Location-based Services: Privacy, Security and Assurance

Hugo JONKER [1], Sjouke MAUW and Jun PANG
University of Luxembourg, 6, rue Coudenhove-Kalergi, L-1359, Luxembourg

Abstract. In a straight-forward setup, location-based services have many trust assumptions amongst the involved parties. However, some of the parties may be honest while still being interested in learning confidential information, and others can have reasons to cheat where possible. Therefore, system design needs to account for a less than perfect setting. Research in this area is currently focused on reducing the necessary amount of trust required by improving security, privacy and assurance of these systems. This paper provides an introduction to the field.

Keywords. Location-based services, tracking, privacy, security, assurance, localization accuracy, multi-cell ID.

Introduction

In the last decade, determining location has transitioned from a niche application for a select group to a ubiquitous application for the general public: nowadays, the average smart phone incorporates location technology.

Location determination systems consist of multiple components: various signal-emitting stations whose locations are well-known, and a receiving user device. The stations can be satellites, such as used in the GPS, GLONASS, and Beidou systems (the Russian and Chinese counterparts to GPS). Satellite-based location systems are collectively referred to as Global Navigation Satellite System (GNSS).

Another possibility is to use terrestrial stations. The rise of wireless technology led to the spread of fixed antennas at known locations over much of the globe. It was recognised that these can be used to determine location. As wireless networks are becoming more and more dense, the number of antennas rises and thus the resolution of these methods is steadily improving. There are various techniques to determine location, including Cell ID (which cell phone antenna is the device connected to), triangulation by the antennas, or triangulation by the location device. Note that these techniques are not limited to cell phone networks; they can (and are) also being used to determine location based on proximity to known WiFi networks.

Location technology caters to a widespread demand. Information on current whereabouts is needed to answer questions frequently encountered while in unfamiliar surroundings, such as route planning, finding the nearest bus stop, finding nearby restaurants, providing directions to be picked up, local weather conditions. In the early days

[1] Corresponding author. E-mail: `hugo.jonker@uni.lu`

of location determination, the technology only provided current location. The user then would combine this with other information (maps, national weather forecasts, etc.) to answer her queries. The first evolution was to cater for route planning, by including maps in the user device. This further evolved to include constant updates affecting route planning (traffic jams, speeding checks, etc.), delivered wirelessly. Route planning addresses one of the questions people have on their current whereabouts.

As access to location technology became more and more ubiquitous, the next evolution in this field was to increasingly support other questions, leading to the development of location-based services (LBS). A location-based service is a service that determines the location of a mobile device and uses this to provide functionalities and information specific to that location. A variety of location-based services has emerged, including route planning, local weather reports and forecasts, information on nearby public transport, usage-based road pricing, tracking, etc.

With the growth of the importance and of the audience of location-based services, questions of security and privacy are brought forward. Initially, only a handful of parties were involved in determining a user's location, and security focused on protection from outsiders. As services are being built on top of this technology, the number of parties increases significantly, and the possibility of a malicious insider (or a misbehaving insider) emerges. The extent to which the parties care to trust each other has reduced, and trust amongst the various parties can no longer be assumed by a location-based service. An attacker may try to steal a service (e.g., claiming to be a client to get free internet access), service providers may gain of private information on user's movements (e.g., determine your preferred shopping areas), and users may lie about their whereabouts (e.g. to lower taxes due in a road pricing scheme).

This decrease of trust needs to be balanced. The dependency on trust can be replaced by adequate safeguards of security and privacy. In this fashion, there is a desire to shift from needing trust towards using security controls. Making this shift possible is currently the focus of research in location-based services. In order to get a better understanding of these trust-related developments, we provide an overview of the challenges concerning security, assurance and privacy in location-based services.

Structure of the chapter. The rest of this chapter is structured as follows. In Section **??** we perform a brief stakeholder analysis in order to motivate the security needs of the involved parties. Section **??** illustrates security, privacy and assurance concerns of location-based services.

1. Stakeholders, incentives, security needs, and adversaries

In this section we introduce the main roles involved in location-based services and describe the relationships amongst them. Knowing the roles, their incentives and the trust relations between the roles helps in understanding the relevant security problems. This analysis basically follows the approach from [**?**], which was based on a variety of methodologies, including domain analysis [**?**] and stakeholder analysis [**?**].

1.1. Stakeholders

We consider three stakeholders: the Location Provider (LP), the User, and the Location-Based Service Provider. Location-based services are built on top of location-providing services. In location providing, a User interacts with a location provider to determine her location. A location-based service provider then interacts with the user to provide location-specific services.

1.2. Incentives

In order to formulate the security needs of these roles, we study their incentives. This gives rise to the desired functionality of the system, from which security requirements that ensure this functionality follow.

- **Location Provider:** The LP wishes to advance its goals. LPs can be either commercial or governmental (providing a public service). Hence, the main incentive for an LP is either to monetize its service (commercial providers) or to provide a public service (governmental provider).
- **User:** People perform many daily tasks whose execution can be enhanced given knowledge of current local conditions (e.g. weather, nearest open restaurant, traffic density). Such local conditions depend on a user's location, but knowing a user's location is not sufficient to derive such knowledge. Location-based services provide users with the desired knowledge about their local conditions, based on their location. This acquisition of relevant knowledge about local conditions forms the main incentive for using location-based services.
- **Location-Based Service:** The incentive of LBS providers is to make profit. There are various ways to achieve this. We make the following distinction:

  ∗ *Directly*: The LBS sells its location-based service to users. For example, road pricing, or a paid service for tracking your children.
  ∗ *Indirectly*: The LBS indirectly profits from offering its services for free to the public. In this case, the LBS supports and augments an existing business model. Examples include a real-time, location-aware route planner for public transport, and services such as Google Maps, that profile users to better sell advertisement space.

1.3. Security needs

Having established the key incentives for each role, we refine these into security needs.

- **Location Provider:** For both categories, a minimal level of quality of service is essential. This implies a certain level of integrity and availability of the service. To support the monetization of its service, the commercial location provider requires *secure handling of payments* and *no theft of service* – access to the service should only be possible via licensed applications/devices.
- **User:** The security requirements of a user follow from her main incentive, which is to make effective use of location based services. This implies availability, integrity and accuracy of the provided service. As location information supports this process, the user has implicit security requirements on this data, viz. *integrity, availability and precision of location data*. In addition, if the user is billed for the service, she requires this billing process to be secure and in accordance with her usage.

- **Location-Based Service Provider:** To make profit, the provider requires protection of the business model. This entails requirements such as *secure handling of payments*, *no theft of service*, and *no leakage of business-criticial data*. As an example of the latter, consider a service to request a cab at your current location. Such requests must be confidential from competing taxi companies.
  In addition to the requirement to protect the business model, note that the usability of the service depends on the quality of the service offered. This quality depends on the quality of the location data. Therefore, the location-based service provider has the following requirements on the location data: *integrity, availability and precision of location data*. Note that, in case of non-anonymous services (e.g. tracking), the service additionally requires *authentication* of the user.

Confidentiality	*Integrity*	*Availability*
● of location data ● of user data (*address*) ● of business-critical data (*encryption keys*) ● of payment data (*credit card number*) ● of service usage (*escort service*)	● of location determination (*no location faking*) ● of location-based service (*no replay of old query's response*) ● of payment ● No theft-of-service (*no license-incompliant service resale*)	● of location determination (*no jamming*) ● of location-based service (*no DoS attack*) ● of payment infrastructure

Table 1. Mapping LBS security needs to the CIA triad.

The incentives-driven approach identifies security needs that ensure the functionality of the system. As privacy is *not* a functional requirement of the system, the above approach does not uncover privacy concerns. Therefore, we extend these security needs with the typical privacy needs of the parties involved.

These privacy needs, together with the high-level security needs listed above, relate to the traditional security classification of Confidentiality, Integrity and Availability (the CIA triad) as shown in Table **??**. For the non-obvious entries, an example is provided.

Note that both the user and the LBS provider have a security need for the assurance of location data, which is also evident in the CIA mapping of the needs. This requirement should be examined on its own, as location-based services depend on the correctness of the provided location data. One approach to achieve assurance, put forth by Harpes et al. [**?**], is to introduce a new role: the **Location Assurance Provider**. This role is charged with fullfilling these location assurance requirements, e.g. by certifying location data.

Consequently, we consider the following requirements classes of the identified security needs: security, assurance, and privacy.

1.4. The adversaries

The normal adversary in a security setting is an external attacker that can inspect, insert, alter and block any and all messages on the network. However, this traditional "external attacker" model is insufficient in this setting, as stakeholders have incentives to cheat.

Location Provider: the main threat coming from the location provider is the possibility of misdirection. He may send out false location information as to mislead the user. In this way, he can, for example, down an enemy plane. This is claimed[2] to be the cause of the recent Irani capture of a US droid. This threat is rather exotic and of limited interest to regular users.

User: for a user, the main incentive to cheat is to save money or effort in obtaining the required services. An example is to reduce transportation costs by lying to a road pricing service. In addition, privacy-aware users may cheat to mask their actual location, while still using a service.

LBS provider: the LBS provider may want to reduce expenses or increase profits. Since maintaining a database of current, accurate location information is expensive, they can reduce expenses by offering an inaccurate view. The can increase their profits by offering a biased view. For instance, a shop-opening hours LBS that offers the top spot to the highest paying supermarket (instead of the one nearest to the user).

Location Assurance provider: the main reason for the location assurance provider to cheat is out of curiosity. With an *honest-but-curious* approach, the LAP may perform the required tasks in a trustworthy way, while still being able to acquire confidential data about the User or LBS' operations.

In addition to these adversaries, one also has to consider that malware or spyware has infiltrated any of the roles.

2. Illustrating security, assurance, and privacy

In this section we will focus on the three identified requirements classes. Each category is illustrated by discussing a typical example.

2.1. Security: preventing theft-of-service

Standard security requirements, such as agent authentication, have been studied in several domains and standard cryptographic solutions have been developed. However, more complex requirements such as *no theft-of-service* require a domain-dependent approach. Below, we take a brief look at this particular requirement for location-based services.

Theft-of-service occurs when a service is used without compensation. Note that "theft", in this case, is not intended in a legal sense, but in the view of the service provider. Hence, preventing theft-of-service entails not only preventing anyone from accessing the service without proper payment, but also preventing anyone from acting as a proxy for the service.

For example, consider an (imaginary) forecast service FoCa. This service provides accurate weather forecasts for the user's current whereabouts. By using traditional security-enhancing mechanisms such as encryption and authentication, the service can ensure that all its users are paying. However, this still leaves open an avenue for attack: since the results (forecasts) are valid for some time, they can be resold. A user could set up a business where he resells previously collected results. In particular: Eve could buy forecasts for various locations, and then sell these on to her own users at a lower cost.

[2] `http://www.csmonitor.com/World/Middle-East/2011/1215/Exclusive-Iran-hijacked-US-drone-says-Iranian-engineer-Video`

This allows Eve to make profit for each area with more than one user in it, without any knowledge or skills in weather forecasting.

Such service abuse is clearly not in the interests of FoCa. Clearly, Eve does need the FoCa service to continue, as she cannot provide weather forecasts by herself. The goal for FoCa is to prevent such misappropriation of her services.

This problem is very similar to the problem of preventing the copying of digital content. In that field, several approaches (e.g. [**?**]) consider the use of trusted devices, and tie the sold content to the device involved in buying the content. This Digital Rights Management (DRM) approach was largely abandoned due to (amongst others) strong consumer opposition. However, a service is different from content: once bought, a service is delivered once. Thus, in this case, protection of the intellectual property of the location-based service provider may be acceptable for the general public. Consequently, a simple, DRM-like service may address the theft-of-service problem.

Remark that such an approach requires that the service provider encrypts the data for each specific user, even if the data encrypted is relatively slow-changing (e.g., weather forecasts may be valid for 24 hours). This means that the service provider has to perform some additional processing for every request. Moreover, the straightforward DRM approach – encrypting the data for a specific device – has obvious privacy implications. An interesting challenge related to theft-of-service is therefore the design of solutions that provide protection from theft-of-service at a reduced processing cost, as well as solutions that allow for a sufficient level of user privacy – e.g. by binding a specific instance of the service to a specific location [**?**].

2.2. Assurance: preventing location faking

While fake and redirected signals are a common topic of study in many fields, the importance of accurate and reliable location data for location-based services merits a special focus hereon. Assuming communication integrity is preserved via standard cryptographic techniques, location claims can be either correct (Fig. **??**a) or incorrect for any of the following reasons:

- The location device lied (Fig. **??**b).
- Location data received by the location device was relayed (*meaconing*, Fig. **??**c).
- The location data received by the location device was faked (Fig. **??**d).

An attack that overrides the genuine signal can be carried out by the owner of the device or by an outside attacker. Unlike the outside attacker, the owner can bypass the antenna and directly feed whatever bits and bytes are required to spoof the location. An outside attacker has a far harder time: in the case of GPS, contact with several satellites is established. To correctly spoof a location, the attacker must fake multiple satellite signals from different directions.

Note the difference between meaconing and overriding: in meaconing, the location device does receive a genuine location signal, but that signal was relayed. In overriding, there is no genuine location signal.

Standard ways to detect faked data (e.g., signing) are not applicable to GPS positioning, because the GPS signals do not support satellite authentication for civil applications. In particular, it is hard to detect whether a signal was relayed. Several authors propose a number of counter measures against signal spoofing attacks, such as monitoring the

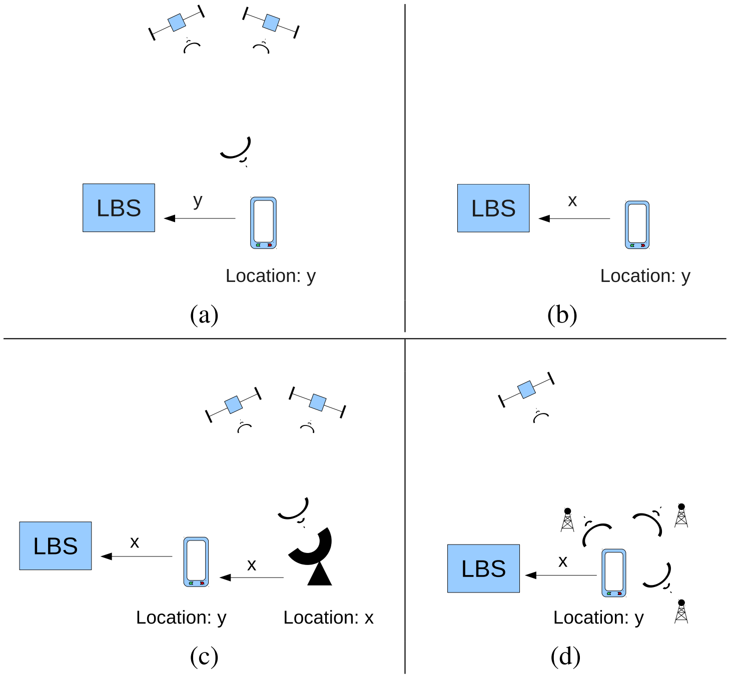

Figure 1. Faking location: (a) correct working; (b) lying device; (c) meaconing; (d) overriding.

signal strength, the satellite constellation, and the difference between the receiver's clock and the satellite's clock [**?**,**?**,**?**].

Faced with these attacks, ensuring quality of the location data is not easy. Differences between a genuine signal and a spoofed one are infinitesmal. However, if location data can be faked, then the foundation upon which location-based services operate is undermined. Incorrect location data can even lead to damage, for example in case of a public transport app that misinforms its user – who will likely find another means of transportation. Making the most of these tiny differences in order to judge veracity of the claimed location is an open and important topic in location-based service security.

2.3. Privacy: privacy in road pricing

Privacy concerns arise when a party can learn a specific property of an individual, e.g., that he/she visited a particular hospital. In general, there are three ways to preserve privacy:

- Hide the individual,
  e.g. by anonymizing data. Data anonymization sounds good in isolation, but data does not exist in a vacuum. Narayan and Shmatikov dramatically illustrated [**?**] this by deanonymizing a large set of anonymized data using publicly available additional data.
- Hide the property,
  e.g. by leaving some uncertainty. Instead of giving a location with a precision of one meter, return a location with a precision of one hundred meters (see e.g. [**?**]).

- Hide the link between individual and property,
  e.g. in voting systems, the ballot box hides the link between voter and vote.

With respect to hiding a property we remark that location-based services usually consider a particular location *at a particular time*. Thus, in some cases privacy is sufficiently preserved if either location or time of the request is obscured.

As an example of privacy issues in location-based services, we consider road pricing. Road pricing, as a location-based service, tracks where users drive by means of a device inside their vehicles. The user is then charged based on how much, where and when she has driven. The appeal of electronic road pricing is that it allows for fine-grained pricing control – a user who drives 20,000 km per year pays more than one who drives 2,000 km, highways can be made more expensive than small roads, and rush hour can be made more expensive than off-peak hours. Thus, in addition to enabling fairer distribution of costs, road pricing can be used to provide incentives to improve distribution of road usage.

To properly compute the due fee, the fee for every road that was used is added. Thus, the roads the driver used (stored in the user device) must be combined with their pricing (available at the taxing agency). This can be done by:

- The taxing agency.
  While this will satisfy the fairness requirement, it also obviously and completely violates privacy of the driver.
- The driver's location device.
  If the driver controls the device, this is an open invitation to fraud. Out of necessity, this option thus assumes that the device is trusted. Morover, the device must be augmented with a database of road prices and the ability to compute the total fee due (see e.g. [**?**,**?**]).
- A trusted third party.
  A third party can act as a "privacy proxy" for drivers, along the lines of the anonymity server in [**?**]. This approach addresses the privacy issues stated above by replacing them with trust assumptions.

Letting any one party compute the fee due poses either a privacy risk or a security risk. Hence, a logical approach is to compute the fee through a combined effort of these parties. An interesting question is how to let multiple parties jointly compute the fee, using secure multiparty computations (e.g., [**?**]).

3. Conclusion

The growing availability and ever-increasing accessibility of location technology provides a fertile ground for location-based services. To grow further, security, privacy and assurance of location-based services must be ensured. Distinguishing assurance and privacy from security is relevant, since violations of the former two properties impact the (perceived) quality of the service, not its operation. Neither privacy, nor assurance in location-based services is sufficiently well understood and further study of these topics is necessary.

Research into the area of location-based services is fairly new and hence there are many open research questions. The main initial goals are to establish precise definitions of requirements, to develop methods to validate these definitions, and to develop methods to verify adherence to these definitions.

Above, the security-related subject *no-theft-of-service* was already discussed. This is but one of many questions related to the correct functioning of an LBS system in a hostile environment. Examples of other security-related questions are "which protocols enable road pricing?" and "which cryptographical primitives can be used to support road pricing protocols?"

With respect to assurance, the most important subject is prevention of location spoofing. Addressing this involves investigating various questions, such as: which physical characteristics of a satellite signal are relevant and hard to spoof (and therefore, conducive to establish authenticity of the signal)? How to merge various diverse indications on the authenticity of a signal into a judgment on its authenticity? How can spoofed wireless communication networks be detected?

Concerning privacy, the question of how to achieve some level of location privacy while enabling tracking (of objects or persons), is still an open question. Some techniques from road pricing systems carry over to the tracking domain, but the problem is sufficiently different to warrant further investigation. Moreover, privacy is not binary (yes/no), but has a statistical nature: how much is known about an individual? As location-based services are used, location information is retained and aggregated. An adversary can still learn information about the individuals via a statistical analysis, even if the data were anonymized. It is interesting to study the notion of differential privacy [**?**] to provide statistical guarantees for location privacy.

Finally, we consider design of new functionalities, such as group location and ownership transfer. Group location is the problem of locating/tracking a group of products. For instance, do not track the truck, but only its cargo. The question isn't merely locating or tracking a set of items, but locating the whole set, that is, a set of items which are all "close" to one another (for a suitable definition of "close"). Ownership transfer is the problem of changing ownership of an object that is being tracked. More precisely, if a tracked object changes owner, forward and backward privacy should be satisfied. That means that after the transfer, the old owner is no longer capable of tracking the object and the new owner cannot track the object's location to before the transfer.

References

[1] G. Lenzini, S. Mauw, and J. Pang. Selective location blinding using hash chains. In *Proc. 19th Workshop in Security Protocols*, LNCS 7114, pp.132-141. Springer-Verlag, 2011.

[2] A. Blumberg and R. Chase. Congestion pricing that respects "driver privacy". In *Proc. 8th IEEE Intelligent Transportation Systems Conference*, 2005.

[3] C. Harpes, B. Jager, B., and B. Gent. Secure localisation with location assurance provider. In *Proc. European Navigation Conference - Global Navigation Satellite Systems*. 2009.

[4] J. Balasch, A. Rial, C. Troncoso, B. Preneel, I. Verbauwhede, and C. Geuens: PrETP: Privacy-preserving electronic toll pricing. In *Proc. 2010 USENIX Security Symposium*, pages 63–78. Usenix Association. 2010.

[5] H.L. Jonker and S. Mauw. Discovering the core security requirements of DRM systems by means of objective trees. In *Handbook of research on secure multimedia distribution (Shiguo Lian and Yan Zhang, eds.)*, pages 71–85. IGI Global publications. 2009.

[6] R. Prieto-Digitalaz. Domain analysis: An introduction. *Software Engineering Notes*, 15(2), 47-54. 1990.

[7] A. Pouloudi. Aspects of the stakeholder concept and their implications for information systems development. In *Proc. 32nd Hawaii International Conference on System Sciences*, IEEE Computer Society Press. 1999.

[8] B.C. Popescu, F.L.A.J. Kamperman, B. Crispo, and A. S. Tanenbaum. A DRM security architecture for home networks. In *Proc. 4th ACM Workshop on Digital Rights Management*, pages 1–10. ACM. 2004.

[9] C. Troncoso, G. Danezis, E. Kosta, and B. Preneel. PriPAYD: Privacy friendly pay-as-you-drive insurance. In *Proc. 2007 ACM Workshop on Privacy in Electronic Society 2007*, pages 99–107. ACM. 2007.

[10] M. Gruteser and D. Grunwald. Anonymous usage of location-based services through spatial and temporal cloaking. In *Proc. 1st Conference on Mobile Systems, Applications and Services*, pages 31–42. ACM. 2003.

[11] J.S. Warne, and R.G. Johnston. GPS spoofing countermeasures, *Homeland Security Journal*, December 2003.

[12] A. Narayanan and V. Shmatikov. Robust de-anonymization of large sparse datasets. In *Proc. 29th IEEE Symposium on Security and Privacy*, pages 111-125. IEEE Computer Society. 2008.

[13] T. Mundt Two methods of authenticated positioning. In *Proc. 2nd ACM Workshop on Q2S and Security for Wireless and Mobile Networks*, pages 25-32. ACM. 2005.

[14] A. Al-Fuqaha and O. Al-Ibrahim. Geo-encryption protocol for mobile network. *Computer Communications*, 30(11-12): 2510-2517. 2007.

[15] H. Wen, P. Yih-Ru Huang, J. Dyer, A. Archinal, and J. Fagan Countermeasures for GPS signal spoofing. In *Proc. ION GNSS 2005*, pages 1285-1290, 2005.

[16] C. Dwork. Differential privacy. In *Proc. 33rd International Colloquium on Automata, Languages and Programming*, LNCS 4052, pp. 1-12. Springer.