Using constraints to protect personal location information

Anand S. Gajparia
Chris J. Mitchell
Information Security Group,
Royal Holloway, University of London,
Egham, Surrey TW20 0EX, UK.
Email: {a.gajparia,c.mitchell}@rhul.ac.uk

Chan Yeun
Toshiba Research Europe Limited.
Telecommunications Research Laboratory,
32 Queen Square, Bristol, BS1 4ND, UK.
Email: chan.yeun@toshiba-trel.com

Abstract— **This paper assesses the possible use of constraints to control the dissemination and use of location information (LI) within a location based service architecture. The various types of constraint which may by required are also considered. Finally, issues and risks with the possible use of constraints are discussed, as are possible solutions to these hazards.**

I. Introduction

As devices used for wireless communication become increasingly ubiquitous and mobile, it is becoming apparent that location based services will play an important role in the evolution of ambient networking. Location based services use location information (LI) to allow an LI subject (the entity concerning which LI is being created) or some other entity to exploit this information to support the provision of one or more services. These range from allowing an emergency service to locate an LI subject, as is the case with E911 in North America [1], to an authentication service based on the location of an LI subject [2]. Location based services are also likely to play a significant role as a vehicular technology [3], including the support of navigational services and toll schemes.

Current technologies which may be used to generate LI include various forms of Global Positioning System (GPS) and Enhanced Observed Time Difference (EOTD) technologies [4]. GPS uses satellites to enable the calculation of the LI of an LI subject. EOTD calculates LI by observing time differences in transmissions between a user device and a base station.

Unfortunately, LI may also be used for malicious purposes. For example, an entity could use LI to stalk an LI subject. Securing the privacy of LI is an issue which needs to be addressed in order to gain the trust of the mass market for such services. Intuitively, privacy of LI can only be gained by limiting its distribution. This would mean that only those authorised by the LI subject would be able to gain possession of LI. With this in mind, this paper introduces LI constraints as a means of allowing an LI subject to exert control over the distribution of its LI. In the context of this paper, LI constraints are simply rules associated with a specific piece or set of LI, restricting the ways in which the associated LI may be used and/or disseminated. To be effective, the constraints must be bound to the associated LI, typically by cryptographic means when the LI is in transit and by access control techniques for stored LI.

LI constraints can be used to help manage the use and distribution of LI. We investigate the possible constraint requirements which an LI subject may have, and discuss how these may be fulfilled. By looking at various uses for LI we investigate restrictions which may be placed on these uses. We look at the limitations which can be placed on the distribution of LI and how responsibility might be determined when LI constraints are abused. Constraints may also be placed on the storage of LI, whereby an LI subject may be able to limit the amount of time for which an entity can hold LI.

The limitations of using constraints to control LI are also studied. Although constraints may allow an end user to have some degree of control over its LI, placing constraints on LI also allows an entity to gain additional knowledge about the LI subject. For example, in order to place storage constraints on LI, time stamps [5, p3] may be used to limit the length of time that an entity is permitted to store the associated LI. However, this mechanism also poses a risk, since placing a time stamp on LI might allow receiving entities to learn the time that the LI subject was at a particular location. We discuss an alternative mechanism which involves recording the time at which LI expires, instead of using a timestamp and duration.

Statements about where LI is not to be distributed give the receiving entity knowledge about entities which the LI subject may have an aversion to. Contrariwise, statements about where LI can be distributed and ways in which it can be used may also give information about services which an LI subject uses.

The paper concludes by looking at further work which may aid the wider use of location based services. We discuss the advantages of using a standardised language for describing constraints and LI, and briefly look at a possible candidate for such a language, namely XML.

II. A model for the use of LI

A. The roles

This section defines the entities involved in a location based service architecture. It also describes the relationships between the different entities. The entities and their relationships in the special case of a mobile User Device are shown diagrammatically in Figure 1.

- **LI subject.** An LI subject is the entity about whom location information is being gathered, managed and used. This entity is most commonly a human user.
- **Malicious Party** This is an entity with malicious intent. A malicious party may act as a threat to the confidentiality, integrity or availability of LI for one or more LI subjects.
- **User Device (UD).** This entity is a device with which the LI subject may interact, e.g. to invoke a location based service. Such a device may either be static, e.g. a desk top computer, or more typically mobile, such as a mobile phone or Personal Digital Assistant (PDA). It is, in fact, this device regarding which LI is generated rather than the user him/herself, since there is typically no way to directly measure the location of individuals. Thus this entity is a key part of the model.
- **Location Information (LI).** This is data which provides information regarding an LI subject's location. LI may occur in many forms. In general, we can divide LI into two types, namely *Inferred* LI and *Actual* LI. Actual LI refers to a directly calculated geographical location. This type of data indicates, to some degree of accuracy, the physical location of an LI subject. Inferred LI is, by contrast, obtained by implication. For example, if a user is present on a network, this implies that they are likely to be within an certain vicinity, although no specific calculation of geographical LI has taken place.
- **LI gatherer.** This is an entity which gathers or possesses LI about an LI subject. A GPS receiver is an example of an LI gatherer, as it obtains location data. An entity in a GSM network which keeps signalling data for a UD is also an example of a LI gatherer. Although a GSM network does not normally pass on this LI (except in certain special cases), it certainly possesses such information, and could, in an appropriate environment, be a valuable source of LI for commercial use.
- **Location Based Service (LBS).** This is a service based on LI, e.g. a vehicular navigation service.
- **LBS directory.** This entity provides information regarding LBSs which are available for use to a particular user. The LBS directory may itself use LI regarding the service consumer when providing the service. For example, it may show a service requestor lists of LBS providers providing information about particular types of retail premises in the area of the requester.
- **Network Entity.** This is a component which provides a network service to a UD. Two important types of Network Entity are the local base station which provides network access to the UD, and the UD's 'home network' with whom the UD owner has a contract and charging arrangement for the provision of network services.
- **Regulator/Legal authority.** This is an entity which exerts legal or regulatory control over the management and use of LI. This includes telecommunications regulators, data privacy authorities, law enforcement bodies, and auditors.

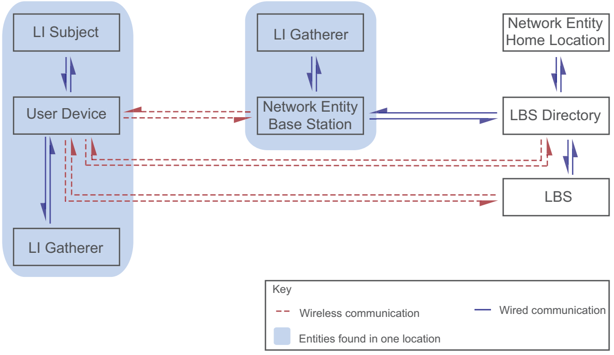

Fig. 1. Mobile scenario for location-based service provision

B. LI abuse

This document discusses the use of constraints to limit the abuse of LI. When we talk about the abuse of LI constraints, we define this as *any use, distribution or storage of LI which contradicts the rules defined by the constraints.* We also assume that the LI, together with the constraints, is transmitted and stored in a secure manner. By this we mean that the receiving entity has been authenticated by the sender, that LI confidentiality and integrity are not compromised during transmission, and that the LI constraints are securely bound to the LI.

III. Using constraints with LI

In order to set constraints on LI we must first look at how an LI subject may want to restrict the use and distribution of LI. In addition, these constraints should be in some common format which is automatically processable.

A. Constraint types

This section looks at the types of LI constraint which may be required.

1) Storage time constraints: Storage time constraints may be used to limit the duration that an entity can store LI. This can be done in two ways.

One way is by the use of time stamps. A time stamp can be used to record the time of creation or the existence of information [5, p3]. By adding a validity period a statement can be made that an entity should not hold LI subsequent to its expiry. For example, the LI subject may state that an entity cannot use LI once one hour after the time set by the time stamp has elapsed. The use of time stamps requires additional security mechanisms. Time stamp protocols require synchronisation and secure time clocks [5, p3]. Also, there should be secure mechanisms to obtain them. The fields needed for such a constraint would be the issue date/time and the validity period.

Another way of adding time constraints to LI is by stating the time at which LI expires. This may be in the form of a date and time after which LI cannot be held. This would eliminate the need for a secure time stamp. The entity receiving LI will, however, need access to a secure clock in order to learn when LI is invalid. The field necessary for this scheme would be the expiry date/time.

2) Distribution constraints: The LI subject may also want to constrain the distribution of LI. Distribution constraints can be specified inclusively or exclusively. Inclusive constraints would show the entities who are permitted to possess LI. Exclusive constraints would show the entities who are not permitted to possess LI.

Consideration should also be made with regard to the way in which LI distribution is managed, and which entity is accountable for misuse of LI. This could be the entity which sends LI to an entity who is not permitted to receive it, or it could be the entity which receives and then stores LI when it is not permitted. Of course having both sender and receiver responsible for protecting LI would be most desirable, to ensure that the probability of misuse being prevented, or at least detected, is maximised.

3) Usage constraints: An LI subject may want to place constraints on the use of LI, to allow them to restrict the way in which their LI is used. Difficulties when constraining usage arise when attempting to enumerate all the different applications of LI, because of the wide range of possible uses. An attempt to classify the main possible uses of LI is given in section III-B immediately below.

B. Uses of constraints

The use of LI can be divided into two main types. LI can be used to:

- provide the LI subject with a service or with location details, or
- provide a service or location details to a separate entity.

The LI subject may, of course, not wish other entities to gain access to its location information, and hence may use constraints to limit uses of LI falling into the second category. Both these two main categories can be further sub-divided, and we now consider some examples of uses of LI within these two broad classes — see also Figure 2. These lists are not meant to be exhaustive.

1) Providing services to the LI subject: We consider four main categories of use of LI where the benefiting entity is the LI subject.

- *Location based security* may be used to provide a security service to the LI subject. For example, the LI subject may not want to carry out transactions with retailers from certain locations. The LI subject can check the location of the retailer and use this information to decide whether or not it wants to carry out a transaction.
- *Location based messaging* may be used to inform an LI subject regarding any "buddies" who may be located nearby. These buddies may be a list of people maintained by the LI subject. This is similar to internet messaging with the added location property. An LI subject may not want "buddies" to know his/her location at a given time, a restriction which can be supported by the use of appropriate LI constraints.
- *Navigation* services are currently one of the most popular proposed uses of LI. LI is used to locate the LI subject, and information is provided according to their navigational needs. For example, the navigation service may have information about nearby traffic congestion which should be avoided. It may also plan a route which avoids this traffic.
- *Directory services* may be used by the LI subject to find local services. For example, LI may be used to help the LI subject locate nearby restaurants.
- *Other services* may be provided to the LI subject, including weather services, where weather information is provided based on the LI subject's location.

2) Providing services to other entities: We consider three main categories of use of LI where the benefiting entity is not the LI subject.

- *Advertising* based on location [6] is a potentially useful tool for retailers. For example, as an LI subject is passing a shop, messages about special offers may appear on the user device. Of course, advertisements may not be something that an LI subject wants; this is a problem similar to junk mail. LI constraints could be employed by the LI subject to prevent such a use being made of LI.
- *Location based security,* as its name suggests, refers to the provision of a security service based on the location of the LI subject. In particular access and authentication [2] may be provided based on the location of an LI subject. An example of where this may be useful arises in the context of wireless LANs. So called 'war-driving' attacks allow unauthorised users to access a network from outside the perimeter of a building [7]. A secure mechanism for providing LI to the entity controlling the network would prevent such attacks.
- *Location based safety* describes where, in an emergency, details of an LI subject's location is sent to the safety entity so they can be located quickly and efficiently. Although the LI subject may eventually be the beneficiary of this service, its immediate use is by the emergency service. In some countries, such as North America where E911 is deployed [1], it may not be possible for an LI subject to prevent its LI being used for this purpose.
- *Other services* that may be provided to entities other than the LI subject include LI subject tracking. This enables a range of possibilities, including allowing an employer to track employees to efficiently manage resources, and allowing a car-leasing company to track their cars.

If an LI subject wishes their LI to be used for one specific purpose, the use of constraints allows this to be made clear.

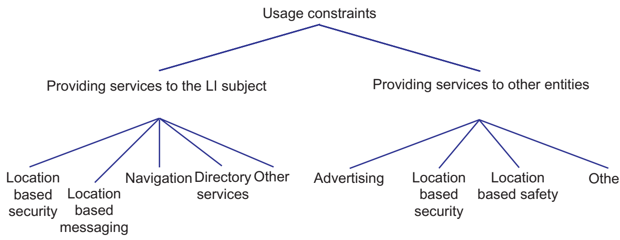

Fig. 2. LI usage tree

IV. Limitations of constraints

Once an entity other than the LI subject has possession of LI, it is difficult to force them to abide by the constraints which have been set.

A. Difficulties in preventing and detecting constraint abuse

As mentioned earlier, once an entity is in possession of LI they are free to do with it as they will. LI is data, and the constraints which may be set on it do not physically prevent the receiving entity from misusing it. What adding constraints does do, however, is to allow entities to know the wishes of the LI subject. A regulatory authority which oversees the way in which other entities handle constraints may go some way towards preventing constraint abuse.

Another problem which arises when considering the use of constraints is proving their abuse. We have already established the difficulties of preventing the abuse of constraints with LI; it is also difficult to prove an entity has abused LI.

B. LI constraint predicaments

The aim of using constraints with LI is to enable an LI subject to dictate its use. Applying constraints to LI may, however, lead to further security considerations.

When a user applies constraints to LI, they give information which indicates how, or how not, to use the LI. Although this information may be necessary to prevent the misuse of LI, applying constraints means that further information is divulged to the receiving entity. Two examples of this are now discussed.

1) Time constraint predicament: Two potential schemes for time constraints were mentioned in section III-A.1. One made use of a validity period for the constraints. The other is where the constraints are valid until a specified point in time.

The first scheme makes use of a time stamp which is added to the constraint. This allows a receiving entity to calculate the time at which a user was at the location shown by the LI. Of course, in most cases, the entities who are likely to receive LI are in all probability trusted by the LI subject, and so the fact that they know that a user was at a location at a particular time should not be a problem. The difference between this and the second scheme for specifying time constraints is that, in the latter case, a receiving entity is not informed precisely when the LI subject was at a particular location. The delay before the receiving entity obtains the LI may only allow an approximate location of the LI subject to be calculated. However, in some cases, LI may be used in real time and, in such cases, the second scheme may be inadequate. An example may be for a navigational service, where the location and movement of the LI subject must be calculated in order to provide the required information.

2) Distribution constraint predicament: If we place the responsibility for enforcing the LI constraints on the receiver of LI, then the presence of non-permitted LI at an entity is evidence that this entity is not acting within the constraints of the LI. Of course the problem with this is that it is not possible to prevent an entity from redistributing LI which it is not permitted to see.

V. Combining constraints with auditability

Preventing misuse of LI is inevitably going to be a complex task. For an entity to be able to use LI, they must have access to it. After an entity has seen the LI, they thereafter can use or misuse it as they please. Even when constraints are bound to the LI, an entity may choose to ignore them or decide not to pass them on.

Instead of trying to prevent misuse of LI, which is almost certainly an impossible task, we therefore propose the concept of auditability of LI. The idea is to enable all users of LI to determine where LI originates from, and to make all users accountable for their uses of LI. To work effectively, the majority of LI users must abide by the auditability rules, but this seems a reasonable assumption (otherwise there is little hope of achieving any control over LI). Of course, auditing will not prevent abuse, but it does enable misuse to be detected after the event, thereby acting as a deterrent to misuse.

The notion of auditability introduced here requires use of digital signatures. Every piece of LI, and its associated set of LI constraints, must be accompanied by a digital signature computed over both the LI and its constraints. That is, when any LI is generated by an LI gatherer, then, as well as generating and attaching the LI constraints, the LI gatherer must create a signature over the LI and the associated constraints. The LI gatherer might also be required to include evidence with the LI of how the LI was obtained, and include this evidence within the scope of the signature.

Any entity receiving LI must verify the accompanying signature, and must log an exception (and must not use the LI) if the signature verification fails or if the signature is not present. Moreover, all LI users must check the constraints accompanying received LI to determine whether they should be in receipt of the LI — again, if they are not then an exception should be generated and the LI should not be used. Finally, the LI and the signature should be retained for auditing purposes for a specified period of time.

We now consider how this combination of rules can prevent (or at least make more difficult) the mishandling of LI. First observe that the mechanism described above does not address the misuse of LI, i.e. the use of LI in ways prohibited by the LI constraints. It is instead intended to address the issue of unauthorised distribution of LI (after all, uncontrolled dissemination of LI is probably the issue of greatest concern to most LI subjects).

Suppose a malicious entity wishes to redistribute LI in a way prohibited by the LI constraints. If the entity simply sends it on as received, then the recipient will detect that the constraints have been violated and the malicious entity can be held responsible for the breach of constraints. Hence the malicious entity will need to change the LI constraints. This, however, will invalidate the original signature, and sending the LI without a signature will also enable the recipient to detect an LI use violation. Hence, if an entity wishes to disseminate LI with modified constraints, then they must sign the LI and indicate from where it was obtained — this may present a major problem for a fraudulent LI user. It will at minimum enable a subsequent audit to detect exactly which entity was responsible for disseminating unauthorised LI.

A further measure to restrict the ability to fraudulently disseminate LI would be to limit the entities capable of acting as LI gatherers and generating signatures on LI. If a LI gatherer required a licence (e.g. in the form of an attribute certificate) to generate signed LI, then a malicious user without such a licence could not falsely disseminate LI, except to other malicious users.

Clearly this notion of auditability is dependent on industry co-operation and a regulatory body to ensure that rules are obeyed.

VI. Conclusions and directions for further work

Although attaching constraints has the advantage of allowing entities to see the requirements of the LI subject regarding LI, in doing so it also allows them to see additional information which may breach the privacy of the LI subject. It is also difficult to ensure that entities abide by the constraints which are set by the LI subject, and to prove when the constraints have been abused. Finding ways to address such issues is an important research challenge.

In order to enable a wide use of location based services it is important to have a single language for the specification of LI. This should allow LI to be generated, transferred and used on a wide variety of platforms. Currently the most promising means of achieving a universally recognised means of specifying LI would be to employ an appropriately devised XML schema. XML (eXtensible Markup Language) is a language for data exchange between different devices. It allows data to be shared regardless of programming language or operating system, making it a strong candidate for use with location based services and to describe LI. If LI is described in XML, it should also be possible to describe constraints in XML, giving similar advantages. XML can also be used to create digital signatures, which may be used to support the auditing scheme mentioned above.

Location is just one aspect of a context based service. A context based service is one in which the context of an application automatically initiates some activity. Examples of possible contexts other than location include temperature and special events. Of course different forms of context have different security aspects. For example, the temperature of a subject's environment may not be private data; however, the end user's personal blood temperature may be private. As with location information, it would be necessary to subject such data to distribution and use constraints. This would mean extending the constraints described here to different contexts.

Although this document identifies some of the constraints which may be set by the LI subject, no formal language is defined whereby constraints are verifiable and unambiguous. Defining such a language may be a fruitful area for future research.

Acknowledgment

The research presented in this paper is being supported by sponsorship from Toshiba Telecommunications Research Laboratory, UK.

References

[1] F. C. Commission, "Revision of the commission's rules to ensure compatibility with enhanced 911 emergency calling systems," *ORDER (DA 02-2423)*.

[2] D. E. Denning and P. F. MacDoran, "Location-based authentication: Grounding cyberspace for better security," in *Internet Besieged, Countering Cyberspace Scofflaws*, 2nd ed., D. E. Denning and P. J. Denning, Eds. ACM Press Books, February 2001, ch. 12, pp. 167–174.

[3] C. Schwingenschogl and T. Kosch, "Geocast enhancements of AODV for vehicular networks," *ACM Mobile Computing and Communications Review*, vol. 6, no. 3, pp. 96–97, July 2002.

[4] *3GPP TS 03.71 V8.7.0 Technical Specification Group Services and System Aspects; Location Services (LCS); (Functional description) Stage 2 (Release 1999)*, 3rd Generation Partnership Project, September 2002.

[5] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, *Handbook of applied cryptography*, ser. CRC Press Series on Discrete Mathematics and Its Applications, S. A. Vanstone, Ed. Boca Raton, Florida: CRC Press, 1997.

[6] U. Varshney, "Location management support for mobile commerce applications," in *International Conference on Mobile Computing and Networking, Proceedings of the first international workshop on Mobile commerce*, M. Devarakonda, A. Joshi, and M. Viveros, Eds. ACM Press, 2001, pp. 1–6.

[7] S. Byers and D. Kormann, "802.11b access point mapping," *Communications of the ACM*, vol. 46, no. 5, pp. 41–46, May 2003.