-Based Mobile Services (PALMS'08), In conjunction with the 9th International Conference on Mobile Data Management (MDM'08) April 27, 2008, Beijing, China