

Privacy and Security in Location-Based Systems With Spatial Models

Christian Hauser

Institute of Communication Networks and Computer Engineering

University of Stuttgart, Germany

hauser@ind.uni-stuttgart.de

Location-Based Systems are systems, that take a user's current position into account for service provision. Famous examples are services like finding the nearest Italian restaurant or navigation from the user's current position to the desired destination. This kind of service is often announced as one of the so-called killer-applications for future mobile services.

In the project NEXUS, founded by the German Research Foundation, we are currently developing an open platform for spatially-aware applications to support location-based applications. The base of the platform is a spatial data model with information about the position of mobile and static objects and data from Geo-Information-Systems (GIS). This platform encompasses, e. g., a so-called Location Service which keeps track of mobile objects like persons, Spatial Model Servers wherein static objects are stored with GIS-information and some base services like an Event Service, which notifies a user on occasion of a preregistered event (e. g., on meeting of two persons). Using this platform it is easy to develop own applications like, e. g., a Child-Care service that keeps track of children while they are playing or a Navigation Service that computes the best (fastest, cheapest, ...) path using several means of transportation while skipping dark and lonely tracks. By development of this platform, we are directly faced with privacy and security problems of location-based systems and are concerned with different requirements of several participants (services, applications, users, communication systems, ...) at the same time.

Looking at threats to users' privacy it is obvious, that it is not only possible to use the position of mobile users for honest purposes. In the technical system, a location profile about the mobile user is emerging by the continuously updated position. Thereby the user's personal profile, like e.g. the service usage profile and possibly some monetary information, is enriched by the trace of its current position. The current position is an information which most users regard as very sensitive. This is not only visible from people's subjective fear about the complete surveillance by such systems, but also from the fact, that indeed the position of a user often lets infer its activity. One example could be the revelation of important company fusion dialogues by the position of managers. This danger will be risen by the fact, that spatial information, like GIS-data, will be broadly available in future, so that principally everybody can easily access context data of a geographic position and thereby can infer more information by knowledge of a user's position.

The danger of disclosed location information in a system already exists in today's mobile communication networks. Nevertheless, there are several aspects which are going to rise these threats in the future systems drafted above. The first aspect is granularity of location information. For many future location-based services to work well the users' positions must be known very exactly. Therefore, location information of different sensors will be aggregated in a Location Service to provide services with the best possible information.

A further aspect is the growth of in the system participating parties. As future systems tend to become open systems (because only by this a broad range of offered services can be achieved), there will be many different parties involved in service provisioning. This means that personal information is potentially known by many different service or content providers and today's trust model, wherein users just trust their mobile provider, e. g., not to disclose personal information do no longer hold. Contrarily, it is often going to be explicitly wished that (sensitive) location information is disclosed to third party service providers. Thus, propagation of personal information is difficult to control. This does not only require a sophisticated access control in the Location Service including an appropriate credential system, but also protection against parties, that want to enlarge their view of the user's profile maliciously by collaboration and aggregation of their respective knowledge about this user.

Nevertheless, a certain degree of interworking between providers will often be necessary for joint service provision. This problem of controlling propagation of personal information is even aggravated by the fact, that services can be provided in a cascaded manner by different providers. For example, the Event Service mentioned above, uses location data from the Location Service, which gathers the users' positions from a mobile network operator. This example shows that it is not trivial to see, which party is involved in a service provision and which party needs to know what (personal) information of the user and how malicious collaboration of the involved parties can be prohibited while still facilitating interworking of service and/or content providers. Thus, the system must

be partitioned in domains (e. g. services) that may know some personal information of a user and that are able to interwork with partners in other domains while still protecting the user's privacy needs.

How can these questions be addressed? As first basic measure, pseudonyms should be used and the user's real identity should be concealed whenever possible. As the disclosure of personal information in the context of a pseudonym is a monotonic process, the users should be enabled to use different pseudonyms. Thereby, different virtual identities (VIDs) of the user emerge in the context of the applied pseudonyms. Thus, a possible service can see the user only under one of its VIDs with the personal information, disclosed for the respective pseudonym. By this mechanism, users can tune their level of anonymity.

One challenge for future open systems like NEXUS thus is to accomplish the application of VIDs. In this context, trust models and attacker models gain on importance. The user has to choose carefully, towards which party he uses which VID and when he has to change this VID, on too much disclosed information in the VID's context. Another critical point of the usage of VIDs is the maintenance of system scalability in view of duplicated user contexts. It is, e. g., not clever to register each VID separately at the Location Service. Firstly, the scalability of the Location Service would suffer an exploding database and secondly the Location Service knows the link between the VIDs anyway, because of the exact similar position trace. Thus, a mechanism like proposed in [1] can be used, with which queries to all VIDs of a user can be linked by the Location Service on one single entry in its database. At the development of such mechanisms again trust models and attacker models must be taken into account carefully. If it would not be possible to trust the Location Service to a certain degree (because it is, e. g., provided by many different parties), it would not be possible to let it link all queries to different VIDs of a user.

A second challenge will become apparent when considering multilateral security. If users are only known by pseudonyms, questions about accountability and non-repudiation will be risen. Therefore, certification of specific confidence-building attributes to VIDs is going to be necessary. This does not only require a scalable certification scheme - like SPKI/SDSI [2] without central certification authority - but also a sound theoretical base for evaluation of (sometimes multiply) certified statements, like e. g. [3]. By reusing pseudonyms several times and certification of specific attributes by other parties, a user is enabled to build a reputation in its pseudonym, like e. g. the feedback profile of eBay [4].

Regarding the application of different VIDs it is a third challenge to accomplish non-linkability of these VIDs and the data disclosed by use of them. Primarily, the link to the user's identity has to be protected. Thereby, it is not sufficient to look at unique or even identifying data in the context of applications (like credit card numbers or position traces) but also in the context of communication systems. VIDs can, e. g., also be linked by concurrent IP addresses or MAC addresses.

As all these sketched measures are based on complex interrelations, it is not possible to demand from possible users to fully understand them and to behave in a clever way, what could render the measures ineffective. Therefore, intelligent user support by sophisticated tools, like e. g. an identity manager [5] is a further challenge.

- [1] **C. Hauser, M. Kabatnik:** *Towards privacy support in a global location service*, Proceedings of the IFIP Workshop on IP and ATM Traffic Management (WATM/EUNICE 2001), pp. 81-89, Paris, September 2001.
- [2] **C.M. Ellison, B. Frantz, B. Lampson, R. Rivest, B. Thomas, T. Ylonen:** *SPKI certificate theory*, IETF, RFC 2693, September 1999.
- [3] **Kohlas, R., Maurer, U.M.:** *Confidence valuation in a public-key infrastructure based on uncertain evidence*, Public Key Cryptography, 2000, pp. 93-112.
- [4] **eBay - The World's Online Marketplace:** www.ebay.com.
- [5] **U. Jendricke, D. Gerd tom Markotten:** *Usability meets security - the Identity-Manager as your personal security assistant for the Internet*, Proceedings of the 16th Annual Computer Security Applications Conference (ACSAC 2000), pp. 344-353, New Orleans, USA, December 2000.