Towards a Unified Interface for Privacy Regulation-conformant Location-based Services

Jan Zibuschka, Tobias Scherner, Lothar Fritsch, Kai Rannenberg
Johann Wolfgang Goethe - University, Frankfurt, Germany

***Abstract* — In today's location based services, location information is still passed around using a multitude of provider- or device-dependent interfaces, which vary both in the data format used for encoding location information and in the amount of identity management parameters, such as policies or negotiation options, and their enforceability.**

We document the necessity of a unified interface and set of policies for controlling the distribution of location information, while presenting different applicable privacy enhancing techniques and deployment scenarios that would have to be supported.

***Index Terms* — Infrastructure, LBS, Middleware, Privacy.**

I. Motivation

This position paper will mainly discuss issues of privacy-supporting infrastructures, which support user's sovereignty by giving him control of his personal information using policies and negotiate between different players in todays and future LBS scenarios, where the involved parties tend to form complex, distributed value-creation networks.

At all times, when this data is made available to location based service providers, privacy requirements like data minimization and user consent apply. Business requirements, such as the requirement to run on low-end mobile devices, may have an additional impact.

The main features of the intermediary architecture we propose can be characterized as: Enable provider-independent development and deployment of privacy friendly LBSs based on a standardized interface.

II. Interoperability

A standardized interface for mediation of location information would allow tapping the network effect immanent in the distributed, multi-party LBS scenario. Mobile operator independence, roaming support, and the unified interface for service providers for easy deployment and migration seem to be viable business propositions in a fast-moving marketplace. Mobility between different services, location sources, involved market players, and applications seems beneficial from users' and service providers' perspective alike. From an ordinary user's point of view, cost effectiveness, synergy effects, and convenient service usage are major issues.

Additionally, location sources are not limited to mobile operators. Depending on use cases and available technology, location information may be aggregated from several sources employing technologies like GPS, Galileo, COO, WLAN, or from several mobile operators. This improves the accuracy of delivered location information [1], and might even become a requirement in a world of converging network technologies. However, involving an independent location intermediary may be seen as undermining privacy, requiring special care.

III. Identity Management Features

Location information is sensitive data, protected by several privacy regulations. At the very least, the user's consent has to be given, as dictated by the applicable EC directives [2, 3], and processed in a comprehensible fashion. Alas, the handling of such information calls for the integration of identity management components.

User-defined policies that express consent for the disclosure of information should be stored at the location source, e. g. the mobile device or the mobile operator. Depending on the deployment, additional policies may be stored at the intermediary, for example for additional per service privacy enhancements, and at the service provider, e. g. data handling obligations. Furthermore, the intermediary may offer the possibility to audit the user's transferred data.

More advanced privacy enhancing technologies, like temporal or spatial cloaking, mix zones [4], or sophisticated information-minimizing secure multiparty computation protocols might also be implemented, depending on the range and extensibility of the standard, the available resources, and the willingness of involved parties to implement more complex solutions. For maximum effectiveness, such a standard would probably have to value footprint – that is, the number of employing organisations, and reached users - above technical perfection, but would still need to offer meaningful security guarantees.

As it mediates the communication of the different parties, an intermediary (that is not deployed on the user's device) offers a limited anonymization of relayed traffic. This can act as a fallback in cases where the implementation of more elaborate measures (e.g. mixes) is impractical, for example because of restricted client hardware or infrastructure capabilities. However, it requires that the user trusts the intermediary, and will only offer meaningful security guarantees if the connections cannot be eavesdropped at the intermediary by one of the communicating parties. If

anonymous communication is available, the intermediary may serve as a rendezvous point for communicating parties [5].

Advanced cryptographic protocols like oblivious transfer have been proposed [6] for the privacy-friendly rendering of location-based services. However, a proxy based protocol still seems to have its merits, e.g. in a mobile scenario, when the bandwidth available between mobile operator and location-based service provider is much bigger than the available bandwidth between operator and mobile device. This performance issue may be fixed by running costly obfuscation protocols between mobile operator (who would be aware of the user's location anyway) and service provider.

IV. Deployment

While intermediary components generally act as middleware, separating the location source from the LBS provider, they don't have to be deployed by independent parties, but may also be deployed as components on the user's device, or on the mobile operator's systems.

But even when independent intermediaries are considered the central question remains: Which players will step up to take the role of intermediaries? We will briefly evaluate several possible configurations in this section.

1) *Users*: A user may deploy the intermediary on his client. This will minimize the exposure of his location information. However, to ensure tamper resistance, certification of data will have to be done directly by the device. This might require trusted components to make sure that security-critical information is not tampered with. Additionally, the service is more likely to contact the user directly in such a scenario, limiting anonymity.

2) *Mobile Operators*: A mobile operator might want to deploy the intermediary directly at one of its facilities.

Most functions of the intermediary, like policy handling, PETs and anonymization towards the service provider may be preserved. Additionally, the mobile operator is already aware of the user's location, so no additional information is spread, and independent yet potentially trustworthy enough to certify it.

However, as several advanced features of the intermediary, including the anonymous rendezvous functionality, depend on the separation of the participating parties, the organizational structure and potentially employed advanced protocols become a key element for security in this case.

3) *MVNOs*: Independent from both mobile operator and LBS service provider, MVNOs deal with customer relations, while a MO manages the underlying infrastructure technology. Interpreting identity management as part of customer relations makes a lot of sense, so MVNOs seem to be well positioned to run location intermediaries, at least when considering organizational structure.

V. Related Standardization Activities

Identity Management features are being discussed in a number of different standardization fora. The most comprehensive view on the different facets of identities and the different features of Identity Management can be found in the current draft of the "Framework for Identity Management (ISO/IEC WD 24760 [7]), that is being worked on in ISO/IEC JTC 1/SC 27 "IT Security Techniques". Especially the consideration of different identity concepts (beyond single-sign-on identities provisioned by one entity) and the identity corresponding life cycle (e.g. Identity choice, provisioning and enrolment, Binding identities with attributes, Identity certification, Identity change, Unbinding of attributes from identities, and Identity revocation) are relevant for this comprehensive approach. One can expect that the new SC 27 WG 5 "Identity Management and Privacy technologies" will complement this initiative with a framework and architecture for privacy technologies.

V. Outlook

Beyond a fixed deployment of identity management functionalities at user or service side, there is also the possibility of a market dominated by independent intermediaries that chose localization and connection options dynamically from a pool of available possibilities – for example, from several MOs and MVNOs – based on the users policies and preferences. Thus, dynamic party matching recommendations may be used to leverage network effects, building a market that offers ease-of-development and –deployment to service providers while preserving the users' privacy. This raises new requirements for identity management frameworks processing location information, but also presents a promising use case for advanced privacy-respecting features.

Acknowledgement

This work was supported by the IST PRIME project; however, it represents the view of the authors only.

REFERENCES

[1] T. Lindner, L. Fritsch, K. Plank, K. Rannenberg, „Exploitation of Public and Private WiFi Coverage for New Business Models", *Proceedings of the 4th IFIP Conference on E-Commerce, E-Business, and E-Government (I3E),* 2004.

[2] European Parliament, *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.* Luxembourg: 1995.

[3] European Parliament, *DIRECTIVE 2002/58/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).* Brussels: 2002.

[4] L. Fritsch, "Mind your Step! How Profiling Location reveals your Identity - and how you prepare for it", *2nd FIDIS Doctoral Consortium*, Santorin, Greece, 2006.

[5] T. Koelsch, L. Fritsch, M. Kohlweiss, D. Kesdogan, „Privacy for Profitable Location Based Services", *Proceedings of the 2nd Intl. Conference on Security in Pervasive Computing*, Lecture Notes on Computer Science (LNCS 3450, pp.164-179), Springer; Boppard, Germany, 2005.

[6] M. Kohlweiss, B. Gedrojc, "Flexible Location Based Service Protocols Using Efficient Oblivious Transfer", *Kryptowochenende*, 2006.

[7] ISO/IEC JTC 1/ SC 27 IT Security Techniques: 1st WD 24760: 2005-10-05: A framework for identity management.