A Privacy Enhancing Mechanism based on Pseudonyms for Identity Protection in Location-Based Services

Oliver Jorns[1,2], Gerald Quirchmayr[2,3], Oliver Jung[1]

[1]Telecommunications Research Center Vienna (ftw.)
Donau-City-Strasse 1
1220 Vienna, Austria
Email: {jorns, jung}@ftw.at

[2]Department of Distributed and Multimedia Systems
Faculty of Computer Science
University of Vienna
Liebiggasse 4/3-4, A-1010 Vienna, Austria
Email: {Oliver.Jorns, Gerald.Quirchmayr}@univie.ac.at

[3]School of Computer and Information Science
Division of IT, Engineering and the Environment
University of South Australia
Mawson Lakes SA 5095, Australia
Email: {Gerald.Quirchmayr}@unisa.edu.au

Abstract

Over the past years Mobile Business has gained significant progress not only because of higher transfer rates as well as advanced processing power and memory capabilities of networks and mobile devices but also because of novel location-based mobile applications which raise many expectations in the mobile market. As a result network operators start to offer their services to 3^{rd} party application providers which fosters the development of innovative applications. However, today mobile applications are forced to operate in the restricted environment of one network operator which is rather cumbersome for the development of novel location-based mobile applications that need to exchange location data between different network operators, over different countries.

In this paper we discuss a system architecture aimed for location-based services that overcomes the aforementioned deficiencies. It uses transaction pseudonyms for the exchange of sensitive data by preserving users privacy and allows the development of novel applications that are operated by 3^{rd} party application providers accessing different network services. We show that the management of identities and pseudonyms allows even roaming users access to different kinds of location-based services.

Keywords: pseudonyms, privacy, security, hash function, identity management, location-based services, telecommunication services.

1 Introduction

Mobile and context-aware software applications are expected to play an even more important role in our everyday life in the near future. Today, we are still not able to fully implement ubiquitous computing as it was envisioned by Weiser (1991). During the last years research in this field has made excellent progress in many aspects and the development is amongst others fostered by the evolution of mobile devices in terms of processing power, memory and provided network interfaces such as GPRS, WLAN and Bluetooth. At the same time network operators gradually allow access to previously hidden location and message services which in turn leads to a new class of service providers. They allow independent service provider access to network services through standardised interfaces such as Parlay X (2006).

One concept that is based on these technologies is the so called location-based service. Even though it has gradually developed over several years it did not turn out to be the "killer application" that it was predicted to become some years ago. Junglas (2005) refers to market predictions which state that by 2005 almost 50% of the subscribers will use location-based services. In the US market the driving force of location-based services is the E911 mandate which forces mobile operators to provide location information in emergency cases. Whereas E911 finds general approval, the users' acceptance of location-based service in other areas is much lower than expected. One reason is that LBS strongly relates to the users' identity. The general acceptance is that identity data is linked to the actual position. This information in the hands of malicious people or organisations may raise severe privacy issues up to life danger.

Anyhow, today's location-aware mobile business offers a variety of services, applications and products such as services for anxious parents who equip their children with GPS and wireless technology embedded watches. Other applications help to find friends[1] whereas curious people watch their spouse[2]. All these applications have in common that they reach deep into the private sphere of persons and families. That is why privacy advocates over and over again point to the potential danger of such applications.

However, there are cases where it is difficult or even impossible to sufficiently protect the user's privacy. Services that require once-only consent in order to provide location information to other users can be misused by family members or others who may lock

[1] http://jackmobile.de
[2] http://www.ehebruch24.de

the mobile for the time necessary to await the localisation confirmation message. In order to avoid misuse and protect peoples privacy it is therefore useful to send messages from time to time that remind users of the activation of the localisation service.

In this respect legal aspects pertaining confidentiality and security as well as the processing of data are prescribed by the European Union Data Protection Guideline Directive 95/46/EC (1995). Article 16 discusses the issue of confidentiality of processing of personal data from a technical and organisational point of view whereas Article 17 deals with security and processing of professional data and the legal constraints. Negotiations between European member states about the processing of data and privacy led to a directive which extends Directive 95/46/EC (1995) and provides a wider scope on privacy and electronic communications, that is Directive 2002/58/EC (2002). This explicitly describes traffic data as "*any data processed for the purpose of the conveyance of a communication channel on an electronic communications network or for the billing thereof*" and location data as "*any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user or a publicly available electronic communication service*". One important requirement is that users must be kept informed about each single location request. In order to prevent users from annoying confirmations each time the location is queried by another user, it must be possible to grant permission once for all subsequent requests. Equally, the system must provide simple and free of charge measures that temporarily prevent from further processing of location.

As Price (2004) states, software systems have to be jurisdiction aware. As privacy regulations vary and change, this is not easy to achieve. From a users point of view one requirement is that the system must provide means which inform the user about the purpose, the time span of location data usage and if other 3^{rd} party providers receive this data. Hence, data must be under the sole control of the owner, which becomes a very complex task and worsens if data is to be processed in different countries. The European Directive 2002/58/EC (2002) therefore defines a so called *transitive closure* which allows data only to be exported to other countries which provide equal data protection guidelines or under the provisions of special contracts. As stated by Fischer-Hübner (2001), from an international point of view however the EU Directives do not provide sufficient privacy protection in the context of a global information society. Fortunately, there is a growing number of countries outside the EU that have started to adopt their new laws to be conform to the EU Directives.

The structure of the paper is as follows: In Section 2 we discuss related work which is followed by a motivation that outlines the importance of privacy mechanisms as well as advantages expected through the implementation of privacy measures. We then extend the discussion with the consideration of an appropriate identity management that allows LBS to exchange location information of users even in case of roaming. Section 4 discusses common concepts of identity management and exemplifies the usage of identifiers and pseudonyms. Section 5 explains the whole system architecture and its different components whereupon Section 6 discusses in detail how and where pseudonyms are generated and processed. This pseudonym mechanism represents the fundamental mechanism for protecting user's privacy and can be seen as the essential mechanism of our system. Next, Section 7 goes into details of the basic system functions and explains how the pseudonym mechanism is applied to perform operations. Section 8 discusses some of the most important security issues such as message integrity, replay protection as well as non-repudiation of messages. In Section 9 we show that minor changes of our pseudonym based privacy enhancing mechanism allow users to exchange location information across different domains. Finally, Section 10 concludes our paper and gives an indication of further work.

2 Related work

Research on privacy for location-based services has led to numerous solutions. Many of them, such as Gruteser *et al.* (2003) and Yee (2005) focus on the definition, distribution and enforcement of privacy policies. Others are 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. There exist also hybrids of the aforementioned approaches. However, from our point of view the most appropriate solutions are those that use pseudonyms in order to veil the real identity of users.

Kölsch *et al.* (2005) show four different business scenarios for location-based services. The most interesting scenario for their location-based services privacy solution is the so called intermediary scenario. 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.

Rodden *et al.* (2003) suggest user generated random pseudonyms. The user provides its location data together with a timestamp and the associated pseudonym to the location service. 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.

Gruteser *et al.* (2003) and Cheng *et al.* (2006) propose location cloaking with the concept of k-anonymity. A user is k-anonymous if the location information he provides cannot be distinguished from the location information provided by k-1 users. In the context of location data k-anonymity means that in a certain rectangular area in a time interval are at least k users present. This is achieved by adapting the size of the rectangular and the time interval accordingly.

The IETF Geographic Location/Privacy (GEOPRIV) working group defines requirements for the authorisation, integrity and privacy of location information. The developed specifications describe how location information is transferred in a secure manner and how the release or representation of such information is to be authorised. In order to enforce the user

controlled privacy policies a so called location object is defined which holds information about the location as well as associated privacy rules.

In Schulzrinne (2006) a message format for authorisation policy rules is defined that supports different transformations for location data with the aim to control e.g. the resolution of data delivered to a location recipient. It allows making authorisation decisions based on location conditions like the presence of the target in a specific area or when the target altitude is within a certain range.

Another important aspect with regard to the exchange of location information concerns roaming between different service providers offering location-based services that may even be located in different countries. Wu (2005) proposes a scheme that allows the integration of location-based services into web services which solves the problem of service roaming without the need of configuration.

3 Motivation

International standardisation bodies identified privacy and identity management as important issues that are addressed e.g. by the upcoming ISO/IEC 24760 - a framework for identity management - and in the CEN Workshop Agreement 15263 (2005). According to CEN the lack of appropriate privacy mechanisms can impose a number of risks for the information system and thus to the enterprise operating the system. Examples are a lack of trust which prevents users from using specific information systems, unlawful usage of personal data which may have serious impact on the enterprise public image as well as the abuse of personal data which can result in lower stock market value.

Therefore, the implementation of privacy measures can have significant advantages such as the reduction of costs for handling unnecessary data as well as improved customer trust in the protection of personal data which results in higher loyalty of customers.

However, Jøsang (2005) analyses the trust relation between customers and identifies and states that the most commonly used model is the *isolated identity management model*. It binds each identifier to one isolated service. In contrast to that the proliferation of new services and applications confronts users and service providers with the problem of how to manage many different accounts. Additionally, the need for new location-based services which allow unlimited exchange of location information also for roaming users challenges new system architectures that also take into account the evidently importance of privacy.

This motivated us to develop a new system architecture that does not necessarily require prior subscription to even non trusted 3^{rd} party providers which thus allows the realization of the aforementioned pay-as-you go model. Although 3^{rd} party providers operate on user's location information, the identity of each of the respective user must be protected even in case of roaming.

4 Management of Identities

Identity management in our context refers to the secure management of various identities. It also encompasses the identification process during which an entity (a person, an institution or an object may have different identities depending on the context) may be verified in a certain context. An identity is the representation of an entity in a context or application domain.

The identification process, which is part of identity management, is based on identifiers associated with every identity. An identifier is a characteristic of an identity and unique in a given context. For privacy reasons also a pseudonym can be used as an identifier. When an identity is identified using a pseudonym one can say that the entity holds an anonymous identity.

Common concepts for identity management are *federated identity management* and *centralised identity management*. Jøsang (2005) additionally introduced the notion of *isolated identity management* which is the simplest way of identity management and used in most systems today. Service providers issue identifiers and credentials to the user that are solely associated with their service and that can only be used with this single service. This leaves the management of identifiers and credentials to the user and will lead to a unmanageable number of credentials. Prior to usage of a specific new service a user needs to register with the service in order to get access. The additional effort required for registration might hinder service usage and leads to a loss of revenues for service providers.

A representative example for this are location-based services. Numerous mobile network operator already provide location-based services for their customers. Unfortunately this only works when the user is in its home network and not in the roaming case. The reasons for this are of technical and of legal nature as already discussed in the introduction. It will be shown later how these restrictions can be overcome with our system.

The concept of *federated identity management* requires trust relationships between different service providers. Federated identities may serve across different contexts by means of cross context identification. It enables a service provider to accept the identification process performed by another service provider, who originally supplied the credentials. In a centralised identity management scenario there is only one issuer of identifiers and credentials. This single set can be used for all services. For our approach we chose the centralized identity management scenario because the user is expected to have the highest degree of trust in the privacy service of his home network provider.

Identifiers and pseudonyms

The usage of pseudonyms as identifiers allows for anonymity in identity management. An essential factor for effectiveness of pseudonyms is the unlinkability between the pseudonym and its holder and if pseudonyms can be linked between each other.

Pfitzmann *et al.* (2001) discriminate different kinds of pseudonyms depending on:

Knowledge of the linking between a pseudonym and its holder: The highest degree of anonymity can be reached with little knowledge of the linking between the holder of a pseudonym and its pseudonym. The more is known about the pseudonym linking the less is the strength of anonymity. The lower and upper limits on the scale of anonymity are public pseudonyms on the one side and initially unlinkable pseudonyms on the other.

Linkability due to the use of pseudonyms in different contexts: The strength of anonymity decreases with an increasing number of pseudonym uses in general and especially in different contexts. The degree of anonymity is raised the more often pseudonyms are changed. The highest degree of anonymity can be provided by transaction pseudonyms that are used only once.

Our system makes use of transaction pseudonyms, where another pseudonym is used for every transaction thus preventing the linking of pseudonyms by equality of pseudonyms. However, the transaction

pseudonyms can be unambiguously linked to an identity as a shared secret is involved in the transaction pseudonym generation process. The user defined shared secret is also known to the privacy service where it can be used to identify the origin of the pseudonym. When we categorise this in the sense of linkage between a pseudonym and its holder the identity of the user could be revealed by the privacy service. However, the mobile operator's privacy service is considered to be trusted in our threat model. The primary role of the pseudonyms is to anonymise the user's identity towards the potential untrusted 3rd party application provider.

5 System Architecture

This section introduces the system architecture as it is depicted in Figure 1. The various services, components and software modules provide in sum the technological basis for different kinds of LBS such as location-aware or location-tracking applications discussed in Section 7.4.

5.1 Client Device

Users interact with the system via a high-end-PC, cellular phone or a personal digital assistant (PDA). In order to be able to receive the current location information the device may implement a GPS module which collects the location data. For our prototype implementation we focus on cellular phones and PDAs with limited computation power and storage capabilities as well as restricted means of communication. The application logic module controls when and how location data shall be sent to the location server. In case of automatic updates it regulates the update-frequency which depends on various factors such as the distance the user covers during a certain time period or a scheduler.

Each client as well as the 3^{rd} party applications and the network operator's privacy service implement a privacy agent. It generates digital pseudonyms on the basis of attributes which are stored by the network operator's user profile database. Beside creation of pseudonyms it is also responsible for the management of pseudonyms during operation. The privacy service's agent has access to sensitive information like the mobile subscriber-integrated service digital network (MSISDN) number which is used by e.g. the location service to perform cell-based localisations.

5.2 3^{rd} Party Application Provider

The core application logic is implemented by the 3^{rd} party application provider which further provides different interfaces to service providers. One example for an external service provider is a geographic information system (GIS) service which allows on-the-fly generation of maps indicated with the actual positions of users.

5.3 Network Operators' Services

Network operators provide different services such as the location, message and presence service which can be accessed by the 3^{rd} party application providers through standardized interfaces such as OSA/Parlay X (2006).

5.3.1 Location Service

The location service may support different ways to obtain location information of a user. One is cell-based localisation where users are localised with the help of the network. The actual localisation is performed by a location server which accesses the user's location data in the network. The advantage of this kind of localisation is that it works as soon as the user is connected to the network. Compared to GPS localisations which requires line-of-sight to satellites, this technology allows localisations of users even if they are in buildings or in the underground. However, one decisive disadvantage is that the locations' accuracy may in some cases not be sufficient enough since the location information is equivalent to the actual position of the antenna the mobile is connected to. Whereas the density of antennas in urban areas is mostly high enough to provide location data with sufficient precision, in the countryside the distribution of antennas is characterised by far distances which may render location-based applications rather useless.

Beside cell-based localisations which are performed by the central location service, users may also wish to update their location data themselves. Therefore, the location service provides a dedicated interface which allows to receive location information that are sent by users directly.

This leads to different active localisation processes with changing location sources that have to be handled by the location service and which also influence each other. For example, cell-based localisations may be interrupted by location updates initiated by mobile users. Depending on the application characteristics, the location service is in charge of the different localisation processes that are running in parallel and controls the update rates which depend on various factors such as time, covered distance or other user defined preferences. Further, upon location changes it notifies 3^{rd} party applications which then react according to the implemented logic.

5.3.2 Presence Service

The presence status of users can be expressed by a vast number of attributes. The most important ones are *activity* (going by car, waking, waiting,...), *communication means* (bandwith,...), *contact addresses* (email, SIP, mobile,...), *location type*, *mood* (happy,...) and *privacy* (can talk). Of course, this list is by far not complete but it gives an idea of the potential sensitivity of that information. The presence service maintains these attributes for each user. I also receives notifications if one or more attributes change and notifies the application.

5.3.3 Message Service

An essential part of the system is the ability to inform users asynchronously about certain applications' states which depend on the location information received from the location service as well as the current presence status of user. In order to receive the appropriate destination address(es) the messages service and the presence service work closely with each other. Given the session context and the pseudonym based privacy enhancing mechanism the user's privacy remains preserved.

5.3.4 Subscription Service

The subscription service provides a web-based interface to allow users to access the privacy service for management and administration purposes of pseudonyms, aliases and privacy access rules. In this respect, the subscription service's responsibility is to provide means of (re)initialisation of pseudonyms between two entities (user - user, user - object) in case that pseudonyms are out of sync and coordination

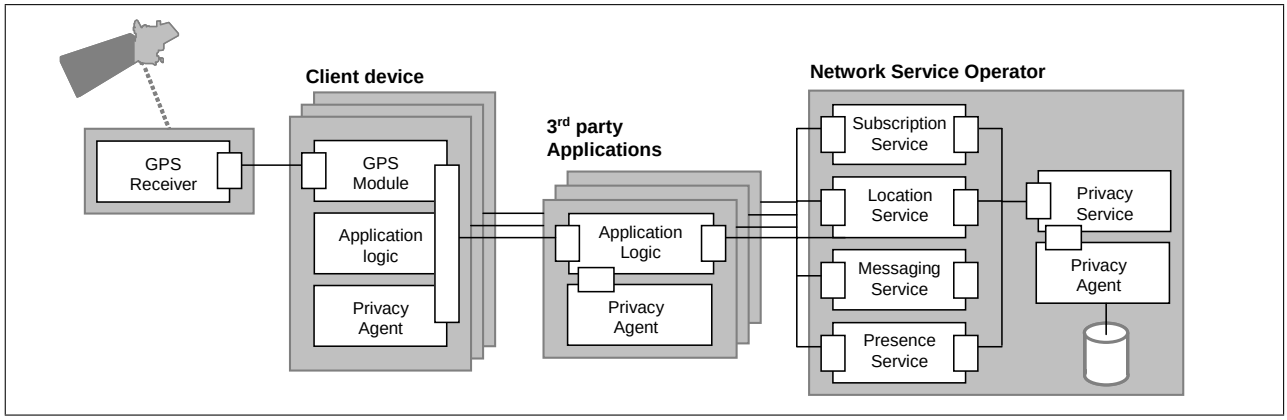

Figure 1: System Architecture

during the subscription and authorisation phase between the watcher and the presentity.

6 Digital Pseudonyms

The first who picked up the idea to use hash values for authentication was Lamport (1981). The process starts by computing the first hash value h_1 from a given shared secret. The first value h_1 is then used as input to compute h_2 and so on. If the client needs to authenticate, it first calculates the n$^{\text{th}}$ hash value on the basis of the shared secret and sends this value to the server. Upon receipt, the server hashes the stored hash value h_{n-1} and compares it with the received n$^{\text{th}}$ hash value. If $h(h_{n-1}) = h_n(sharedsecret)$ the authentication was successful and the server stores the actual value of n decremented by one. For the next authentication, the client generates and sends h_{n-1}. This is compared by the server that rehashes the stored hash value $h(h_{n-2}(sharedsecret))$.

Given Lamports' system, the computational effort depends on the number of hash values n and increases with order $O(n^2)$ for more than one authentication. In other words, since each hash chain of length n requires $n\cdot(n+1)/2$ hash value calculations, this scheme is not suitable to be applied to mobile devices with low computing power since high computational effort affects heavily the battery.

We therefore applied a pseudonym generation scheme that was invented earlier by Jorns et al. (2005) and that is based on HMAC by Bellare et al. (1996). In the following we explain our proposed pseudonym generation scheme in detail.

Initialisation and Generation of Transaction Pseudonyms

HMAC is based on standard hash functions such as MD4/5 or SHA-1/2. Each hash value is used in combination with a shared secret key which must be negotiated in a secure manner between the client and the mobile operator prior to the first service usage. One way to securely negotiate secret keys offers the Diffie Hellman key exchange protocol by Diffie (1976). Another possible solution is to use the already existing contractual relationship between the user and his network operator. However, for security reasons the latter solution is rather disadvantageous since human readable secrets are more likely to be guessed.

As depicted in Figure 2, the pseudonym scheme is initialized with an initial random value we call *anchor* that is sent from the network operator to the client. The network operator's privacy service then computes the first pseudonym p_1 by applying the *anchor* together with the user's shared secret to the HMAC function. For the first service call, the user's privacy agent computes pseudonym p_1 in the same way.

Figure 2 depicts the pseudonym calculation scheme in table form. It is visible that both, the user's privacy agent and the network operator's privacy service compute the same pseudonym for each service request. In this example we assume that user A has already subscribed to the location of user B. However, before user A is allowed to ask for the location of B, B has to grant the permission to A. It is also possible that user A subscribes to his own location whereupon the *anchor* is sent immediately to A.

As the privacy service receives a pseudonym that is e.g. p_1, it searches in the database if the pseudonym is stored. If so, the associated identifier is returned to the respective service. For example, for cell-based localisations, the location service receives the telephone number whereas the messaging service may receive an e-mail address.

Now, the privacy service computes p_2. It therefore applies p_1 together with the user's shared secret to the HMAC function and stores the new pseudonym in the database. For successful authentication, the user's privacy agent has to compute p_2 whereupon the privacy service computes p_3 an so on.

7 Basic System Functions

This section is divided into two parts. The first one explains the implemented mechansisms for the realisation of position-aware applications and sporadic queries. The second part of this section shows how periodic location notifications that can be used by applications which rely on long-term tracking of users and objects is realized.

7.1 GPS Location Update

We start our explanations with one of the most important basic function for location-based services, that is *location update* at the location service performed by the user.

When a user initiates a location update, the user's privacy agent first generates a self-identifying pseudonym and sends it together with the actual coordinates to the respective 3^{rd} party application. There are two reasons why location update requests are sent directly to the application. One is to hide the network operator's services from users. The second one is to provide users a unique interface. Since the application cannot resolve the pseudonyms they are forwarded together with the coordinates towards the location service.

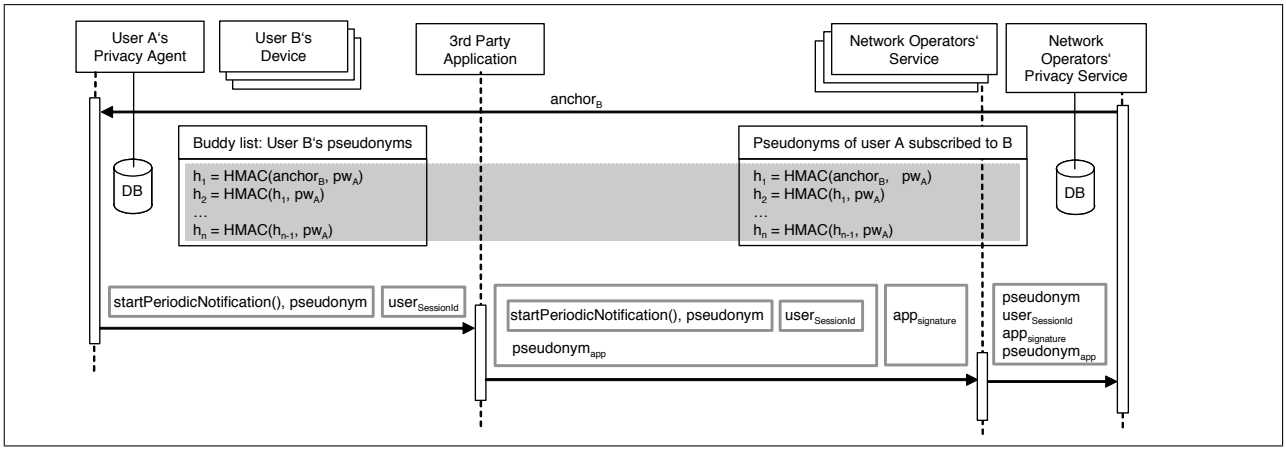

Figure 2: Pseudonym Schema and Message Integrity through HMAC

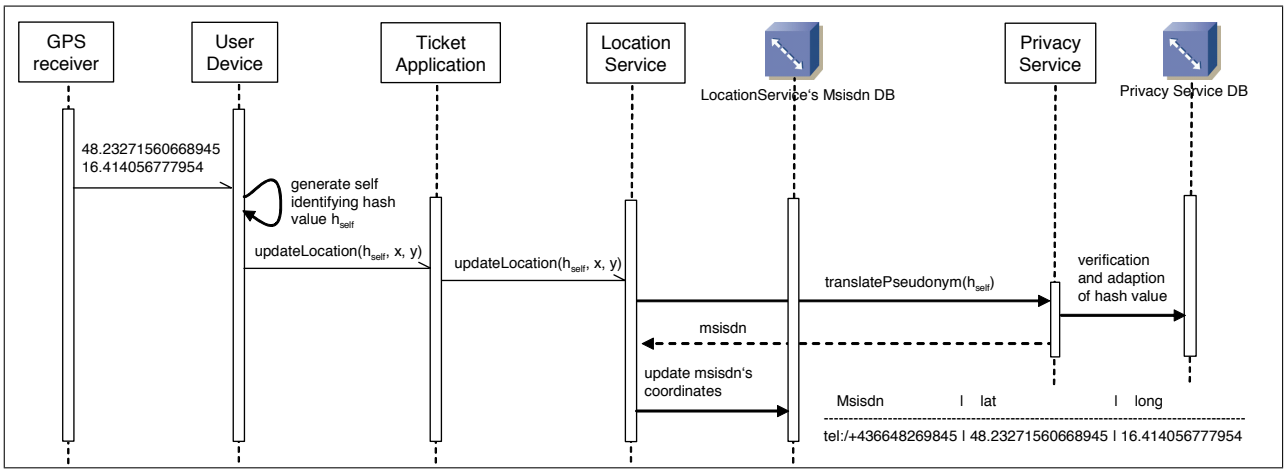

Figure 3: User updates GPS location information

Depending on the respective service the request for translation of pseudonyms comes from, the privacy services' answer is either the MSISDN which identifies each user unambiguously or an identifier which is used to hide the identity of the respective person and to prevent correlations of a person's MSISDN with its location information. For cell-based localisations the MSISDN is mandatory because a location request towards the location server must contain the MSISDN. As the location service is part of the network operator's domain no additional privacy protection is necessary. The identifier is used if the location service is not entirely trustworthy. This allows the integration of location services which are operated by 3^{rd} party providers. Figure 3 shows the location update procedure. In this example the location information is associated with the MSISDN which means that the location service is within the network operator's domain.

7.2 Location Query

Besides location updates, users may also query location information. From the technical point of view it makes no difference if the user asks for his own position or the position of buddies. By the same token also static or moving objects can be localised. The only requirement is a valid pseudonym for each localisation. Similar to location updates as described in the previous subsection, the user sends a request to the application. This time the request contains the command `getLocation` as well as one or more pseudonyms of the respective persons or objects. These pseudonyms are translated by the privacy service whereupon the location service may either initiate cell-based localisations or access already stored location data.

7.3 Periodic Notification and Processing

In addition to location updates and queries as described above, the system further allows users to initiate long-term localisation processes which are operated on behalf of users by the 3^{rd} party application providers' application logic. Upon activation, the application module is constantly notified about location changes by the location service and allows users to be notified asynchronously upon location combinations of presentities in consideration of additional contextual information provided by the presence service. As depicted in Figure 4 the watcher first sends a list of pseudonyms that represent those presentities that shall be part of the long-term localisation process to the application. The $user_{SessionId}$ value represents the HMAC of the values of the message which is also used to provide message integrity (see Section 8.1). In the context of management of long-term processes, the location service uses the $user_{SessionId}$ value in conjunction with the command `startPeriodicNotification`. This session-context reaches from the privacy agent of the client to the privacy agent of the privacy service and allows the users' client to initiate subsequent user interactions referring to particular long-term processes under a given $user_{SessionId}$ value.

In case the location service is part of the network

operator, it may contact the location server in order to perform cell-based localisations. The update-rate of each localisation process may depend on various factors such as the current number of required localisations per second in total, if and how often changes of the positions are recorded and if there are priorities to consider. Since it is also possible that the position updates may stem from each presentity directly the client's application has to decide when to send location information to the location service by taking into account traffic costs. Upon receipt of location information, the location service also decides when to send a location-update message to the application. The location update-strategy in sum depends on various factors and may be vary from application to application. Further questions such as whether user are equipped with a GPS receiver or not and if the location service supports also cell-based localisations or not must be considered in order to achieve reasonable application's behaviour.

Each location update message the location service sends to the application contains the session identifier which allows the assignment of the coordinate-pairs (latitude, longitude) to the respective presentities. The applications' task is to process this location data conveniently. User may therefore specify rules which analyse the current position of presentities and thereupon initiate further processing such as message delivery, adaption of the presence status and others. Depending on the characteristics of the application this rules can be adapted to express different requirements in changing situations.

7.4 Example Applications

Each of the following applications can be implemented on the proposed architecture and represents an example of position-aware, sporadic-queries and locaction-tracking applications.

Position-aware and Location-Tracking Applications: The distinction between position-aware and location-tracking applications is also discussed by Junglas (2005). The main difference between these two kinds of applications is the role of the requester. For position-aware applications the requester is the user herself. For each request the user may provide her actual location information in order to e.g. receive the route to the closest restaurant. The 3^{rd} party application receives the location information directly from the users or from the location server. This allows 3^{rd} party application providers to provide a variety of applications which receive and process location information independently.

Sporadic Queries: In most cases location-based services are designed to collect and process location information about persons or objects. This location information can then be used combined with other information sources. However, Weiß et al. (2006) refer to a different class of location-based services called *Zone Services*. Given a certain location or geographical zone, this special kind of LBS provides e.g. the number of users or objects within the vicinity.

8 Security Considerations

In the following we discuss some of the most important security issues which include message integrity, message replay protection, non-repudiation of messages as well as message integrity.

8.1 Message Integrity

One fundamental security requirement is message integrity, that is, the receiver of a message should be able to notice whether the content of a message has been changed during transit or not. Due to computational limitations of the users' devices, we prefer a light-weight solution that is technically equal to the aforementioned pseudonyms. Now, the input values of the HMAC function are the command (e.g. `startPeriodicNotification`) and one or more pseudonyms. Alike pseudonyms these HMAC values are verified exclusively by the network operator's privacy service. As explained in Section 7.3 the HMAC value is further used as session identifier. It gives users control over the applications' behaviour in long-term localisation processes (see Figure 2). The first message contains the command `startPeriodicNotification`, a pseudonym and the HMAC value denoted by $User_{SessionId}$. Upon receipt, the 3^{rd} party application generates a pseudonym h_{app} which allows the privacy service to verify the authenticity of the application. Finally, the application uses its shared secret to generate a HMAC value $app_{signature}$ as signature.

As the privacy service receives the message from the location service, its task is to identify the sender of the message. It first checks if it finds the pseudonyms of the respective watcher and the application and then fetches the respective shared secrets to recompile and verify the validity of the signatures. In case of long-term localisation processes the privacy service further establishes a session-context which associates the watcher with the respective presentities.

8.2 Replay of Messages

Each message contains one or more unique pseudonyms whereby each one denotes exactly one particular person. According to the pseudonym generation scheme, each consecutive service call requires the respective next pseudonym. That is why it is not possible to reuse any pseudonym, thus it is not possible to send messages repeatedly.

8.3 Non-Repudiation

In the same spirit as the system protects from replay attacks, it also provides non-repudiation. Each message respectively each pseudonym the network operator's privacy service receives can be assigned to one particular identity. Thus, as long as the shared secret was not stolen it is impossible to decline that a messages was not sent. To provide higher security the shared secret can be generated periodically. As described in Section 6 the Diffie Hellman key exchange protocol can be used.

8.4 System Security and Privacy Protection in General

For the realisation of location based services Unni et al. (2003) state that it is essential that the different security and privacy concerns of each of the involved entities are considered carefully:

Network Providers have vital interest in keeping trust with their customers. Through the advent of location-based services, network providers are encouraged to offer appropriate privacy measures such as permission-based services, aligned level of precision concerning location information as well as tiered relationships with third party providers and content providers. *Application Providers* have the means to build context-aware applications that not only make use of users location information but also from other sources. The combination of these partially sensitive data may raise serious privacy concerns of users. Hence, application providers walk a

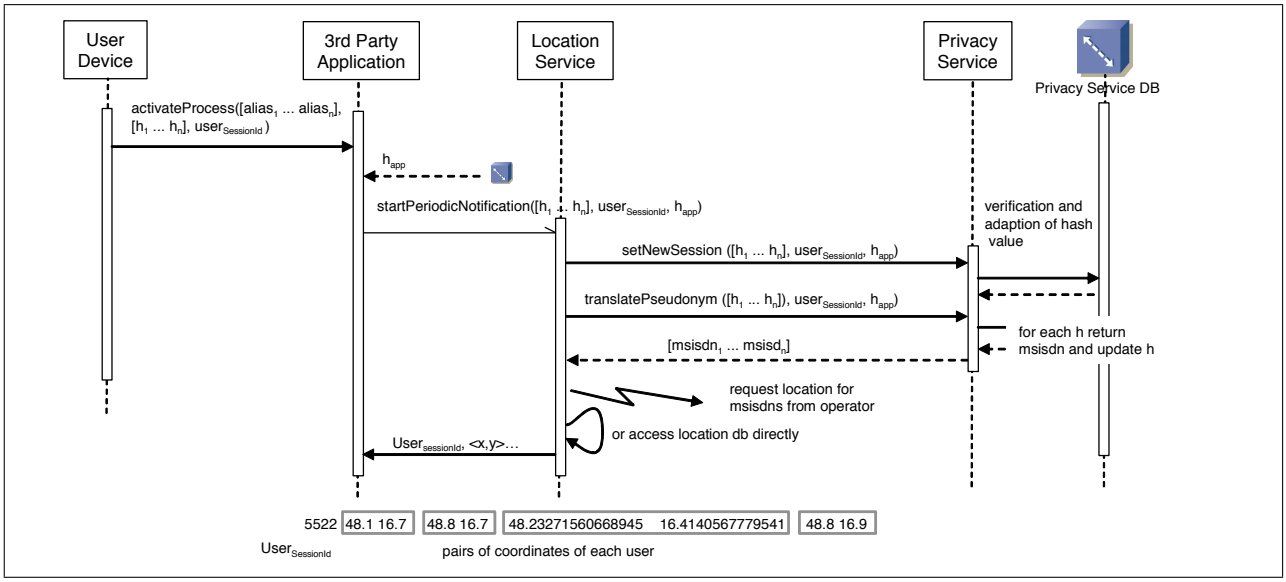

Figure 4: Long-term Process Activation and Periodic Location Notification

tightrope between personalization and accommodating privacy obligations. *Users* may be concerned of using location-based services if they are not able to control who may access their data and when. In order to allay users privacy concerns the potential of mobile devices to store personal data and enable location-based services has to be well-balanced.

9 Location-Based Services for Roaming Users

In the introduction we discussed legal obligations which clearly show the importance of privacy with regard to location-based services and in succession technological requirements necessary to build stable solutions. We assumed that all involved parties such as user and the 3^{rd} party application providers have a contractual relationship with only one particular network operator. The proposed privacy enhancing mechanism that is based on pseudonyms constitutes a good solution with regard to the technical conditions imposed by the clients' hardware capabilities.

The notion of privacy gains even more importance if sensitive data shall be exchanged between 3^{rd} party application providers and network operators of different domains. An attempt in this direction was proposed by OMA (2005). It describes how visited operators may push tourist information to roamers. It does however not cover some fundamental aspects of location-based services such as the possibility to allow users to update their position.

Our solution addresses the aforementioned deficiencies. We show, that minor extensions of our pseudonym based privacy enhancing mechanism allow the secure exchange of sensitive data by providing privacy.

9.1 Extended System Architecture

Each user as well as each 3^{rd} party application provider disposes of a contractual relationship with at least one network operator. The architectural challenge is a solution that allows users to exchange location information under the assumption that at least one user is roaming or even both users have contractual relationships to different network operators. In any case, the system provides the ability to exchange location information across different domains without the loss of privacy.

Figure 5 shows the proposed architecture. Compared to the system architecture depicted in Figure 1. this time several network operators located in different geographical areas provide their services to application providers. For the sake of clarity the following explanations refer to only two different network operators and applications.

Clients may directly access 3^{rd} party applications, no matter to which network the user is connected to. In order to be able to receive location information from users our architecture allows the recognition and translation of pseudonyms even over different service provider specific identity domains. This is archived through a virtual identity domain which passes assertions between the service providers. Compared to the definition of an identity domain of Jøsang (2005) where each identity in an identity domain is unique, we distinguish each domain rather by the respective network operator.

It is difficult to map our solution to commonly known identity management architectures. The used identifiers do not only represent identifiers but are at the same time the credentials that are necessary for verification. As the credentials are included in the identifiers or pseudonym they can also be denoted as "self verifying identifiers".

For the inter-domain exchange of location data we chose a centralised identity management architecture. Pseudonyms that are used in the visited domain are always forwarded to the home domain of the presentity for verification. The verification process is a simple matching procedure. If the pseudonym can not be found within the set of active pseudonyms this indicates either an unauthorized access or a synchronization error of the HMAC chain. In case of non matching pseudonyms an error notification is send back to the originator of the associated message which may then initiate the re-initialisation of the HMAC chain.

9.2 Message interaction

The following description of message interactions demonstrates the simple example when one user with device A asks for the location of another user with device B whereby user A roames in a different network.

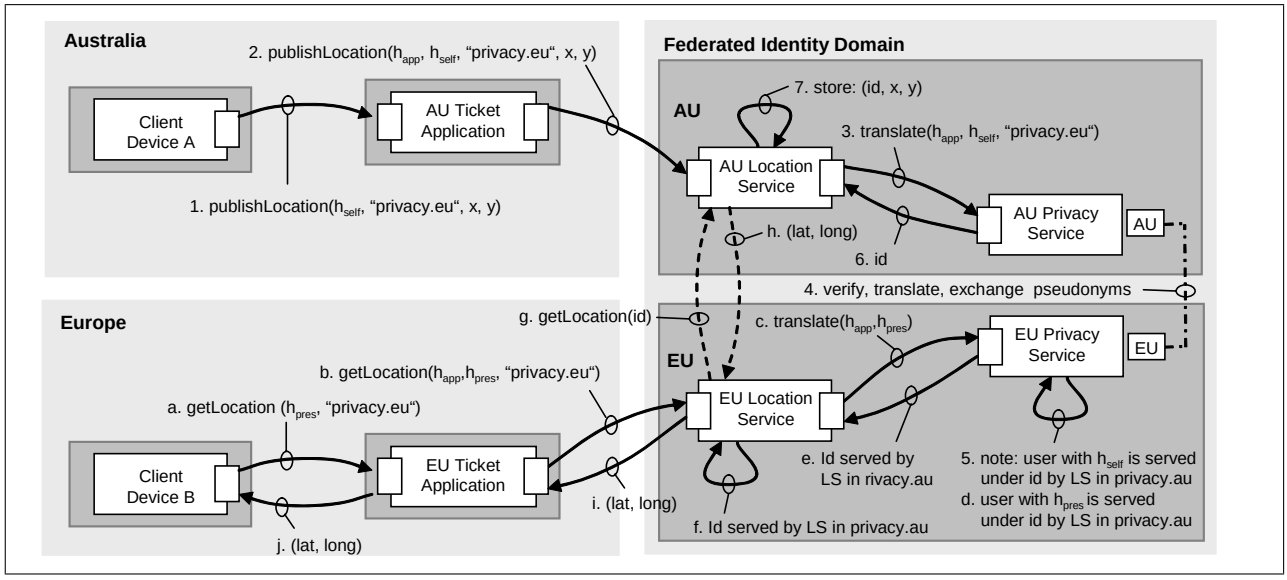

Figure 5: Federation of Identities: Management of Identities maintained in different domains

Publish Location

User A is located in the AU domain and wants to publish her current location. Therefore she sends her self identifying pseudonym h_{self} together with the coordinates received from the GPS module to the AU 3^{rd} party application (message 1. `publishLocation(`h_{self}`, "privacy.eu", x, y)`). Now, the AU application generates the next self identifying hash value h_{app} and sends it as part of the second message (`(`h_{app}`, `h_{self}`, "privacy.eu", x ,y)` to the AU location service which in turn forwards only the pseudonyms to the AU privacy service (message 3. `translate(`h_{app}`,`h_{self}`, "privacy.eu")`. If h_{app} is valid, the next step is the verification and translation of the user's pseudonym h_{self}. Since A's home network operator is located in the EU domain, the AU privacy service cannot verify and translate h_{self}. The users' home domain `"privacy.eu"` allows the AU privacy service to contact the EU privacy service (message 4.) which eventually verifies h_{self} and notes that user A is now served by the location service located in the domain of AU (see message 5). The AU privacy service receives the identifier `id` from the EU privacy service and sends this to the AU location service (message 6) where it is stored in association the users' location (message 7. `store(id, x, y)`).

Location Query

The transparent use of pseudonyms allows user `B` to query the location of user `A`. Thereby it is irrelevant in which network domain each client is.

As depicted in Figure 5, user `B` sends message a. `getLocation(`h_{pres}`)` to the EU application which forwards the contained pseudonym together with its self-identifying pseudonym h_{app} and the domain information `"privacy.eu"` to the EU location service (message b. `getLocation(`h_{app}`, `h_{pres}`, "privacy.eu")`). The EU location service requests the verification of the applications' hash value and the translation of the presentities' pseudonym from the EU privacy service by message c. (`translate(`h_{app}`, `h_{pres}`, "privacy.eu")`). After successful verification the result of the translation is returned to the EU location service. Since the location is stored by the location server in domain AU, the result is the `id` that denotes user `A` together with the note that the AU location service has recently received `A`'s location information (message e). The EU location service queries the AU location service for the position of user `A`. It sends the `id` in message g. `getLocation(id)` and finally receives `A`'s current location. Messages h. to j. propergate the coordinates of user `A` back to the requestor `B`.

Periodic Notification

In case user `B` wants to be notified about location changes in regular intervals, the AU location service notifies the EU location service periodically. When `A` stops to publish its location information, the AU location service deletes the stored location information after a predefined period of time. It may further inform the EU location server that it does not provide the location information of `A` anymore. Then, also the EU privacy service deletes the respective AU location service entries (messages 5. and d.).

10 Conclusion

In this paper we have described a solution for the exchange of location data of mobile users between different network operators which can also be viewed as independent of national borders. The proposed system architecture uses transaction pseudonyms to hide information that might reveal the user's identity and to assure that the user's requests cannot be linked.

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 in case users are roaming, we propose an architecture that not only incorporates easy to compute and flexible transaction pseudonyms for security and privacy assurance, but also allows the implementation of different kinds of location based services.

At the moment our system does not support privacy policies which allows users to decide under which condition location data can be accessed. Hence, one of the next steps will be the extension of the privacy service by a definition of appropriate privacy policies. We believe that the proposed architecture in combination with privacy policies and flexible mechanisms, such as the transaction pseudonyms which can also be implemented in mobile devices, represents a

This work was supported by the Austrian K*plus* program.

promising way to stimulate the development of novel location-based services.

References

Bellare M., Canetti R. & Krawczyk H. (1996), Keying Hash Functions for Message Authentication, In Koblitz, N., ed.: Advances in Cryptology CRYPTO 96, Volume 1109 of Lecture Notes in Computer Science, Springer-Verlag, 1996

Cheng, R., Zhang, Y., Bertino, E., & Prabhakar, S. (2006), Preserving User Location Privacy in Mobile Data Management Infrastructures, *in* 6th Workshop on Privacy Enhancing Technologies(PET'06), Cambridge, UK

CWA 15263 (2005), Analysis of Privacy Protection Technologies, Privacy- Enhancing Technologies (PET), Privacy Management Systems (PMS) and Identity Management systems (IMS), the Drivers thereof and the need for standardization, European Committee for Standardization (CEN), Brussels, 2005

Diffie W., & Helman M. (1976), New directions in cryptography. IEEE Transactions on Information Society, 22(6): 644–654, 1976.

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, 23 November 1995, Official Journal of the European Communities L 281 p. 31.

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), 12 July 2002, Official Journal of the European Communities L 201/37

Fischer-Hübner S., IT-Security and Privacy-Design and Use of Privacy-Enhancing Security Mechanisms, Springer Scientific Publishers, Lecture Notes of Computer Science, LNCS 1958, May 2001, ISBN 3-540-42142-4.

Gruteser, M. & Grunwald, D. (2003), Anonymous Usage of Location-Based Services Through Spatial and Temporal Cloaking, *in* Proceedings of The First ACM/USENIX International Conference on Mobile Systems, Applications, and Services (MobiSys), San Francisco, USA, pp. 31–42

Jorns, O., Jung, O., Gross, J. & Bessler, S., A Privacy Enhancement Mechanism for Location Based Service Architectures using Transaction Pseudonyms, TrustBus'05, Copenhagen, Denmark, 2005

Jøsang A., Fabre J., Hay B., Dalziel J. & Pope S., Trust Requirements in Identity Management, AISW2005, Australia, 2005

Jøsang A. & Pope S., User Centric Identity Management, Proceedings of the Asia Pacific Information Technology Security Conference, AusCERT2005, Australia, 2005

Junglas I. A & Spitzmüller C., A Research Model for Studying Privacy Concerns Pertaining to Location-Based Services, Proceedings of the 38th Hawaii International Conference on System Sciences, 2005. HICSS '05. 03-06 Jan. 2005 Page(s):180b - 180b

Kölsch 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

Lamport L.: Password Authentication with Insecure Communication, Communications of the ACM, vol. 24(11), 1981, pp. 770-772.

National Institute of Standards and Technology: Secure hash standard (SHS). Federal Information Processing Standards Publication 180-2, 2002

OMA (Open Mobile Alliance), Policy Evaluation, Enforcement and Management Requirements, Candidate V1.0, 12. June 2005

Parlay X 2.0, The Parlay X 2.0 specification, URL: http://www.parlay.org/en/specifications/

Pfitzmann, A., & Köhntopp, M., Anonymity, Unobservability and Pseudonymity – A Proposal for Terminology, Proceedings of Designing Privacy Enhancing Technologies: International Workshop on Design Issues in Anonymity and Unobservability, Lecture Notes in Computer Science (LNCS 2009, pp.1-9), Springer-Verlag, Berlin, Germany, 2001

Price Blane A., The Law is Not Enough: Legislation and Privacy Enhancing Technology for Location-Aware Computing, Workshop on Location Systems Privacy and Control, MobileHCI 2004, Glasgow, Scotland, 2004

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

Schulzrinne H., Tschofenig H., Morris J., Cuellar J. & Polk J., A Document Format for Expressing Privacy Preferences for Location Information, Internet-Draft, draft-ietf-geopriv-policy-08, 2006

Unni R., & Harmon R., (2003), Location-Based Services: Models for Strategy Development in M-Commerce, *in* Proceedings of the 2003 Management of Engineering and Technology, Technology Management for Reshaping the World (PICMET'03), Portland, Oregon, USA, 2003

Weiser M. (1991), The Computer for the Twenty-First Century, Scientific American, September 1991, pp. 94 - 100

Weiß, D., Krämer, I., Treu, G., & Küpper, A. (2006), Zone Services An Approach for Locationbased Data Collection, *in* Proceedings of The Third IEEE International Workshop on Mobile Commerce and Services (WMCS'06), IEEE, San Francisco, USA, pp. 504–511

Wu C. & Mei H. (2005), Location-Based-Service Roaming based on Web Services, *in* Proceedings of The 19th IEEE International Conference on Advanced Information Networking and Applications (AINA'05), IEEE, Taiwan

Yee G. (2005), Using Privacy Policies to Protect Privacy in UBICOMP, *in* Proceedings of The 19th IEEE International Conference on Advanced Information Networking and Applications (AINA'05), IEEE, Taiwan