Privacy Aspects of NEXUS

ABSTRACT

Regarding user acceptance of location-aware systems, privacy of personal data – especially location data – is of great importance. Therefore, security and privacy investigations are an important research topic in the NEXUS project. In this article, we give a short introduction to privacy issues and depict approaches for an access control within the Location Service, alleviating those.

Dipl.-Ing. Christian Hauser

Research Staff Member of the Institute of Communication Networks and Computer Engineering, University of Stuttgart
Address: IND, Universität Stuttgart,
Pfaffenwaldring 47, 70569 Stuttgart,
Germany
E-Mail: hauser@ind.uni-stuttgart.de

ZUSAMMENFASSUNG

Datenschutzaspekte von NEXUS
Um die Benutzerakzeptanz ortsbasierter Systeme zu gewärleisten, ist es wichtig, persönliche Information und insbesondere Ortsinformation zu schützen. Daher haben Sicherheits- und Datenschutzbetrachtungen in NEXUS einen hohen Stellenwert. In diesem Artikel führen wir in Datenschutzfragestellungen ein und leiten mögliche Realisierungen einer Zugriffskontrolle auf Ortsinformation der Benutzer ab, welche diesen Aspekten Rechnung tragen.

1 Privacy Aspects

Today, cellular telephone service operators, which already have some location information about their users, also offer a whole range of value added services, but are not allowed to reveal their location data to anybody else. Here, the user is obliged to trust this single provider regarding his personal data. In next generation scenarios, there will also be value added services provided by third parties, that must be able to access location data of users. Thus, users are forced to trust several providers instead of one. Moreover, in tomorrow's location-aware systems a well controlled disclosure of a user's position to distinct services or other users is required. Considering these requirements, today's trust models are no longer applicable but protection of personal user data is to be ensured.

Nevertheless, only considering users' privacy needs is not sufficient as service providers must also be protected against fraudulent users or malfunctioning applications or devices. Beyond that, a user can act as an information provider regarding his own location. Considering the privacy and security needs of users and providers, there will often be conflicts. They have to be resolved by negotiation between them, resulting in a compromise that satisfies all needs.

Regarding NEXUS from a security point of view, there are a lot of standard problems of distributed systems, e.g. confidentiality and integrity of communication or authentication of principals. Furthermore, not every information provider wants to make all of his information publicly accessible, thinking e.g. of sensitive indoor data residing on a Spatial Model Server like the location of safes.

2 Main Threat

Users are very sensitive when their personal data, especially their location, is revealed to (unknown) services. In fact, the users' fear of abuse of their location n is one of the main points of criticism of location-aware systems. Regarding the whole range of applicability of NEXUS, this fear is indeed understandable because a lot of personal data is exchanged. This permits the creation of exact user profiles. Especially, the activity of a user is often known, if his location is known. Even if the activity could only be imprecisely inferred, it already goes too far. For example, most people do not want to be seen in a dubious area even if the possibility of a straight walk through is well given. Furthermore, as this sensitive knowledge is part of an electronic system, a possible attacker does not need any complicated surveillance equipment, but just simple observations of a link or queries to a service, which can be done with a usual device. As knowledge of "who is located where" is the main new privacy problem imposed by NEXUS, we focus thereon in our privacy research.

3 Protection Approaches

In order to tune the usage of location information there are principally two possible parameters to be varied

- accuracy or resolution of location information
- amount of identity information known about a user

A first approach, which does not require any trust in the Location Service, reduces the accuracy of location data reported by the sensors and thus maintained by the Location Service. For reduction of accuracy of location information, several possibilities exist, like rounding or truncation of coordinates or the addition of a random error to the real position. The main drawback of this approach is that no instance can be authorized to attain more accurate location information. Thus, the general usability of the platform is reduced significantly.

A second approach can provide high accuracy of location data, while protecting the users' identity. Concealment of identity is more difficult, because it is not possible to do any numeric calculations on identity information and add, e.g. a random error. Instead, a user is not known to other parties by his real name, but he establishes several pseudonyms as identifiers, typically one pseudonym for each party he is in contact with. Additional information may be bound to each pseudonym, e.g. a customer number or a transaction code. By using different pseudonyms, it is aggravated, that different parties derive more information about the user by cooperation (see for details).

As the Location Service does not know the user's real identity, it can maintain very accurate location information. Thus, the accuracy of data disclosed to querying subjects must be controlled by tuning the second parameter mentioned, the accuracy of location information. Hence, this approach requires a more sophisticated access control of the Location Service than the first approach and the user's trust regarding the correct functionality of the Location Service.

In case a service issues a location query on behalf of a user, the rights of the original caller, i.e. the user of the service, must be considered for the access control decision.

Keeping the identity of users secret imposes the problem of accountability of actions. This can be alleviated by trusted third parties, which guarantee for the user's soundness.

This second approach is favorable because of its flexibility and better usability. Nevertheless, it can be combined with an overall reduction of accuracy like depicted in the first approach, if a user does not want to be located exactly by any subject.

4 Towards Privacy in NEXUS

As accurate location information in NEXUS is available due to several integrated sensor systems (see Infobox „Positioning Sensors") and as many services can benefit well from this accuracy, we maintain location information with the highest accuracy in the Location Service. Hence, according to the second approach, in case of a query this accuracy eventually has to be tuned down with respect to the access rights of the requesting subject.

Due to the open and global scope of NEXUS, a large number of participants and therefore a large number of location queries is expected. Moreover, relationships between users change frequently, invoking frequent change of access permissions. Therefore, the Location Service needs a scalable, dynamic and fast access control function.

Untraceability of a user's movement profile is one of the major design goals of our privacy architecture. This is achieved by pseudonymous usage of the Location Service, concealing the user's real identity. Hence, the Location Service knows a user's position with high accuracy but does not know the user's identity (principle of data economy). This lowers the necessary trust in the Location Service, which however still has to be trusted with respect to correct functionality, especially of the security functions. The NEXUS user has full control over disclosure of his data, i.e. nobody can get any location information without prior authorization by the user. Nevertheless, a user may give certain rights to an anonymous user, who is equivalent to the public.

A usual problem with security settings is that users find it difficult to understand their consequences. Hence, for preventing mistaken decisions, a user is supported by the client device displaying him exactly what is known about the other user, who wants to get access permissions, and what consequences a possible authorization will have.

5 Conclusions

Privacy of personal user data, especially location information, is a very important issue in location-aware systems, and is a prerequisite for user acceptance. In this article, we outlined privacy aspects of NEXUS, which most location-aware systems will have to deal with, too. A global Location Service needs a fast, scalable and dynamic access control. Moreover, it has to maintain most accurate location information for allowing a flexible use of the platform. This however requires pseudonymous usage of the Location Service, as we want to prevent linkage of users' identity and position.

Within NEXUS we are developing a privacy architecture, which meets the derived requirements as well as improved methods for concealment of location information, to make the accuracy of disclosed location controllable. Moreover, we examine how services can cope with a low accuracy of location information, since these services operate best with most accurate information.

As exchange of information external to NEXUS, e.g. passing a card with the real identity, is always possible, we can just protect against threats imposed by the technical system NEXUS.

This article only focuses on the access control to location information. Apart from that, integrity of location information is another question, since it is always possible for a user to report malicious locations, e.g. by a bogus location sensor or by just not taking his location sensor with him. More generally, this is extensible to integrity of all data within NEXUS, e.g. the geographical data in the Spatial Model Servers, on which services operate.

References

[1] 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.